

CIPFA
BETTER GOVERNANCE FORUM

**DO YOU KEEP CREDIT CARD INFORMATION SECURE?
CAN YOU PROVE IT?**

The **CIPFA Better Governance Forum (BGF)**, in conjunction with IT security specialists **encription**, have put together a selection of services which will ensure that your organisation is Payment Card Industry (PCI) compliant and remain so. The service involves regular security testing as well as the implementation of security standards and procedures. These services are detailed on the attached sheet.

Any BGF member signing up for one or more of these services before 31st March 2008 will be given a 15% discount on the service.

Computer and credit card fraud is increasing. Malicious hackers can steal unprotected credit card information, sell it on, clone it or use it themselves. Some time ago the credit card industry introduced PCI standards to try and ensure that information is stored and handled in a secure manner.

Their main focus of attention was on the larger merchants who processed more than 150,000 transactions per annum. These organisations are required to go through a formal third party IT audit to ensure compliance, failure to do so can lead to a £250,000 fine.

Recently, there have been several high profile frauds involving the loss of computer held credit card data, TK Maxx for example. A serious issue for the credit card companies is that they are seeing more and more fraud and loss of data occurring where the merchant is handling considerably less than the 150,000 threshold.

As a result of this, smaller credit card processors are being urged to become PCI compliant. Where fraud is taking place the credit card companies are being far more aggressive and are imposing the same level of fines that they impose on the larger merchants, up to £250,000 as well as taking legal action to recover any losses.

Contact:
Tony McDowell
encription limited
01905 754440

www.encription.co.uk



CLH3 SEP07



PCI (Payment Card Industry) SECURITY STANDARDS

How do these standards apply to you?

If your computer systems, including your web site, processes credit or debit card payments then you are required to be PCI DSS compliant.

What is PCI DSS (Payment Card Industry Data Security Standard)?

This standard (commonly known as 'PCI') represents a common set of security practices that help to ensure the safe handling of payment card data. Created by the 5 major card companies (American Express, JCB, MasterCard and Visa) this standard is designed to:

- Build and maintain a secure network
- Protect (cardholder) data in transit or at rest
- Maintain a vulnerability management programme
- Implement strong access control measures
- Regularly monitor and test your IT infrastructure
- Maintain an information security policy.

What happens if you are not compliant?

You must show that you have taken the necessary actions to protect the data and conform to the PCI standards, failing to do so may result in up to a £250,000 fine and other legal action.

How do you ensure compliance?

If the number of card transactions that you process annually is less than 150,000 then you can carry out self certification against the stated PCI DSS requirements and hence prove compliance. IT Security experts encription limited in conjunction with IPF have developed a series of testing modules and services that will assist you in self certification:

The Services	encription does	encription advises
Build and maintain a secure network		✓
Protect (cardholder) data in transit or at rest	✓	
Maintain a vulnerability management programme		✓
Implement strong access control measures	✓	
Regularly monitor and test your IT infrastructure (3/6/12 months)	✓	
Maintain an information security policy.		✓
Test web site security daily	✓	

What are the benefits?

1. You will be able to gain PCI DSS self certification thus showing that you have taken the necessary actions to protect the data and conform to the standards.
2. You can be sure that your web site conforms to the highest level of available security on a daily basis.
3. Your risk of an IT security breach on your e-commerce site is greatly reduced.



CLH3 SEP07

