

AN INTRODUCTION TO BECOMING PCI DSS COMPLIANT.

Written by Michael Green.

This white paper discusses the background of Payment Card Industry Data Security Standard (PCI DSS), its commercial and technological implications and NetBenefit's own experience of implementing the PCI DSS Standard and how this experience could help you to reduce lead times, lower audit costs and reduce infrastructure expenditure for your own business's PCI compliance programme.

Every merchant that processes card payments and retains card payment details must adopt the Payment Card Industry Data Security Standard (PCI DSS). Failure to do so can result in merchants being subject to substantial fines, higher transaction costs or ultimately the suspension of banking facilities.

For NetBenefit the PCI accreditation marks the end of a comprehensive project to attain high security in payment standards across its managed hosting facilities and enables it to provide merchants with a purpose built hosting environment that will meet the stringent requirements of the Standards Council.

Darren Wiltshire,
Head of Engineering, NetBenefit.

What is 'PCI'?

A single retailer, or merchant, can process millions of records each year. If an authorised route is found into that merchant's system then the potential for fraudulent use of credit and debit card details is huge.

The ultimate purpose of the Payment Card Industry Data Security Standard (PCI DSS) is to help card issuers and banks manage their risk and exposure, by ensuring that

merchants take responsibility to ensure that every individual, be it an employee or contractor, that comes in to contact directly or indirectly with processing card payments takes consistent precautions against data theft and security breaches that could compromise cardholder data. PCI recognises that merchants in particular are a prime target for data thieves because they engage in activities – such as storing sensitive information – that place cardholder data at risk. However, it is in



Michael Green
Senior Product Manager

Michael Green first started working in the emerging Telecommunications and Internet Industry in 1995.

Michael has 16 years of experience, in various Product Management roles with leading Internet and Hosting organisations such as Virgin Media, KPN Qwest, Viatel and now currently with NetBenefit since March 2008.

In these roles Michael has managed products from the emerging broadband technologies, the rise of managed hosting and more recently large Cloud solutions and PCI DSS compliant platforms.

everyone's interest – whether consumer, merchant or bank – that the standard is consistently enforced so that sensitive data is protected and the cost of fraud is minimised for all parties. Indeed many public organisations that store sensitive customer information (not necessarily specifically payment card data) will also benefit from adopting PCI DSS standards. .

The Payment Card Industry Data Security Standard (abbreviated to PCI DSS or, commonly, just 'PCI') is a set of 12 requirements designed to secure and protect customer payment data. The standards are the brainchild of the PCI Security Standard Council, an independent body established in 2006 by major card companies American Express, Discover Financial Services, JCB International, MasterCard and Visa. PCI is an international initiative, intended to enhance all cardholder data security whether transactions take place in a store or online. PCI is regulated by the industry through a set of standards that cascade down from the card brands via banks to the merchants. The standards are enforced by the banks (card-issuing banks are known as 'acquiring banks') working in conjunction with the merchants to ensure they fulfil PCI requirements. Merchants that do not comply face fines for non-compliance ranging from €5,000 to €23,000, higher transaction charges or even the threat of banking facilities being suspended altogether - typically resulting in the cessation of trading. Although each

acquiring bank has previously taken its own approach to enforcement, there is increasing homogeneity and consensus on accelerating PCI.

There is no explicit regulation of PCI in the UK, although in the US there are states that have state laws in place which force components of PCI DSS. There is speculation that PCI may eventually have wider legal enforcement elsewhere and it has been noted that the UK government and regulatory authorities are generally getting more active in the area of data protection. From a PCI perspective, every touch point represents a potential data breach. At the simplest level it means all payment card slips must be destroyed. At the most complex level there are strict rules governing the technology used to manage and protect cardholder data. A PCI-compliant organisation must remove sensitive authentication data and limit data retention; protect their perimeter, internal and wireless networks; secure its applications and protect everything through ongoing monitoring and access control.

Acquiring banks are duty-bound to report regularly to card issuers about the status of merchants' compliance with PCI. They take the view that merchants should regard the cost of PCI compliance as an insurance policy, protecting them from the financial costs of failing to secure card data. Working toward PCI is, in any case, good practice because it can help improve the efficiency of an organisation's processes and also allows it to operate more securely

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 01

Install and maintain a firewall configuration to protect cardholder data.

– ultimately protecting their brand and reputation.

