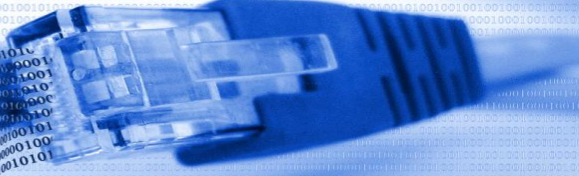


**A&O IT Solutions LLC**



**609-859-8071**

**PCI  
Assessment**

# PCI Management Plan



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for:  
Prospect or Customer  
Prepared by:  
A&O IT Solutions LLC

## Management Plan







The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the global Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

### High Risk



Risk Score	Recommendation	Severity	Probability
100	<p><b>PCI DSS Requirement 3.2 - Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.</b></p> <p>Identify and remove the source resulting in storage of Primary Account Numbers (PAN) in the file system.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Corp.MyCorp.com\PITMARC-PC: C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SmbShare\en-US\SmbOpenFile.cdxml-help.xml</li> <li><input type="checkbox"/> Corp.MyCorp.com\PITMARC-PC: E:\ECOMM Documents Folder\Rapid Fire Tools\SAM and NAM Sample Reports\Network\Full Detail Report.docx</li> </ul>	H	H
95	<p><b>PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).</b></p> <p>Enable antispyware on all computers commonly affected by malicious software.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> HYPER04 / 192.168.1.104 / Windows Server 2012 R2 Datacenter</li> <li><input type="checkbox"/> CORY-WIN7 / 192.168.6.44 / Windows 7 Enterprise</li> <li><input type="checkbox"/> HYPER01 / 192.168.1.111 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> UTIL-1 / 192.168.1.15 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> OPSTFS / 192.168.1.16 / Windows Server 2012 Standard</li> <li><input type="checkbox"/> HYPER02 / 192.168.1.121 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> TSUMMER-WIN764 / 192.168.7.18 / Windows 8.1 Enterprise</li> <li><input type="checkbox"/> RD-GATE / 192.168.1.21 / Windows Server 2012 R2 Datacenter</li> <li><input type="checkbox"/> TS01 / 192.168.6.80 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> TSUMMER-PC / 192.168.6.40 / Windows 8.1 Pro</li> <li><input type="checkbox"/> FS-2012 / 192.168.1.41 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> HYPER00 / 192.168.1.100 / Windows Server 2012 R2 Datacenter</li> <li><input type="checkbox"/> VPNGW / 192.168.1.5 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> OPSTFSBUILD / 192.168.6.67 / Windows Server 2012 R2 Standard</li> </ul>	H	H
95	<p><b>PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly</b></p>	H	H

Risk Score	Recommendation	Severity	Probability
	<p><b>personal computers and servers).</b>            Enable antivirus on all computers commonly affected by malicious software.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> TSUMMER-WIN7TEST / 192.168.6.53 / Windows 7 Professional</li> <li><input type="checkbox"/> HYPER04 / 192.168.1.104 / Windows Server 2012 R2 Datacenter</li> <li><input type="checkbox"/> CORY-WIN7 / 192.168.6.44 / Windows 7 Enterprise</li> <li><input type="checkbox"/> HYPER01 / 192.168.1.111 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> UTIL-1 / 192.168.1.15 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> OPSTFS / 192.168.1.16 / Windows Server 2012 Standard</li> <li><input type="checkbox"/> HYPER02 / 192.168.1.121 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> TSUMMER-WIN764 / 192.168.7.18 / Windows 8.1 Enterprise</li> <li><input type="checkbox"/> RD-GATE / 192.168.1.21 / Windows Server 2012 R2 Datacenter</li> <li><input type="checkbox"/> TS01 / 192.168.6.80 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> TSUMMER-PC / 192.168.6.40 / Windows 8.1 Pro</li> <li><input type="checkbox"/> FS-2012 / 192.168.1.41 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> HYPER00 / 192.168.1.100 / Windows Server 2012 R2 Datacenter</li> <li><input type="checkbox"/> CONFERENCEROOM / 192.168.6.33 / Windows 7 Professional</li> <li><input type="checkbox"/> VPNGW / 192.168.1.5 / Windows Server 2012 R2 Standard</li> <li><input type="checkbox"/> OPSTFSBUILD / 192.168.6.67 / Windows Server 2012 R2 Standard</li> </ul>		
94	<p><b>PCI DSS Requirement 1.1.6 - Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.</b>            Close or unpublish external facing ports using inherently insecure protocols or provide additional security features and documentation.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> 42.26.150.2 : 80/tcp (http)</li> </ul>	<b>H</b>	<b>H</b>
92	<p><b>PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).</b>            Update antispyware definitions to ensure protection against the latest threats.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> WS-1 / 192.168.6.97 / Windows 8 Enterprise</li> </ul>	<b>H</b>	<b>H</b>
92	<p><b>PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).</b>            Update antivirus definitions to ensure protection against the latest threats.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> WS-1 / 192.168.6.97 / Windows 8 Enterprise</li> <li><input type="checkbox"/> CONFERENCEROOM / 192.168.6.33 / Windows 7 Professional</li> </ul>	<b>H</b>	<b>H</b>
92	<p><b>PCI DSS Requirement 2.3.b - Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.</b></p>	<b>H</b>	<b>H</b>

