

Abstract – PCI Compliance

tif. Subscriber Workshop: Thursday 19th April 2007

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 Information

22 delegates from the retail sector attended

Introduction: Workshop Scope

This workshop covers concerns raised following the release of Version 1.1 of the PCI DSS Standard (September 2006). Specifically issues relating to; compensatory controls, audio-recorded data and how changes could render a currently-compliant merchant non-compliant.

Representatives of Mastercard, and AmbironTrustWave Ltd were in attendance and were positive in helping to answer delegates' questions. They have submitted written responses to issues could not be dealt with on the day. These are included in relevant sections of the report

Summary and Best Practice Conclusions

Overall Summary: this topic is still HOT—problematic, confusing, and unachievable for some, even with the revised deadlines.

Significant Changes Since the Last tif. PCI Workshop

- ◇ Note: Unless marked as a direct quote the statements here are summarisations of the actual statements made. See the main Output Report for a fuller dialogue
- ◇ For Level 1 Merchants there are now *three* different compliance dates: one for each of Visa, MasterCard, and American Express!
- ◇ Compensating controls are *temporary*: they are not classed as permanent solutions. At some point you must get rid of the compensating controls and *go for full compliance*. (Source: MasterCard)
- ◇ Compensating controls appear to be organisation specific, or Acquirer specific: the control used in one organisation may not be valid in another
 - “The Acquirer can accept or reject compensating controls at will.” (Source: Ambiron Trust Wave)
- ◇ Compensating controls will *not* be publicly shared with Merchants by the QSAs, the PCI, or Card Associations (Source: Ambiron Trust Wave)
- ◇ You may achieve compliance by just showing evidence from other non-PCI compliance mechanisms
 - “Get your QSA and Acquirer to work with you on that so that it is fully understood that you are *compliant by another means*” (Source: Master Card)

Confidential: Corporate IT Forum

- ◇ The scan does *not* need to be done by an approved scanner, but the results need to be approved by the QSA. (Source: Ambiron Trust Wave)
- ◇ Part of the Merchant responsibility is to ensure its suppliers (including software vendors) are PCI compliant, regardless of whether that third party organisation is within the scope of the scheme or not. (Source: MasterCard)
 - Card Issuers are *within* the scope of PCI but are *not compliant*. MasterCard is not currently focussing on them. Instead it is focussing on Merchant and Acquirer compliance. (Source: Master Card).
 - To a Merchant a Card Issuer is a third party used by them.

Current Main Areas of Uncertainty or Problem

- ◇ Key problem areas are encryption, voice recording, third party software, and legacy systems
- ◇ Third-party software vendors are not compliant: there is no timescale for them to comply: the Card Schemes have completely omitted this when they set the deadlines for Merchants
- ◇ The uncertainty of third-party software compliance adds significant risks to an organisation's PCI/DSS project
- ◇ Master Card, Visa and AMEX all have *their own* penalty scheme for *each of the Acquirers*: the Acquirer has the right to pass that down to the Merchant
- ◇ The PCI and Card Associations policy is not to disclose any existing agreed compensating controls, making reinvention/rediscovery necessary
- ◇ There is no specific date for compliance that the Card Schemes agree on—an issue for organisations using multiple Card Schemes.

Delegate Interest Areas

- ◇ Delegates were strongly interested in other organisations' compliance status, and the handling of specific items—mainly encryption, voice recording, and legacy systems
- ◇ Some delegates have PCI-affected systems or infrastructure which is outsourced
- ◇ Main Interest Areas:
 - Encryption
 - Voice recording (analogue and digital)
 - Legacy systems
 - Contractual relationship between the Merchant and the Acquirer
 - Data retention
 - Compensating controls
 - Penalties and fines
 - Delegate status on compliance
 - How to achieve compliance at minimum cost.
- ◇ Issue: there is no specific date for compliance that the Card Schemes agree on—an issue for organisations using multiple Card Schemes
- ◇ Some organisations have multiple business units which are at different Merchant levels e.g. Level 1 and Level 2 is common
- ◇ Cited: we have 50 applications and 10 processes where card data is processed. We also have worldwide Contact Centres which must be PCI compliant.

Confidential: Corporate IT Forum

Contents of the full Report

- ◇ Summary and Best Practice Conclusions
- ◇ Significant Changes Since the Last tif. PCI Workshop
- ◇ Current Main Areas of Uncertainty or Problem
- ◇ Delegate Interest Areas
- ◇ Part 1: Workshop with Master Card and Ambiron Trust Wave Present
- ◇ Update & Review of the Revised Standard: Version 1.1
- ◇ The Council
- ◇ The New Version
- ◇ Compliance Dates
- ◇ Financial Penalties
- ◇ Compensating Controls
- ◇ The Feasibility of the PCI/DSS Requirements
- ◇ Third Parties
- ◇ Third-Party Software
- ◇ Network Segregation & Encryption
- ◇ Audio Recorded Data
- ◇ Staff Checks
- ◇ Merchant Slip's
- ◇ Hot Cards
- ◇ Other
- ◇ Part 2: Workshop Delegates only present: MC and ATW not present
- ◇ Compliance Status & Plans
- ◇ QSAs Used
- ◇ Policies
- ◇ Ongoing Maintenance of PCI
- ◇ Encryption
- ◇ Monitoring, Logs & Audits
- ◇ Data Retention
- ◇ Contractual Relationships with Acquirers
- ◇ Related Links
- ◇ 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.