Does PCI apply to my business?

If you store, process or transmit any cardholder data electronically or manually, then your business needs to comply, regardless of its size. For example, you are allowed to store primary account numbers, cardholder names, service codes and expiry dates, provided they're protected in line with PCI requirements, but you are not allowed to store items such as PINs, CVC codes and other sensitive authentication data, even if the data is encrypted.

In practice, acquiring banks have concentrated their efforts so far on larger merchants, but as they address their commitments, they are gradually turning their attention to medium and small businesses. Each acquiring bank has taken a different approach to prioritising the size and type of merchants it requires to comply at any one time, but your business is likely to be considered favourably if you are already taking active steps toward PCI. Each card brand operates its own requirements for PCI compliance so minor variations do exist.

There is no escaping the fact that achieving PCI compliance can be a long, painful process for many businesses, but it is a necessary step – not only for a merchant to remain competitive but also in the long-term to allow it to continue to trade.

The commercial implications of PCI

Ultimately there is no escape from PCI. Whether you are a sophisticated multinational retailer or a small business that accepts card payments – online or offline, it is widely expected that much more rigorous enforcement will be commonplace from 2012.

Technologies and strategies for dealing with PCI are still catching up, although technology firms are ramping up research and development investment to provide better services and tools to cope with demands. PCI is here to stay, and it will become increasingly pervasive as time goes on.

Because higher transactional processing costs are now routine for many non-compliant merchants, some have done the sums and realised that the cost of compliance is lower than the overall financial implications of non-compliance. With this commercial imperative now clear, a number of companies are accelerating their PCI programmes and arguably those who achieve compliance earliest could even achieve a competitive advantage through their reduced cost base in the long term.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 02

Do not use vendor-supplied defaults for system passwords and other security parameters.

Since PCI covers your entire trading environment, all third-party partners that store, process or transmit cardholder data must also comply before you can achieve full compliance. Such third parties include:

- Payment service providers
- EPOS vendors
- Data storage providers
- Shopping cart providers
- Software vendors
- Web hosting providers

As an example, for those merchants that do not interact directly with an acquiring bank, but instead use a third-party payment gateway (such as WorldPay or PayPal) the implications are both technical and commercial. That payment gateway is also required to meet PCI standards though not all have become compliant with the same speed. For you to be compliant as a merchant, you would need evidence that your payment provider's standards meet the requirements of your own certification. Using such a payment gateway theoretically reduces your exposure – after all, such providers are experts in securely managing such transactions – but each provider has a different cost model for dealing with PCI and this aspect of compliance has yet to reach equilibrium. What's more, some payment services providers are now starting to refuse to take on merchants who are not already well down the road to PCI compliance themselves, so using a payment provider does not take your organisation out of scope.

The PCI community's focus is currently on volume – i.e. preventing hundreds of cardholder details being stolen. There have been a number of high-profile cases where business operations have been seriously affected by loss of cardholder data. For example, the cosmetics firm Lush had to close its UK web site in January 2011, in response to a sustained hacking attack over a three-month period which left users' details vulnerable to credit card fraud.

How does my business become PCI compliant?

There is a threshold of 6 million transactions per year, below which merchants are able to self-certify PCI compliance (although if a merchant has already experienced a security breach, independent auditing is still required). For businesses operating above this threshold, then annual, independent on-site auditing is compulsory. All merchants, regardless of size, must also submit to a quarterly network scan by an approved scanning vendor (ASV).

Those who have worked through ISO or Sarbanes-Oxley certification processes will be familiar with the kind of approach needed for PCI certification. It is just as demanding, if not more so. In the case of PCI, if your organisation processes more than 6 million transactions per year, then it needs to be independently audited and certified against the PCI Data Security Standard by a Qualified Security Assessor (QSA), who is in turn certified by the PCI Security Standards Council.

The QSA will assess your situation, recommend remedial action to address any shortcomings, and ultimately issue a clean bill of health. The QSA will also re-audit everything on an annual basis to ensure you remain compliant.

