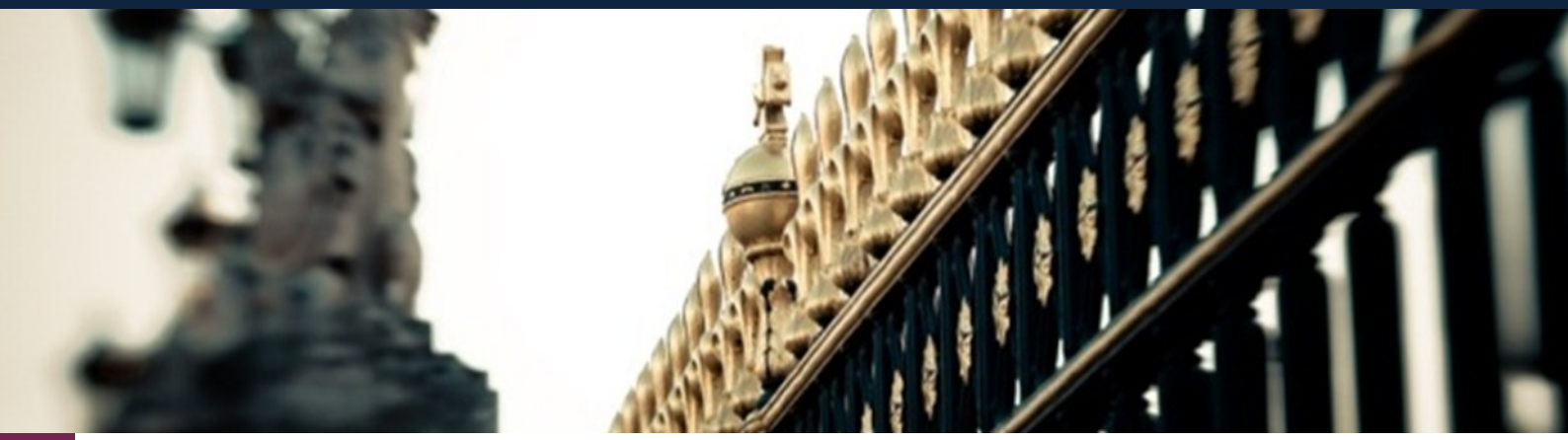
PCI DSS Version 3.0
From Compliance to Security



PCI DSS 3.0 - Themes & Challenges

With a focus on security, the new standard addresses global payment security threats and introduces solutions for ensuring the effective maintenance of PCI compliance.

Whilst version 3.0 offers greater clarity and flexibility enabling your business to focus on achieving the right security controls, the evolving challenges are clear.

"Cardholder data continues to be a target for criminals. Lack of education and awareness around payment security and poor implementation and maintenance of the PCI Standards leads to many security breaches" . PCI SSC 'PCI DSS 3.0 Change Highlights', August 2013

Key Themes

- **Compliance Maintenance** – added requirements and controls for maintaining PCI compliance in the business-as-usual.
- **Security Awareness** – new requirement aimed at increasing security training and awareness.
- **Security as a shared responsibility** - new requirements for working with third parties (service providers, cloud services, security services, etc.), to define responsibilities and ensuring PCI compliance is maintained by third parties.
- **Flexibility** – the standard provides greater flexibility in terms of ability to provide alternatives to specific requirements (without the needs for compensating controls).

Comsec Advantage for Version 3.0

As your security partner, Comsec will guide you through the entire PCI DSS compliance and certification process.

Comsec's dedicated team of QSA certified professionals have the expertise specifically required for version 3.0. Our key advantages for version 3.0 include:

- Adopting a security orientated approach to PCI Compliance as required by v3.0
- Our team of highly experienced QSA will enable your business to comply through the adoption of security controls that are best fitted to your organisation.
- Comsec will utilise the flexibility guidelines afforded by version 3.0 to achieve compliance to match your organisation's broader business and IT strategy.
- We provide proven PCI Compliance Maintenance and Work Plan development as required by v3.0.
- Comsec's shared PCI services and responsibility matrix (required by v3.0) enables compliance using third party entities (service providers, hosting providers, cloud services).
- We ensure that resource and costs associated with PCI compliance are kept to a minimum.

Our Approach

We provide turn-key PCI compliance solutions across all business sectors.

Our PCI packages provide a tailored end-to-end approach to match your organisation's requirements and establish security best practices.

Turn-Key PCI Compliance

- Scoping the Card Holder Data Environment
- Full on-site PCI DSS Gap Analysis
- Development of prioritised work plan
- Remediation Consulting
- Required PCI security testing (Penetration Testing, ASV & vulnerability assessment
- Security Awareness Training
- PCI compliant policy pack
- Assisting in certification process and liaison with PCI council
- On-site assessment and PCI ROC (Report on

Changes in Focus - PCI Version 3.0

Requirement	PCI DSS 3.0
SDLC (6.5)	SDLC should be aligned to current coding security vulnerabilities and trends (including new application vulnerabilities introduced by OWASP top 10).
Physical Security (9.9)	Requires physical inspection of payment devices (POS, Card Readers).
Security Policies (2.4)	Requires organisations to maintain a system component inventory.
Passwords & Authentication (8.2, 8.6)	New password policy requirements providing greater flexibility. QSA can provide expert consulting in the field of passwords and authentication to design a secure password policy for the business.
Key Management (3.5, 3.6)	New specific requirements for Key Management e.g. KEK must be equal or stronger than the DEK (Data Encryption Key).
Penetration Testing (11.3)	New requirement to ensure that Penetration Testing is based on industry-accepted security approaches and methodologies (NIST, ISO).
Security Training & Awareness (9.9.3, 8.4)	New Training & Awareness requirements bringing greater focus on specific areas (password strength, secure development practices).

A Unique Partnership

Our approach to PCI DSS compliance leverages upon years of experience and the successful collaboration with over 100 companies across Europe, including leading brands and enterprises across all sectors.

Our unique advantage stems from Comsec's ability to provide the end-to-end support and guidance you require to achieve PCI compliance while remaining product agnostic.

Our Commitment

Security as a Business Enabler

We believe that the role of information security is to enable business growth. At Comsec we are constantly looking for the synthesis of security into the business requirements. Our deep industry and business understanding enables us to tailor our services to facilitate specific business requirements.