



Automating Regulatory Compliance and IT Best Practices Reporting

# Automating Compliance Reporting for PCI Data Security Standard version 1.1

The PCI Data Security Standard version 1.1 was released in September 2006 by the PCI Security Standards Council and consists of 12 requirements spread among 6 major control objectives for Merchants and Service Providers.

Ecora Auditor Professional is the only automated solution providing pre-installed, audit-ready report templates that validate 10 of the 12 PCI DSS requirements.

### Control Objective: Build and Maintain a Secure Network

For Requirement 1, Install and maintain a firewall configuration to protect data, Ecora Auditor Professional captures the information and generates the reports to validate:

- Firewall configuration standards and other required documentation are complete
  - The process for changing firewall configurations
  - Firewall configuration standards include a description of groups, roles, & responsibilities for logical management of network components
  - Firewall configuration standards include a documented list of services/ports necessary for business
  - Each service in use is necessary and secured
- Connections are restricted between publicly accessible servers and components storing cardholder data
  - Inbound Internet traffic is limited to IP addresses within the DMZ
  - Internal addresses cannot pass from the Internet into the DMZ

For Requirement 2, do not use vendor-supplied defaults for system passwords and other security parameters, Ecora Auditor Professional captures the information and generates the reports to validate:

- Vendor-supplied defaults are changed before installing a system on the network
- Configuration standards for network components, critical servers, and wireless access points are consistent with industry-accepted hardening standards, as defined, for example, by SANS, NIST, and CIS.
  - System configurations are applied when new systems are configured
  - Unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service
  - Common security parameter settings are included in the system configuration standards for system components, critical servers, and wireless access points.
  - All unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed from system components, critical servers, and wireless access points.
- Non-console administrative access is encrypted for system components, critical servers, and wireless access points.
- Shared Hosting Providers protect their entities' (merchants and service providers) hosted environment and data.

**Table 1. Domain Admins Group**

Domain	User Name	User Full Name	User Account Expires	User Lockout	User Disable
SampleOrgDOMAIN	Administrator		No	No	
SampleOrgDOMAIN	ecm_2	ecm_2	No	No	
SampleOrgDOMAIN	PMPUser	PMPUser	No	No	
TESTSRV4DOMAIN	a1		No	No	
TESTSRV4DOMAIN	Administrator		No	No	
TESTSRV4DOMAIN	as	1	No	No	
TESTSRV4DOMAIN	cm_admin3	cm_admin3	No	No	
TESTSRV4DOMAIN	ecm_2458000	ecm_2	No	No	
TESTSRV4DOMAIN	ecm_3	ecm_3	No	No	
TESTSRV4DOMAIN	ecora	ecora	No	No	
TESTSRV4DOMAIN	gobbo	Gobbo	No	Yes	
TESTSRV4DOMAIN	king for a day	King for a day	No	Yes	
TESTSRV4DOMAIN	tester	For Testing	No	No	
DOMAIN-A	Administrator	Administrator	No	No	
DOMAIN-A	ecora	ecora	No	No	
DOMAIN-A	User_A1_B1	User_A1_B1	No	No	
DOMAIN-B	Administrator		No	No	
DOMAIN-B	ecora	ecora	No	No	
DOMAIN-B	User_B1_A1	User_B1_A1	No	No	
DOMAIN-C	Administrator		No	No	
DOMAIN-C	ecora	ecora	No	No	
ECORA	Administrator		No	No	
ECORA	ecora	ecora	No	No	
TESTSRV4DOMAIN	db2admin	db2admin	No	No	
TESTSRV4DOMAIN	ecm_4	ecm_4	No	No	
TESTSRV4DOMAIN	ecora	ecora	No	No	
TESTSRV4DOMAIN	ecorapvm	ecorapvm	No	No	
TESTSRV4DOMAIN	PMPUser	PMPUser	No	No	
MORDOR_NBI	Administrator		No	No	
MORDOR_NBI	ecora	ecora	No	No	

Ecora's Domain Admins Group Report fulfills PCI DSS 1.1.4, "Verify that firewall configuration standards include a description of groups, roles, and responsibilities for logical management of network components."



Ecora's Baseline Comparison Report fulfills PCI DSS 2.2.c, "Verify that system configuration standards are applied when new systems are configured."