The PCI Data Security Standard consists of 12 requirements:

Build and Maintain a Secure Network

- Requirement 1:** Install and maintain a firewall configuration to protect cardholder data
- Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3:** Protect stored cardholder data
- Requirement 4:** Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5:** Use and regularly update anti-virus software
- Requirement 6:** Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7:** Restrict access to cardholder data by business need-to-know
- Requirement 8:** Assign a unique ID to each person with computer access
- Requirement 9:** Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10:** Track and monitor all access to network resources and cardholder data
- Requirement 11:** Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12:** Maintain a policy that addresses information security

The 12 requirements of PCI DSS compliance can be quite daunting for any merchant. NetBenefit has worked through all of the steps as both a merchant and a service provider which means we understand the full scope of the project.

We wanted to be able to offer our customers a PCI DSS compliant solution that can scale with their requirements from customers using payment gateways all the way up to merchants who manage the payment process themselves. We have addressed as many of the requirements as possible in delivering the PCI compliant hosting environment so that customers can concentrate on their own systems, processes and policies.

Darren Wiltshire,
Head of Engineering, NetBenefit.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 04

Encrypt transmission of cardholder data across open, public networks.

Each requirement is actually broken down further within the standard with more specific sub-requirements.

As can be seen, achieving PCI compliance is a major undertaking for any organisation and is a board-level programme – not something that falls exclusively into the realm of the CIO, estates manager, customer service team or marketing specialists, all of whom have an interest. Your sales and marketing director will want to reassure customers and protect brand equity; your credit controller will want to reassure your bank that you are minimising risk; and your IT service delivery team will want to provide watertight continuous availability.

PCI encompasses physical security throughout the organisation (even down to ensuring that visitors wear identity badges) as well as many potential discrete processes and policies. That said, the compliance framework is chiefly aimed at preventing electronic fraud and breaches of data security, and it naturally focuses heavily on technology.

Technology implications of PCI

A payment card transaction process begins with the authorisation at the point of sale – usually via a PDQ ('Process Data Quickly') terminal. The merchant requests and receives authorisation from the card issuer, which enables the merchant to complete the purchase with the expectation of getting paid. The acquiring bank then

exchanges information with the card issuer, which enables the merchant to complete the purchase with the expectation of getting paid. The merchant bank pays the merchant, and the cardholder's bank debits the cardholder's account.

The merchant's responsibility lies with the first of these steps. Regardless of whether a separate payment provider is used or whether the merchant engages directly with the acquiring bank, the merchant must be able to demonstrate that all points of potential vulnerability (servers, routers, gateways, network connectivity, wireless access points, storage and backup systems to name but a few) are compliant. A necessary prerequisite of engaging electronically with any partner or third party during the authorisation process is that they must demonstrate their compliance to you so that you, in turn, can demonstrate compliance.

A PCI-compliant infrastructure needs multiple layers of security (including Firewalls and Web Application Firewalls), and the data centre itself installed on a secure site. If your systems are running Windows and Linux, you could be accredited for both, but each would require separate auditing; indeed, different releases of the same operating system would need to be audited individually. Even application code needs to be certified as secure. However, it should be borne in mind that although PCI compliance appears onerous, it mirrors best practice for overall information and network security anyway.

As a rule, PCI compliance is consequently easier to achieve for a start-up than for an established, large business running a mixed environment of legacy servers and storage solutions. Such unstructured, complex environments present their own challenges in terms of data loss prevention, availability of information, archiving and cost - and for these companies it may be that PCI compliance falls within the scope of a planned consolidation, virtualisation or migration programme intended to address other business issues.

One solution is, of course, to outsource aspects of data centre management – or even the data centre itself – to a third party. Although you would still need to audit each component, you should expect your hosting provider to be able to deliver a PCI-compliant toolkit; this can substantially reduce the time and cost involved with auditing the infrastructure. Not all hosting providers are geared up to provide this however - and the cost benefit to your business of outsourcing could be negated if you find yourself having to specify and audit every element yourself (including the non-technical physical security aspects of PCI).

NetBenefit: a PCI compliance case study

NetBenefit has both the experience of offering a PCI-compliant toolkit to its hosting customers and, as being part of GroupNBT, its sister company “Easily” has been through a rigorous PCI compliance process as a merchant. Because Easily.co.uk as a company processes card

transactions from its customers, it has had to become PCI certified itself. This section describes its experiences and highlights areas where it can offer advice to customers to help minimise the pain of transitioning to a compliant environment. Easily.co.uk PCI-compliant certification arose as a result of commercial pressures. The company was required by the acquiring banks to achieve certification and, as noted earlier, it was becoming subject to higher transaction costs through not being certified. The project began by appointing a QSA (in the case of Easily.co.uk, from personnel from CNS, a specialist consultancy based in London). The statement of work defined timescales, responsibilities, and the overall process. The starting point was a gap analysis followed by remedial action. All aspects were then audited and individually re-audited until they could be certified as compliant. Despite Easily’s procedures, process and technology being perceived to be of a high standard to start with, the project was still huge in scope and took 18 months overall to complete. The PCI project was managed, implemented and supported by the NetBenefit engineering team.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 06

Develop and maintain secure systems and applications.

