

---

## PCI-DSS Free Online resources from Advent IM

### **Companies looking for clarification on the Payment Card Industry Data Security Standard (PCI DSS) can now take advantage of free online resources from security consultancy. Advent IM**

With an imminent compliance deadline of October 2009, the Payment Card Industry Data Security Standard (v1.2) applies to all those who physically or virtually transmit, store or process card payments, including any media such as voice recordings that might carry card details. Failure to comply with the standard could see organisations facing a minimum of £50K fines, damage to brand reputation, loss of business and the risk of closure.

PCI DSS promotes best practice information security. It is designed to protect the customer and all those involved throughout the payment process and is supported by five major credit card companies: Visa, MasterCard, American Express, Diners Club and JCB. The standard, which covers internal and external networks and all applications both fixed and online, also encompasses all active and unattended Point of Sale (POS) terminals. Ultimately, CEOs or equivalent are accountable for ensuring their organisation meets the standard. Retailers can look to external consultancies to independently assess the organisation's processes for storing and transmitting details and conduct necessary 'penetration tests' to gauge their compliance.

Mike Gillespie, Director at Advent IM, says: "In 2007, the UK truly became aware of the PCI DSS standard, and the implications on merchants for failing to comply when TK Maxx was fined for not adequately protecting customer data and more specifically, cardholder data. Since then very little has happened in the UK with regards to mandating compliance. However, as incidents of security breaches in general rise, Acquirers are beginning to insist on evidence of merchant compliance to safeguard them from any potential risks. However, we are aware that a lot of companies are still confused about what regulations apply to each organisation's merchant level, whether they need an ASV or USA and what each acronym means. We are encouraging all companies that have any access to card details to come forward to ascertain their merchant level and determine their compliance requirements. We will be able to advise whether the standard applies to them and the measures that need to be adopted to become compliant."

There is the consultancy adds a common misconception that compliance can only be achieved using the services of a Qualified Security Advisers (QSA). However, in many cases, merchants do not need the services of a QSA, especially those that are at Merchant levels 2, 3 or 4. It is also important that merchants maintain independence by ensuring that their Automated Scanning Vendor (ASV) and the QSA, should they need one, are not one in the same or from the same company.

Advent IM has worked successfully with a number of public and private sector organisations already by mentoring them through the standard, assisting with process flow identification and providing holistic security advice across the 12 standard requirements, including physical security. Gillespie adds, 'There is a tendency to overlook physical security as often PCI DSS compliance projects are given to IT or Finance departments to run. As with the whole of the standard it is as much about people, places and processes. Simply throwing technology at the problem is not the answer to compliance. Many companies will install a CCTV camera and think that satisfies the physical security element but an ineffective or unnecessary camera is useless in the event of a breach. Where we add value is by bringing our specialist knowledge of ISO27001 into play to ensure measures are appropriate and commensurate with business risk. Even if your Acquirer insists on a certificate of compliance from a QSA, consultancies like ours can still provide you with advice and guidance that will help you maintain compliance not just now but in the future- and without the QSA price tag.

Online resources are available at:

[http://www.advent-im.co.uk/website/pci\\_compliance.aspx](http://www.advent-im.co.uk/website/pci_compliance.aspx)

Press release: Information Security Online – 18.08.2009