



The Versatile BI Solution!

Click&DECiDE's PCI DSS Version 1.2 Compliance Suite

Nerys Grivolas

December 1, 2009



Executive Summary

The strict requirements of the Payment Card Industry (PCI) Data Security Standard (DSS) are forcing retailers to face severe penalties for the disclosure of a security breach of protected cardholder information. Today retailers must demonstrate the ability to prove diligence in managing information security risk. Enterprises must monitor and protect databases, down to the individual consumer level. Retailers need to centrally collect and store audit trails from these databases and correlate them with perimeter devices to recognize and prevent security breaches before they occur. Finally, they need to render vulnerability assessment data actionable by correlating scanner data with asset value and delivering it to the network organization to accelerate proactive patch management.

Click&DECiDE's PCI DSS Compliance Suite offers complete security Log or Event Management – i.e. a type of software that automates the collection and consolidation of event log data from operating systems, applications and network devices. The Security Log Management software securely archives and translates the logged data into correlated and simplified formats, offers alerting features and provides security reporting and forensic analysis. Security Log management thus encompasses the processes of log centralization, archiving, monitoring and reporting.



Table of Contents

- 1. Introduction 4
 - 1.1. Introduction to PCI DSS 4
 - 1.2. Structure of PCI DSS Version 1.2 4
 - 1.3. The Consequences of Non-Compliance..... 4
- 2. Click&DECiDE’s PCI Compliance Suite 5
- 3. Mapping..... 5
- 4. Conclusion 6
- 5. Going forward with Click&DECiDE..... 6
- 6. Contacting Click&DECiDE..... 7

Legal Notice

The information contained in this document is subject to change at any time without notice. Except as expressly set forth in the applicable agreement, Net Report SAS makes no warranty, (and this document is not intended to create any warranty), express or implied by law, statute or course of dealing. This document is intended only as a guide to assist the customer in understanding Click&DECiDE’s software application, and the customer should review all results from the Click&DECiDE PCI DSS Compliance Suite with its professional advisors.

Document Release: December 1, 2009



1. Introduction

1.1. Introduction to PCI DSS

PCI DSS stands for Payment Card Industry (PCI) Data Security Standard (DSS). It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and other security issues. A retailer processing, storing, or transmitting credit card numbers must be PCI DSS compliant or they risk to lose the ability to process credit card payments.

PCI DSS reflects the combined interests of VISA, MasterCard, Discover, American Express, and JCB. These five credit card brands agreed on a common set of security standards. Prior to this, each card brand managed their own set of requirements:

- MasterCard - Site Data Protection (SDP) Program
- VISA - Cardholder Information Security Program (CISP) and Account Information Security (AIS)
- Discover - Discover Information Security and Compliance (DISC)
- American Express - Data Security Operating Policies
- Merchants and Service Providers must validate compliance with an audit by a PCI DSS Qualified Security Assessor (QSA)

1.2. Structure of PCI DSS Version 1.2

The current version of the standard (Version 1.2) specifies twelve requirements for compliance, organized into six logically related groups called "control objectives".

The six control objectives and their requirements are:

- **Build and Maintain a Secure Network**
 - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
 - Requirement 3: Protect stored cardholder data
 - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
 - Requirement 5: Use and regularly update anti-virus software
 - Requirement 6: Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
 - Requirement 7: Restrict access to cardholder data by business need-to-know
 - Requirement 8: Assign a unique ID to each person with computer access
 - Requirement 9: Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
 - Requirement 10: Track and monitor all access to network resources and cardholder data
 - Requirement 11: Regularly test security systems and processes
- **Maintain an Information Security Policy**
 - Requirement 12: Maintain a policy that addresses information security

1.3. The Consequences of Non-Compliance

Those organizations who are found to compromise cardholder data must notify legal authorities. They must offer free credit-protection services to all the consumers who may have potentially been affected. Card companies may also impose fines – up to 500,000 USD per incident – on member banking institutions when data is compromised and merchants and service providers are found to be in non-compliance with PCI DSS. In extreme cases, organizations can lose the ability to process credit card transactions. All the above measures can lead to substantial business loss not to mention brand recognition issues.