### Control Objective: Protect Cardholder Data

For Requirement 3, protect stored data, Ecora Auditor Professional captures the information and generates the reports to validate:

- Full content on any track from the magnetic strip on the back of the card are not stored in system components, critical servers, and wireless access points under any circumstances.
- Cryptographic keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys

For Requirement 4, Encrypt transmission of cardholder data and sensitive information across public networks, Ecora Auditor Professional captures the information and generates reports to validate:

- Encryption (for example, SSL/TLS or IPSEC) is used wherever cardholder data is transmitted or received over open, public networks.
- Appropriate encryption methodologies are used for any wireless transmissions, such as: Wi-Fi Protected Access (WPA or WPA2), IPSEC VPN, or SSL/TLS.

• [Hpux - Checksum Files](#)  
 • [Solaris - Checksum Files](#)  
 • [Linux - Checksum Files](#)

[ File integrity report of Checksum (binary) files ]

**Table 1. Hpux - Checksum Files**

Computer Name	Filename	Checksum
hud0	/usr/bin/crontab	1740014336
hud1	/usr/bin/crontab	4047284871

**Table 2. Solaris - Checksum Files**

Computer Name	Filename	Checksum
sud12	/usr/bin/crontab	91323c85d073bdfc35a0a9be8ea87205
sud48	/usr/bin/crontab	89c34c399ada5e435f6eea7efc70c03d

**Table 3. Linux - Checksum Files**

Computer Name	Filename	Checksum
vmLinux-9	/usr/bin/crontab	503850519
vm-server	/usr/bin/crontab	2211403144

Ecora's Checksum Report fulfills PCI DSS 3.5.2, "Examine system configuration files to verify that cryptographic keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys."

### Control Objective: Maintain a Vulnerability Management Program

For Requirement 5, use and regularly update anti-virus software, Ecora Auditor Professional captures the information and generates the reports to validate:

- Anti-virus software is installed on system components, critical servers, and wireless access points
- Anti-virus software is current, actively running, and capable of generating logs

For Requirement 6, develop and maintain secure systems and applications, Ecora Auditor Professional captures the information and generates the reports to validate:

- Current vendor patches are installed on all system components, critical servers, and wireless access points
- All relevant new security patches are installed within 30 days
- Processes to identify new security vulnerabilities include use of outside sources for security vulnerability information and updating the system configuration standards as new vulnerability issues are found
- Custom application accounts, usernames and/or passwords are removed before system goes into production or is released to customers
- Changes/security patches for each system component, critical server, and wireless access point was change and documented according to the change control procedures
- Processes are in place to confirm that web applications are not vulnerable to insecure configuration management

### Computers Without Antivirus Software Installed

Prepared For: Mr. John Customer (Customer@ecora.com)  
 Prepared On: 10/24/2008 2:07:42 PM  
 Prepared By: Ecora Auditor Professional 4.0 - Windows Module  
 Prepared Using: FFR Definition (Computers without antivirus software installed)  
 Prepared Time Criteria: Last 30 week(s)

Copyright © 2008 your organization. All rights reserved.

PCI section 5.2 This report includes the computer name of systems that do not have an antivirus application installed. If all systems have an antivirus application installed, then it will state "No relevant data found".

**Table 1. Computers Without Antivirus Software Installed**

Domain Computer
COMPLIANCE-ORIG@ECORA-DC.COMPLIANCE.ORG
COMPLIANCE-AUDIT@ORDEMO
COMPLIANCE@ECORA-DC
COMPLIANCE@SHURE@CNT
TEST.LOCAL@CLUSTER1

Ecora's Computers Without Antivirus Software Installed Report fulfills PCI DSS 5.1, "For a sample of system components, critical servers, and wireless access points, verify that anti-virus software is

**ecora** Missing Patches Summary

ECORAQA@ALBANY IP Address: Operating System: Windows 2003 Advanced Server  
 Missing Internet Information Services 5.0 Patches - 100% - 0 out of 2 patches installed  
 Missing MDAC 2.8 Patches - 100% - 0 out of 1 patches installed  
 Missing Windows 2000 Advanced Server Patches - 65% - 5 out of 34 patches installed  
 Missing Windows Media Player 6.4 for Windows 2003 Patches - 80% - 1 out of 5 patches installed

ECORAQA@BOSTON IP Address: Operating System: Windows 2003 Advanced Server  
 Missing MDAC 2.6 Patches - 100% - 0 out of 1 patches installed  
 Missing SQL Server 2000 Patches - 100% - 0 out of 6 patches installed  
 Missing Windows 2000 Advanced Server Patches - 66% - 2 out of 6 patches installed  
 Missing Windows Media Player 6.4 for Windows 2003 Patches - 100% - 0 out of 5 patches installed

ECORAQA@DENVER IP Address: Operating System: Windows XP Professional  
 Missing Internet Explorer 6 Patches - 100% - 0 out of 15 patches installed  
 Missing MDAC 2.7 Patches - 100% - 0 out of 3 patches installed  
 Missing Windows Media Player for Windows XP Patches - 100% - 0 out of 3 patches installed  
 Missing Windows XP Professional Patches - 96% - 5 out of 30 patches installed