Risk Score	Recommendation	Severity	Probability
	Block or disable access to Telnet and other insecure remote-login commands for non-console access. <ul style="list-style-type: none"> <li><input type="checkbox"/> HTTP (80/TCP) on HHOLT-DT (192.168.7.45) / 80</li> <li><input type="checkbox"/> HTTP (80/TCP) on OPS-1 (192.168.7.65) / 80</li> <li><input type="checkbox"/> HTTP (8080/TCP) on OPS-1 (192.168.7.65) / 8080</li> <li><input type="checkbox"/> HTTP (80/TCP) on WS-2 (192.168.7.89) / 80</li> </ul>		
89	<b>PCI DSS Requirement 10.2.2 - All actions taken by any individual with root or administrative privileges.</b> Enable auditing of all actions taken by any individual with root or administrative privileges.	H	M
87	<b>PCI DSS Requirement 1.3.5 - Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.</b> Block web traffic to all sites not required by the CDE. <ul style="list-style-type: none"> <li><input type="checkbox"/> http://espn.go.com</li> <li><input type="checkbox"/> http://gmail.google.com</li> <li><input type="checkbox"/> http://isohunt.to</li> <li><input type="checkbox"/> http://mail.yahoo.com</li> <li><input type="checkbox"/> http://thepiratebay.se</li> <li><input type="checkbox"/> http://www.cnet.com</li> <li><input type="checkbox"/> http://www.facebook.com</li> <li><input type="checkbox"/> http://www.myspace.com</li> <li><input type="checkbox"/> http://www.playboy.com</li> <li><input type="checkbox"/> http://www.tucows.com</li> <li><input type="checkbox"/> http://www.youporn.com</li> <li><input type="checkbox"/> http://www.youtube.com</li> <li><input type="checkbox"/> https://plus.google.com</li> <li><input type="checkbox"/></li> </ul>	H	H
83	<b>PCI DSS Requirement 8.2.3 - Passwords/phrases must meet the following: * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.</b> Enforce password complexity of at least 7 characters and contain both numeric and alphabetic characters.	M	H
81	<b>PCI DSS Requirement 8.2.5 - Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.</b> Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	M	H
77	<b>PCI DSS Requirement 8.1.6 - Limit repeated access attempts by locking out the user ID after not more than six attempts.</b> Ensure password lockout is enforced after more than six attempts.	M	H
77	<b>PCI DSS Requirement 2.2.3 - Implement additional security features</b>	M	H

