

THE CORPORATE IT FORUM

The Corporate IT Forum (tif.) provides an environment for IT professionals to exchange their experience of IT issues. The Forum is run by a professional management team on behalf of its corporate subscribers. These subscribers require a truly unique service: a confidential, SUPPLIER-FREE environment, in which corporate-level IT professionals openly and honestly hold discussions, attend workshops & seminars and make use of a moderated, E-mail-based Q+A service to exchange ACTUAL experiences of IT. This exchange of expertise significantly benefits both the subscribing organisations and participating individuals alike.

The Forum is extremely effective because over 3,600 corporate IT professionals, within 150+ subscribing organisations (including over half of the eligible FTSE 100), contribute over 60,000 man years' know-how and experience in implementing IT solutions. No larger knowledgebase of real-world, current IT expertise exists within the UK. The use of tif.'s expertise within its subscriber community has directly contributed to reducing IT project costs and shortening implementation timescales.

To further discuss the many benefits to your organisation of taking out a subscription to The Corporate IT Forum, contact us on 01442 866 634 or visit our website, www.tif.co.uk.

Delegate Organisations

7 delegates from the retail sector participated.

Workshop Process

The event provided an update on subscriber experience in trying to implement PCI standards following the release of PCI 1.1 in September 2006. The implementation deadline of June 2007 is fast approaching and there are still many unresolved issues and contradictions in both the requirements and the likely consequences of any non compliance.

Summary

- ◇ Be Aware: The recent changes to the PCI standard can make you non compliant if you are currently compliant under PCI 1.0
- ◇ VERY IMPORTANT: It does not matter whether you are Tier 1,2, or 3, the *same* standards apply: the level of compliance required does not differ
- ◇ IMPORTANT: ALL Compensatory Controls have to be approved by the Acquirer *regardless* of whether you are a Tier 1, 2, or 3 merchant
- ◇ Unless you are significantly into the implementation of the PCI standard already you are unlikely to complete its implementation by the new June 2007 deadline. If you are in the gap analysis or planning stage you are unlikely to complete implementation by the end of 2007 if you are a Tier 1 Merchant
- ◇ Best Practices:
 - Avoid keeping credit card information in any system AT ALL: instead keep the Merchant copy until six months after payment is completed and then shred it
 - If keeping data, have it in as few systems as possible and keep these ring fenced
 - Encrypt data at the *point of entry* to the system: this ensures, inter alia, that the data cannot be read except by the application
 - Reduce the scope of PCI applicability by not holding data in systems that don't need it, and by segregating any systems that do need it—this can considerably reduce the scope of work to be done.

- ◇ Page 2 of the standard has a table of data elements that cannot be stored
- ◇ Audio recorded data comes under PCI
 - Under PCI 1.1, certain data cannot be stored, even with mitigating controls, and this creates an issue for audio recordings
- ◇ If you have reasonable plans, can show continuing and sustainable progress, and have business support then
 - Visa are unlikely to fine you at June 2007 for not being implemented
 - MasterCard's position is that you will be non-complaint and liable to fines.
- ◇ If renewing contracts with MC/V or other card scheme then get a Non Disclosure clause inserted: this is to ensure that they cannot disclose whether you are compliant or not and protect you from any 'name and shame' campaign
- ◇ Some do not use a Qualified Security Assessors (QSA) until the Gap Analysis has been done, or the work program identified
- ◇ MC/V are unlikely to move to turnover-based Tier qualification: the aim of the PCI standard is to protect *card* data and transaction level qualification meets this objective
- ◇ Some organisations are seeking to apply the *minimum* level of controls necessary to meet the standard whereas others (Tier 2) are seeking to become compliant at the *highest* degree possible
- ◇ There is a lack of consistency between MasterCard, Visa and Barclaycard over what can and can't be displayed on the Merchant slip
- ◇ CVC2 / CVV2 Storage: The standard explicitly says this must NOT be stored yet some delegates have been told it can be.

Contents of the Full Report

The following is a list of the additional material contained in the full output report from 'PCI Establishing the Facts WebEx. Subscribers can download any of the 200 workshop output reports via the website. Non subscribers will receive the full output report (circa 15 pages) from the workshop that they attended for which the full fee of £475 has been paid.

- ◇ Summary and Best Practice Conclusions
- ◇ Introduction & Background
- ◇ The PCI Standard 1.1
- ◇ PCI Project Approaches: Case Examples
- ◇ Launch Of The PCI SSC 1.1 Standard
- ◇ Deadlines
- ◇ Priorities
- ◇ Handling Partner Organisations
- ◇ Encryption & Multi Platform Encryption
- ◇ Compensating Controls
- ◇ Related Links
- ◇ Actions
- ◇ Delegate Information

Disclaimer: The views and opinions expressed herein do not necessarily reflect the views held by subscribers to The Corporate IT Forum neither does The Corporate IT Forum Ltd accept responsibility for the correctness or consequences of following any of the suggestions expressed herein.