ECORAQA@NEWYORK IP Address: Operating System: Windows 2003 Advanced Server  
 Missing MDAC 2.5 Patches - 100% - 0 out of 1 patches installed  
 Missing SQL Server 7.0 Patches - 100% - 0 out of 4 patches installed  
 Missing Windows 2000 Advanced Server Patches - 64% - 2 out of 6 patches installed  
 Missing Windows Media Player 6.4 for Windows 2003 Patches - 100% - 0 out of 5 patches installed

Ecora's Missing Patches Summary Report fulfills PCI DSS 6.1.a, "For a sample of system components, critical servers, and wireless access points and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed."

## Control Objective: Implement Strong Access Control Measures

For Requirement 7, restrict access to data by business need-to-know, Ecora Auditor Professional captures the information and generates the reports to validate:

- Policy for data control is followed and incorporates the following:
  - Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities
  - Assignment of privileges is based on individual personnel's job classification and function
  - Requirement for an authorization form signed by management that specifies required privileges
  - Implementation of an automated access control system
- An access control system is implemented and includes the following:
  - Coverage of all system components
  - Assignment of privileges to individuals based on job classification and function
  - Default "deny-all" setting

For Requirement 8, assign a unique ID to each person with computer access, Ecora Auditor Professional captures the information and generates the reports to validate:

- All users have a unique username for access to system components or cardholder data
- Users are authenticated using unique ID and additional authentication for access to the cardholder environment
- Two-factor authentication is implemented for all remote network access
- Procedures are implemented for user authentication and password management
  - Each user is authorized to use the system according to company policy
  - IDs for employees terminated in the past six months have been inactivated or removed
  - No inactive accounts over 90 days old
  - Any accounts used by vendors to support and maintain system components are inactive, enabled only when needed by the vendor, and monitored while being used
  - User ID lists from system components, critical servers, and wireless access points reflect the following:
    - Generic User IDs and accounts are disabled or removed
    - Shared User IDs for system administration activities and other critical functions do not exist
    - Shared and generic User IDs are not used to administer wireless LANs and devices

## Sites with Anonymous Access

Prepared For: Mr. John Customer (customer@ecora.com)  
 Prepared On: 10/26/2026 2:30:26 PM  
 Prepared By: Ecora Auditor Professional 4.0 - MS-DI-Abdullah  
 Prepared Using: FPG-Definion Sites with Anonymous Access  
 Prepared Time Criteria: LAST 20 week(s)  
 Copyright © 2026 your organization  
 All rights reserved.

Requirement 7 - Section 7.1 - Description for Sites with Anonymous Access

Name	Anonymous Username	Anonymous Access
auditorsdemo	USER_AUDITOR	Enabled
ecora-DC	USER_ECORA-DC	Enabled

Ecora's Sites with Anonymous Access Report fulfills PCI DSS 7.1, "Obtain and examine written policy for data control, and verify that the policy incorporates the following: Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities, assignment of privileges is based on individual personnel's job classification and function, and implementation of an automated access control system."

PCI section 8.2 and 8.5 This report contains four tables (1. Domain Password Policies, (2. Local Computer Password Policies, (3. Domain Account Lockout Policies, and (4. Local Computer Account Lockout Policies). Review these policies and set according to corporate guidelines. Adhere to Microsoft, IANS or other security best practice guidelines if in doubt.

Domain Name	Min Password Length	Max Password Age	Min Password Age (Days)	Password History (Uniqueness)
COMPLIANCE.ORG	8	42 days	2	24

  

Domain Computer	Min Password Length	Max Password Age	Min Password Age (Days)	Password History (Uniqueness)
COMPLIANCE.ORG/ECORA-DC.COMPLIANCE.ORG	8	42days	2	24
COMPLIANCE/AUDITORDemo	1	42days	2	24
COMPLIANCE/ECORA-DC	8	42days	2	24
COMPLIANCE/SHAREPOINT	7	42days	2	24
TEST.LOCAL/CLUSTER1				

  

Domain Name	Account Lockout Enabled	Account Lockout Threshold	Account Lockout Duration (Minutes)	Account Lockout Window (Minutes)	Force Logoff
COMPLIANCE.ORG	Yes	50	30	30	No

  

Domain Computer	Account Lockout Enabled	Account Lockout Threshold	Account Lockout Window (Minutes)	Account Lockout Duration (Minutes)	Force Logoff
COMPLIANCE.ORG/ECORA-DC.COMPLIANCE.ORG	Yes	50	30	30	Forced off immediately
COMPLIANCE/AUDITORDemo	Yes	50	30	30	Forced off immediately
COMPLIANCE/ECORA-DC	Yes	50	30	30	Forced off immediately
COMPLIANCE/SHAREPOINT	Yes	50	30	30	Forced off immediately
TEST.LOCAL/CLUSTER1	No				

Ecora's Password and Account Lockout Report fulfills PCI DSS 8.5.15, "For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that system/session idle time out features have been set to 15 minutes or less."