By attaining the service provider accreditation, NetBenefit has demonstrated that its processes, systems, policies and procedures comply with the relevant requirements and can now provide a comprehensive PCI DSS compliant environment to its customers seeking PCI DSS as a merchant.

Kevin Dowd,
Director of Security Assessment, CNS

The transition was managed by a steering group drawn from across the business, including department heads from:

- Development
- Engineering
- Service delivery
- Operations manager (physical security and facilities)
- Product management
- Credit control
- Marketing

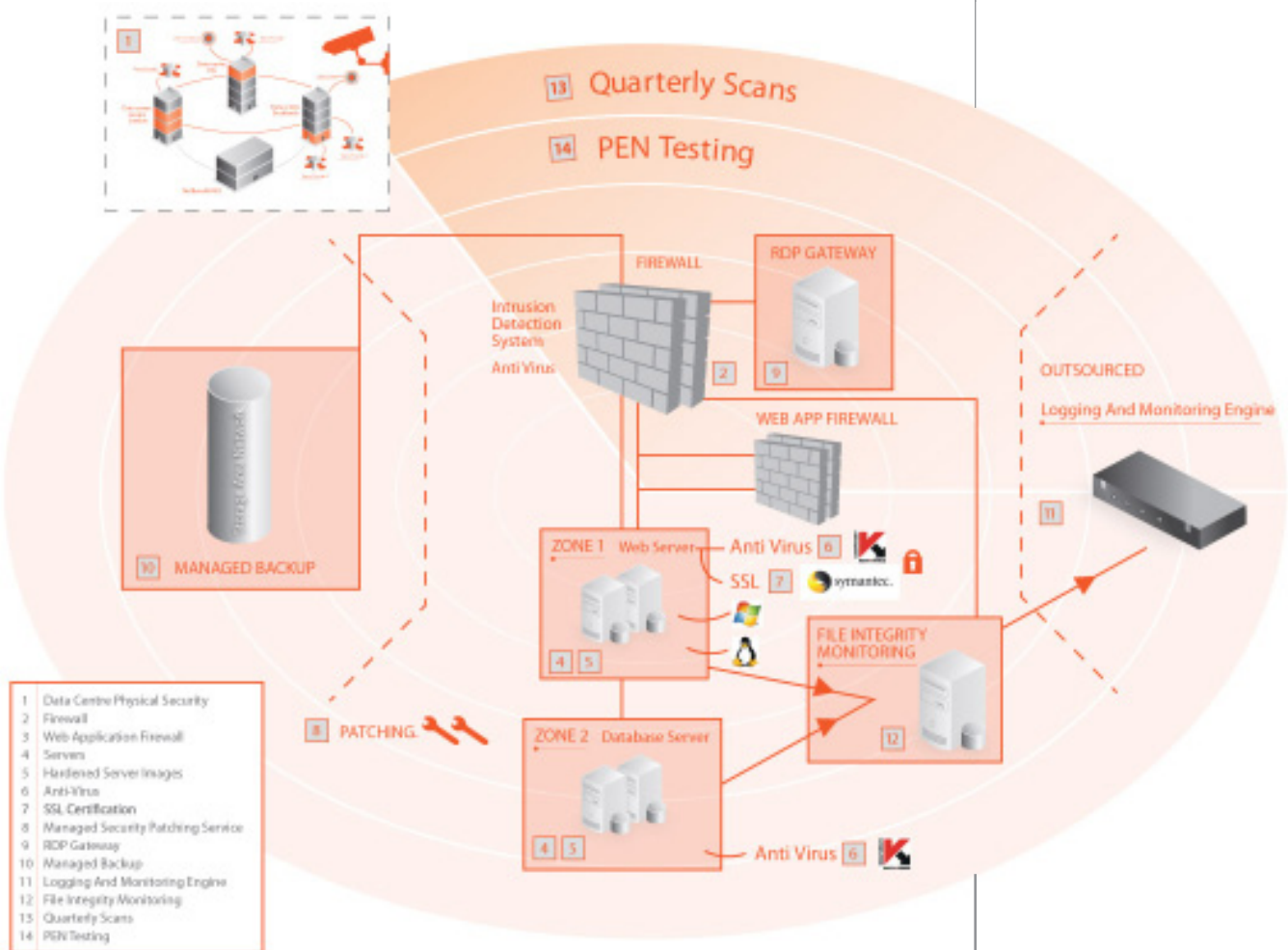
Ultimate sign-off for all aspects rested with the chief technical officer, reporting to the board.