Risk Score	Recommendation	Severity	Probability
	<p>for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.</p> <p>Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> HHOLT-DT.CORP.PERFORMANCEIT.COM / 80</li> <li><input type="checkbox"/> OPS-1.CORP.PERFORMANCEIT.COM / 80</li> <li><input type="checkbox"/> OPS-1.CORP.PERFORMANCEIT.COM / 8080</li> <li><input type="checkbox"/> WS-2.CORP.PERFORMANCEIT.COM / 80</li> </ul>		
75	<p><b>PCI DSS Requirement 6.2 - Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.</b></p> <p>Address patching on computers with missing security patches.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> DC-3 / 192.168.1.23, 192.168.1.4, 192.168.1.3</li> <li><input type="checkbox"/> JACK-WIN8 / 192.168.7.44</li> </ul>		
74	<p><b>PCI DSS Requirement 8.1.7 - Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.</b></p> <p>Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.</p>		
72	<p><b>PCI DSS Requirement 8.1.3 - Immediately revoke access for any terminated users.</b></p> <p>Disable or remove accounts for former employees and vendors.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> mwest / Mary West</li> <li><input type="checkbox"/> cweston / Candy Weston</li> </ul>		

## Medium Risk

Risk Score	Recommendation	Severity	Probability
70	<p><b>PCI DSS Requirement 8.1.1 - Assign all users a unique ID before allowing them to access system components or cardholder data.</b></p> <p>Investigate and either disable or note compensating controls to ensure these potential generic accounts are not used inappropriately. Service accounts are excluded.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Corp.MyCorp.com\admin</li> <li><input type="checkbox"/> Corp.MyCorp.com\Administrator</li> <li><input type="checkbox"/> Corp.MyCorp.com\sales</li> <li><input type="checkbox"/> Corp.MyCorp.com\support</li> <li><input type="checkbox"/> Corp.MyCorp.com\DDRTTest</li> <li><input type="checkbox"/> Corp.MyCorp.com\SUPPORT\$</li> </ul>		



Risk Score	Recommendation	Severity	Probability
	<input type="checkbox"/> Corp.MyCorp.com\supportguy <input type="checkbox"/> Corp.MyCorp.com\nonadminuser <input type="checkbox"/> Corp.MyCorp.com\marty-test <input type="checkbox"/> Corp.MyCorp.com\Tester		
69	<b>PCI DSS Requirement 10.2.5 - Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.</b> Enable auditing of changes to account identification and authentication mechanisms.	M	M
67	<b>PCI DSS Requirement 8.1.5 - Manage IDs used by vendors to access, support, or maintain system components via remote access</b> Disable vendor accounts when not in use. <ul style="list-style-type: none"> <li><input type="checkbox"/> dperry / David Perry</li> </ul>	M	M
62	<b>PCI DSS Requirement 8.1.3 - Immediately revoke access for any terminated users.</b> Investigate and determine if the users are former employees or vendors. <ul style="list-style-type: none"> <li><input type="checkbox"/> admin / admin admin</li> <li><input type="checkbox"/> adminonly / admin only</li> <li><input type="checkbox"/> jcosmore / Jsff Cosmore</li> <li><input type="checkbox"/> tmorret / t morret</li> <li><input type="checkbox"/> mwest / Mary West</li> <li><input type="checkbox"/> mwilder / Mike Wilder</li> <li><input type="checkbox"/> hr / MyCorp HR</li> <li><input type="checkbox"/> partners / MyCorp Managed Services Partners</li> <li><input type="checkbox"/> info / MyCorp PR</li> <li><input type="checkbox"/> sraki / Steve Rakie.</li> <li><input type="checkbox"/> cweston / Candy Weston</li> <li><input type="checkbox"/> slouder / Sarah Louder</li> </ul>	M	L
62	<b>PCI DSS Requirement 8.1.5 - Manage IDs used by vendors to access, support, or maintain system components via remote access</b> Disable or remove accounts for former employees and vendors.	M	L
60	<b>PCI DSS Requirement 1.1.4.b - Verify that the current network diagram is consistent with the firewall configuration standards.</b> Updated the network diagram to be consistent with the requirement to deploy a firewall at each Internet connection or note in the CCW any exceptions.	M	M

 Low Risk

Risk Score	Recommendation	Severity	Probability
50	<b>PCI DSS Requirement 6.5 - Address common coding vulnerabilities in software-development processes</b> Establish a program to train developers on secure coding guidelines to protect applications.		