- User password parameters are set to require users to change passwords at least every 90 days
- Password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts
- Password parameters are set to require that system/session idle time out features have been set to 15 minutes or less
- Access to databases is authenticated, including for individual users, applications, and administrators
- Direct SQL queries to the database are prohibited

Ecora's compliance reporting solution does not apply to **Requirement 9**, Restrict physical access to cardholder data, Ecora Auditor Professional captures the information and generates the reports to validate:

### Control Objective: Regularly Monitor and Test Networks

For **Requirement 10**, track and monitor all access to network resources and cardholder data, Ecora Auditor Professional captures the information and generates the reports to validate:

- Audit trails are enabled and active, including for any connected wireless networks
- Required events are included into system activity logs
- Each auditable event includes: user identification, type of event, date and time, success or failure indication, including those for wireless connections, origination of event, and name of affected data, system component, or resources
- Audit trails are secured with appropriate permissions
- Security logs are reviewed at least daily and that follow-up to exceptions is required
- Audit logs are retained for at least one year

Ecora's compliance reporting solution does not apply to **Requirement 11**, regularly test security systems and processes.

**ecora**  
**Security Events**

Prepared For: Chris Cole <ccole@ecora.com>  
Prepared On: Tuesday, November 24, 2009 8:18:19 AM  
Prepared By: Ecora Auditor Professional 4.1 - Windows Module  
Prepared Using: FPE (Default) Security Events  
Prepared Time Criteria: Last 20 week(s)  
Copyright © 2008 Ecora Software  
All rights reserved.

• All Security Events

The report shows ALL security events from all computers that were collected in reverse chronological order. It can be used to track security events in a given time range across all computers. All computers imply that WMI event log collection was selected and the data was collected.

**Table 1. All Security Events**

ComputerName	Logfile	TimeGenerated	TimeWritten	EventCode	Message
AUDITRDEND	Security	2009-11-14 09:08:20-09:00	2009-11-14 09:08:20-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:29-09:00	2009-11-14 09:08:29-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:21-09:00	2009-11-14 09:08:21-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:28-09:00	2009-11-14 09:08:28-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:19-09:00	2009-11-14 09:08:19-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:18-09:00	2009-11-14 09:08:18-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:17-09:00	2009-11-14 09:08:17-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:15-09:00	2009-11-14 09:08:15-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:14-09:00	2009-11-14 09:08:14-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:13-09:00	2009-11-14 09:08:13-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:11-09:00	2009-11-14 09:08:11-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0
AUDITRDEND	Security	2009-11-14 09:08:10-09:00	2009-11-14 09:08:10-09:00	4802	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1.0 Logon account: Administrator Source Workstation: AUDITOR Error Code: 0x0

Ecora's Password and Account Lockout Report fulfills PCI DSS 8.5.15, "For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that system/session idle time out features have been set to 15 minutes or less."

## Control Objective, Maintain an Information Security Policy

For Requirement 12, maintain a policy that addresses information security, Ecora Auditor Professional captures the information and generates the reports to validate:

- Daily operational security procedures are consistent with PCI DSS specifications, and include administrative and technical procedures for each of the requirements



Ecora's Password and Account Lockout Report fulfills PCI DSS 8.5.15, "For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that system/session idle time out features have been set to 15 minutes or less."

### Find Out More

To learn more about how Ecora can help you achieve and maintain PCI compliance, call **877.923.2672**, email [sales@ecora.com](mailto:sales@ecora.com), or visit us on the web at [www.ecora.com](http://www.ecora.com).

### About Ecora

Proven in nearly 4,000 worldwide customer sites, Ecora's leading enterprise-wide audit and compliance management solutions are designed to reduce the time and costs associated with managing IT configuration controls, for enhanced infrastructure security. Ecora provides automated, centralized solutions to collect, analyze, and report on the most in-depth, multi-platform configuration information across enterprise operating systems, applications, databases, and networking devices. Ecora works to optimize IT environments and delivers an immediate return on investment. For more information about Ecora, visit [www.ecora.com](http://www.ecora.com).