To achieve PCI DSS certification as a Service Provider, NetBenefit built a model environment that included all the technology requirements of the PCI standard. Elements were selected from industry-standard software and hardware components. Although in a live situation the actual systems used would still need to be audited alongside the customer's own applications, the intention of the model environment is to ensure that all components within it are effectively 'pre-audited', meaning that auditing by a customer's own QSA should be a relatively fast and painless process.

The technology and key features of NetBenefit's model environment are described below. The model environment provides a blueprint for customer solutions; more detailed technical documentation is available to NetBenefit's customers.

Since achieving PCI compliance, NetBenefit submits itself for auditing each year – comparable to having an annual PCI 'MoT' – to retain its certification.

Overview of the NetBenefit model PCI environment



The schematic diagram illustrates the configuration of NetBenefit’s PCI-compliant service provider model environment. The data centre is physically secure. It, and all NetBenefit sites which can access it, are governed by strict access control procedures. The system comprises industry-standard firewalls, anti-virus tools, managed backup,

file integrity and log monitoring. The whole system is subject to quarterly network scans and additional penetration testing.

For those used to dealing with compliance with Sarbanes-Oxley, PCI has some important differences (apart from being based on contractual agreements rather than being

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 08

Assign a unique ID to each person with computer access.

enshrined in law). Whereas Sarbanes-Oxley lays out general principles concerning auditing, PCI requires that audit trails exist for all actions taken by any individual with root or administrative privileges. One of the key requirements for a PCI-compliant solution is therefore that all user connections can be directly tracked and audited.

By separating the network between the NetBenefit offices and the data centre and using a secure gateway solution to control access to customer servers, a central logging area has been created for auditing and security purposes. For Windows environments, the remote desktop protocol gateway (RDP Gateway) allows users to point their RDP clients to the gateway, which then acts as a central logging and security point for all connections.

RDP is installed on a server configured for high availability which provides a publically and privately accessible fully qualified domain name. A certificate server is installed, allowing a domain-verified public SSL certificate from VeriSign or similar to be used. The DNS resolution (from within the merchant and from outside) points to a public IP address in order to make sure the certificates are valid from both internal and external networks. An alternative solution using SSH Keys (Secure Shell) is available for Linux environments.

All server logs, including application and security logs are backed up and stored for a minimum of 1 year to comply with PCI.

PCI compliance benefits of partnering with NetBenefit

NetBenefit is in a unique position not only to offer its customers advice that can help reduce the time and audit costs associated with moving to PCI compliance, but also to provide a toolkit of hosted technology solutions that have been proven to pass a demanding auditing process.

Time to market can be reduced because customers do not have to start their compliance programmes from scratch. For customers with legacy e-commerce systems looking to move to a PCI-compliant platform, NetBenefit's solution offers an environment that already sits within scope. Customers may not need all of NetBenefit's component offerings, but NetBenefit's model environment can reduce some aspects to a 'tick in the box' rather than a full audit.

Looking again at the '12 requirements' of PCI, NetBenefit can advise customers on most of them with the exception of requirement 6 (which relates to the customer's application) and requirement 7 (restricting access to data within the business itself on a need-to-know basis). Indeed, a NetBenefit hosted solution takes on responsibility for complying with security centre aspects of seven of the requirements:

