

Comply with PCI DSS. Quickly. Safely.

To comply with PCI DSS you have to meet the standard's 12 requirements

The Payment Card Industry Data Security Standard* (PCI DSS) was set up by major payment-card brands in 2006 to keep credit-card data safe. If you process, store, or transmit credit-card data then you have to comply with the standard. The standard has 12 requirements, and over 200 sub-requirements.

Fail to comply with PCI DSS and you could face hefty fines and higher transaction costs during the time that it takes – usually two years – to regain compliant status. Worse still, data breaches make headline news and can crush consumers' confidence.

It takes time and effort to comply, and to manage ongoing compliance

To be validated as PCI DSS compliant, most companies will have to pass an annual audit by a Qualified Security Assessor (QSA) who will check every sub-requirement.

Once you're compliant you have to pass an annual QSA audit, and quarterly security scans. You have to put in place processes for everything from how to change a firewall setting, to who has access to a server. And set up processes to log system changes, and process documents to create auditable records. To find out more about compliance, download the Security Standards Council's 'Ten common myths of PCI DSS'**.

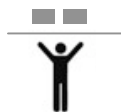
The Bunker meets all 12 requirements so we can get you to compliance quickly

We have been certified as meeting all 12 of the PCI DSS requirements – we're one of only a handful of UK data centres that are. You'll see The Bunker listed as a 'managed services' provider on Visa Europe's list of PCI DSS approved suppliers‡.

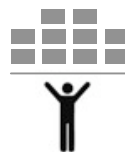
While the payment-card brands hold companies responsible for compliance, companies can hand-off requirements to external providers. For example, over 30 UK data centres meet two of the 12 requirements ('hosting providers' on the Visa Europe list). But if you hand-off two requirements – usually requirements 9 and 12 – to a 'hosting provider' you still have to comply with the other ten PCI DSS requirements. A 'hosting provider' can help you get to compliance, but it could be a slow and tiring road if you don't have the necessary resources. We have ready-made compliance components in place and solid PCI DSS know-how. So we can get you to compliance quickly.

But you may, like many of our clients, only need a hosting provider who can cover requirements 9 and 12 if you have the required capabilities to manage the remaining 10 in-house. Or you may want our gap-analysis to explain what you have to do to comply. Whatever you need, we can help you comply in the way that best suits your business.

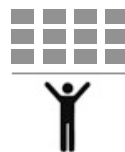
Comply with PCI DSS in a way that fits your business



You may just want us to cover **two** requirements, and house your servers in our compliant data centre.



You may prefer to cover the other **ten** requirements in house – it depends on your resources and priorities.



Or we can cover **all twelve** requirements for you. We can help you comply quickly, and manage compliance for you.



Whatever you need, we make sure that you can get on with your **business**.

“Validation of compliance is a snapshot in time. Effective compliance is a full-length feature film”

Bob Russo, General Manager,
PCI Security Standards Council

* The PCI DSS standard

Five major credit-card brands (including American Express, MasterCard, and Visa) set-up the PCI DSS standard in 2006. The standard is managed by the PCI Security Standards Council.

There are 12 requirements and over 200 sub-requirements. The standards document, notes, and glossary, run to over 100 pages.

** 'Ten common myths of PCI DSS'

Download this useful briefing here:
https://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf

‡ Visa Europe's list of PCI DSS validated suppliers

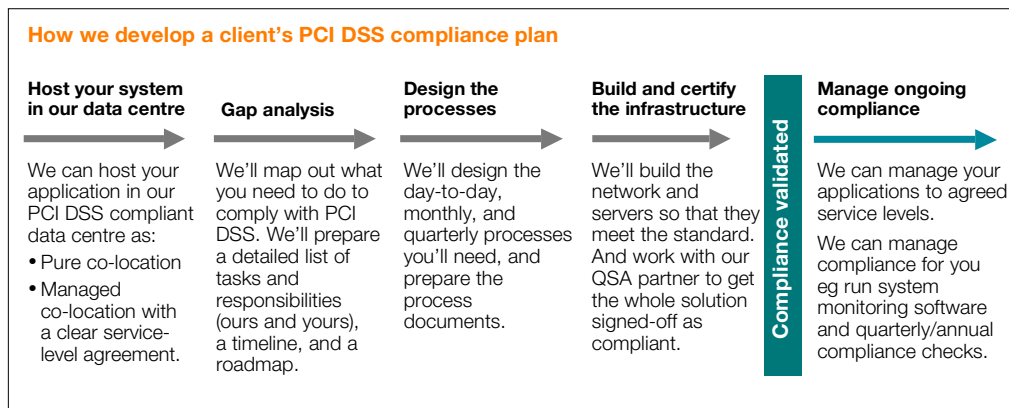
You can find the list here:
http://www.visaeurope.com/en/businesses__retailers/payment_security/ser vice_providers.aspx

You need to meet PCI DSS compliance in a way that fits your business

However you comply, it has to work for you – what works for one company won't suit another. We'll work with you to design a compliance process that fits: the way that your applications process, transmit and store card data; the way you work; your facilities; and your appetite for compliance responsibility – you may want to keep sign-off responsibility for most, a few, or the minimum of PCI DSS requirements.

We can get you to compliance quickly and manage your day-to-day compliance

We use a five-step process to get clients to PCI DSS compliance quickly, and manage ongoing compliance once you've passed your first audit. Many companies underestimate the resources and focus that you need to stay compliant – compliance can be easy to reach but difficult to maintain. Our process works like this:



We can work with you on a single piece of the process. Or we can take you from where you are now, through the system design-and-build process to compliance validation.

Then we can look after the day-to-day compliance activities. The processes, the documentation, the audits, the scans, and the record keeping (for example, we use Convergent Network Solutions'* COMPLIANCEngine to automate tests, and keep records of compliance-specific functions like log-file management, and vulnerability assessments).

We understand process, we comply with ISO 27001, and we're ultra-secure

We've mentioned that staying compliant with PCI DSS can be harder than getting that first compliance sign-off. You can't stay compliant unless you know how to keep to – and document – process. Our security-first culture means that we know the value of process, and we comply with ISO 27001 (the international standard for managing data in a secure way). So working to an auditable process is built into our business.

We understand the ground-level detail of PCI DSS: the fine detail of processes, server builds, and network design; what QSAs will and won't sign off.

And it's all backed-up by The Bunker Protocol™. That's PCI DSS peace of mind.

The Bunker Protocol™

All Bunker-base systems and applications are protected by The Bunker Protocol, our proprietary, Ultra* Secure process framework that includes:

Military-Grade Data Centres – in our underground bunker outside the M25 in Kent and our mirror facility in Berkshire. Both are protected by integrated processes for physical, digital and human security

Hardened Source™ – our unique combination of open source and proprietary technologies built and integrated in-house from the source code up

Flexible Support – our services desk uses ITIL v3 best practices for all service requests, and you decide what amount of incident management is appropriate to your in-house skill set and business processes



The average cost of a UK data breach is £1.9m, and costs range from £36,000 to £6.2m

Ponemon Institute research into 38 UK data-security breaches in 2010

To find out more about The Bunker's PCI DSS compliant services call 01304 814800 or visit thebunker.net/pci

*Convergent Network Solutions CNS is a specialist IT security and networking consultancy, and a PCI DSS Qualified Security Assessor.