2. Click&DECiDE's PCI Compliance Suite

Click&DECiDE's PCI Compliance Suite helps the PCI Compliance control team to respect key mandates of PCI DSS Version 1.2. PCI DSS mandates that an information security policy must be established, published, maintained and disseminated. This policy includes:

- A process to identify and assess threats, vulnerabilities and risks
- A formal annual review and subsequent updates when the environment changes

Click&DECiDE enables organizations processing credit card transactions to respect these mandates, to collect data, archive data and monitor, report and alert on all systems and applications that contain sensitive cardholder data. For example, Click&DECiDE manages the following security events:

- Security Events:
 - Failed system-level and application-level login attempts
 - Failed access attempts to files or application data
 - IDS/IPS events
 - Exploitation of a system by a virus, worm or an unauthorized individual (i.e., hacking)
- Configuration Changes:
 - Routers
 - Firewalls
 - Hosts
 - Applications
 - Other IT assets that are part of the credit card process
- Asset Changes:
 - Applications being installed or removed
 - Addition or removal of user and group accounts
- Service changes
 - Vulnerabilities:
 - Understanding vulnerabilities resident on an asset

3. Mapping

The following table illustrates the PCI DSS Version 1.2 requirements which Click&DECiDE addresses:

PCI DSS Section	Click&DECiDE Compliance
1. Build and Maintain a Secure Network	1.1.5, 1.1.6, 1.1.7, 1.1.8, 1.2, 1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.5, 1.3.6, 1.3.8, 1.4.1, 1.4.2
2. Do not use vendor-supplied defaults for system passwords and other security parameters	2.1, 2.2.2, 2.3
3. Protect stored cardholder data	3.6.7
4. Encrypt transmission of cardholder data across open, public networks	4.1, 4.1.1
5. Use and regularly update anti-virus software	5.1, 5.2
6. Develop and maintain secure systems and applications	6.1, 6.3, 6.3.3, 6.4, 6.5, 6.6
7. Restrict access to data by business need-to-know	7.1
8. Assign a unique ID to each person with computer access	8.1, 8.5.1
10. Track and monitor all access to network resources and cardholder data	10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.4,, 10.5.1, 10.5.2, 10.5.3, 10.5.5, 10.6, 10.7
11. Regularly test security systems and processes	11.1, 11.2, 11.4, 11.5
12. Maintain a policy that addresses information security	12.1.2, 12.8, 12.9, 12.9.5, 12.9.6



4. Conclusion

Succeed with Click&DECiDE's PCI Compliance Suite:

- Quickly identify hidden threats while meeting audit, regulatory and legal requirements with scalable and centralized log and event consolidation
- Improve system availability, service assurance and protect intellectual property with real-time intrusion detection and protection
- Identify real incidents from amongst event noise and false positive alerts to gain meaningful and real-time security information

Here are just a few of the reasons why our customers turn to us:

- Centralize logs from any device or network.
- Reduce business risk by replying in real-time to security incidents.
- Generate added-value to your investments.
- Analyse activity by user and department.
- Optimize network capacity planning management.
- Improve IT staff efficiency.
- Help you improve your corporate governance.
- Help manage your internal controls.
- Get compliant with international regulations.

To summarize, Click&DECiDE covers all your enterprise log lifecycle management needs:

- Collect and archive logs.
- Generate dynamic dashboard reports and automate their distribution to the key stakeholders.
- Manage your logs, correlate and alert.
- Enable advanced forensic analysis and data manipulation.

With Click&DECiDE your IT team now has the ability to proactively discover, detect and prevent intrusive activities and provide up-to-the minute dashboard reports for the management.

5. Going forward with Click&DECiDE

Click&DECiDE has more than 150 customers, such as Toyota, MBDA, Crédit Agricole Indosuez, Total, Expert, Société Générale. Click&DECiDE is the only Business Intelligence software fortreating all enterprise data: data from business applications as well as from your enterprise equipments (web usage, networks, security, telephony, physical access,...).

To help our customers take factual and quick decisions, Click&DECiDE brings the pertinent intelligence to your finger tips: you can then investigate ion a click, and get the details you want before taking decisions. It's easy, fast, and does not require an IT resource, nor costly PS: we dramatically increase your intelligence capacity – quality, efficiency and productivity, and lower your TCO against all competitors.

We also allow you to achieve compliance pragmatically and automate your internal data security controls (PCI DSS, Sarbanes-Oxley, HIPAA, GLBA, Basel II,...).

To find out more about Click&DECiDE's PCI DSS Compliance Suite and our security log management software solutions please visit us online at www.clickndecide.com - you can read our comprehensive product sheets, view a company movie and download an evaluation. To request an online demo please contact our Sales Team: sales@clickndecide.com.



6. Contacting Click&DECiDE

Nerys Grivolas

Senior Consultant

E-mail: nerys.grivolas@nclickndecide.com

Tel: +33 (0)6 15 32 62 42

Sales Offices:

E-mail: sales@clickndecide.com

Tel : +33 (0)6 71 99 86 60

98, route de la Reine - 92100 Boulogne-Bt, France.

To contact your nearest Click&DECiDE partner, [click here](#).