Our PCI DSS Toolkit

Firewall	Fortinet
Anti-virus	Kaspersky
Intrusion detection system	IDS on the firewalls
SSL (traffic encryption)	Verisign SSL's
Web application firewall	Barracuda Networks model 360 up to 660
Physical data centre security	
Two factor authentication	VPN with key/password combo on firewalls
Individual logins	RDP gateway for Windows or individual SSH keys for Linux
Server hardening	
Secured network	Private Vlan for customers with PCI settings on their part of the network; our Network Operations Centre network is secure to PCI standards
Logging and monitoring solution (outsourced)	CNS COMPLIANCEngine: Provides monitoring, central logging and incident response
File Integrity Monitoring (FIM)	Managed Server with OSSEC (Open Source Security, Host-Based Intrusion Detection System) installed

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks (achieved through SSL certification)

Requirement 5: Anti - virus

Requirement 5: Unique ID

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

In summary, the three key benefits of partnering with NetBenefit for your PCI-compliant solution are:

- Reduced lead times
- Lower audit costs
- Lower infrastructure costs (through hosted infrastructure)

Whether considering outsourced hosting for the first time, or moving from another hosting provider, NetBenefit can advise on the most effective shortcuts to support your own PCI compliance programme.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 10

Track and monitor all access to network resources and cardholder data.

Glossary

Acquiring Bank: A bank that issues payment or credit cards from a card issuer

ASV: Approved Scanning Vendor (responsible for scanning the network on a quarterly basis)

PCI (DSS): Payment Card Industry (Data Security Standards)

PCI Security Standards Council: The body that sets PCI DSS Standards

QSA: Qualified Security Assessor (certified by the PCI Security Standards Council to carry out independent on-site annual audits)

ROC: Report on Compliance (a formal document completed for the acquiring bank by the QSA)

RDP: Remote Desktop Protocol

SAQ: Self-Assessment Questionnaire (used for certification of merchants processing fewer than 6m transactions per year)

SSH: Secure Shell

Tier 1 – Tier 4: The PCI Security Standards Council has tiered merchants according to the number of transactions they carry out each year, and acquiring banks have focused most attention on Tier 1 merchants, i.e. those carrying out over 6m transactions per year and which require QSA assessment. Tiers 2 to 4 – which include merchants of all other sizes – must all undertake self-certification and quarterly network checks.

Further reading

Official PCI Security Standards Council web site: www.pcisecuritystandards.org

About NetBenefit

Established in 1995, NetBenefit is one of the UK's most experienced managed hosting companies. We specialise in providing tailored managed hosting solutions that deliver security, resilience and online performance for business critical websites, applications and online advertising campaigns.

We have evolved with the internet to our position today as a leading provider of bespoke, flexible managed hosting solutions to well known brands while remaining small enough to be committed to the success of all our customers.

Our team consists of experienced consultants, pre-sales, project managers, technical architects and engineers, all of whom are here to help guarantee the online success of your business. We are focused on delivering hosting peace of mind so that our customers can focus on what they do best.

- The NetBenefit team consists of approximately 70 members of staff committed to making our customers' business a success.
- We have offices in both the UK and France.
- We provide technical, professional UK based support 24x7 365 days a year.
- We have three customer data centres and a fourth located in Copenhagen for additional resilience.
- Our team is vetted to Baseline Personnel Security Standard.
- In addition to providing technical support and information architecture for our customers, we work closely with both Dell and Microsoft to develop, test and launch new hosting services.
- NetBenefit is a part of Group NBT. Group NBT is AIM listed and has successfully established its brands as leading providers of domain name and internet related services across Europe and into the United States.

About CNS

CNS is a specialist IT security and networking consultancy; established in the City of London in 1999 it is wholly owned by its employees and directors. Its customers vary in size, from FTSE 100 and large public sector organisations to SMEs, but are united in understanding the importance of digital information to their business, in their desire for pragmatic, knowledgeable help in securing their systems and data and in meeting their connectivity requirements. CNS is a PCI DSS Qualified Security Assessor (QSA), CESG CHECK & CLAS Consultancy & ISO27001 Lead Auditor providing advisory, project and managed information assurance and compliance services. www.cnsuk.co.uk www.compliancengine.com.

"NetBenefit are one of very few Hosting Providers in the UK that have taken on the not inconsiderable task of becoming PCI DSS Accredited Service Providers.

NetBenefit have embraced the value of gaining the Accreditation and are now in an ideal position to share that value with their customers. We have found them to be pragmatic, enthusiastic and, above all, compliant. That makes them rare."

Kevin Dowd,
Director of Security Assessment, CNS

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 12

Maintain a policy that addresses information security.