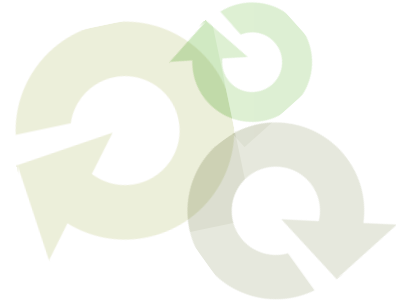


 **Solution Brief:**



**Shavlik Security Suite  
for PCI DSS**



## Solution Brief:

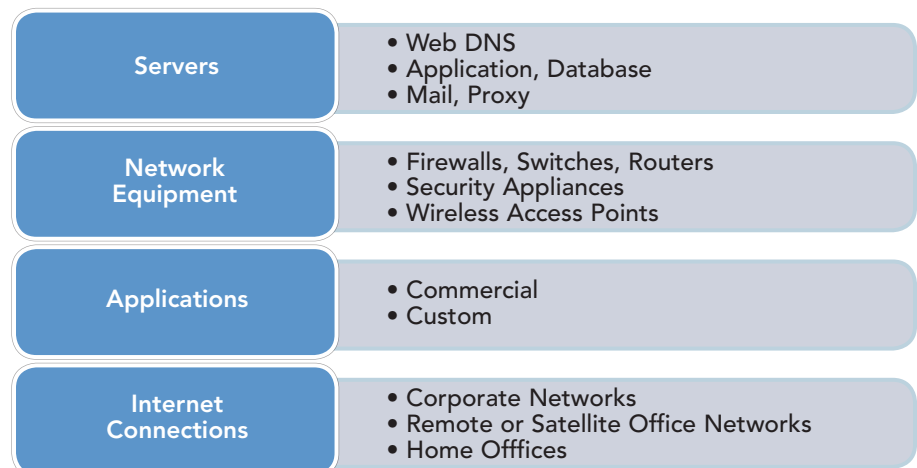
### Shavlik Security Suite for PCI DSS

## Introduction to PCI DSS

**What is it?** The Payment Card Industry Data Security Standard (PCI DSS) was developed to maintain a high level of trust in the payment card system. The PCI DSS is enforced by the PCI Security Standards Council through the oversight of major credit card providers.

**Who and What is Subject to PCI DSS compliance?** All merchants and credit card processors worldwide that store, process or transmit cardholder data are required to comply with the PCI standards. More technically, PCI standards apply to “all system components” that are part of the network that possesses cardholder data or sensitive authentication data. These components are described in the diagram below.

## What Network Components are Subject to PCI DSS?



*This document is provided strictly as a guide. No guarantees can be provided or expected.*

 **Solution Brief:****Shavlik Security Suite for PCI DSS****Overview of PCI DSS Requirements**

PCI DSS comprises a comprehensive set of security measures to be undertaken by merchants and transaction processors that collectively prevent, detect and respond to threats involving the disclosure of sensitive cardholder data. The standards require merchants and card processors to:

1. Build and maintain a secure network;
2. Protect cardholder data;
3. Ensure the maintenance of vulnerability management programs;
4. Implement strong access control measures;
5. Regularly monitor and test networks; and
6. Ensure the maintenance of information security policies.

**PCI Compliance and Certification**

The PCI standards are enforced by a combination of audits, remote scans and self assessments. All system participants must have their Internet-facing IP addresses scanned for vulnerabilities each quarter by an Approved Scan Vendor (ASV).

In addition to the quarterly scans, high volume participants must annually subject their networks to an on-site audit conducted by a Qualified Security Assessor (QSA). Instead of an on-site audit, low-volume participants must complete and submit a self-assessment questionnaire.

All banks are required to have received certified proof of PCI compliance from merchants that generate more than 20,000 transactions per year. Many banks are already requiring all merchants, regardless of transaction volume, to produce a certification of PCI compliance.

PCI compliance is not a single, point-in-time project. Businesses change. Networks change. Systems change. Mandates change. To achieve and sustain PCI compliance, organizations must adopt a holistic view that includes an easy-to-use, cost-effective approach to identify and remediate weaknesses or deficiencies and periodically generate reports that demonstrate compliance in this ever-changing environment.

*This document is  
provided strictly as a guide.  
No guarantees can be  
provided or expected.*



## Solution Brief:

### Shavlik Security Suite for PCI DSS

The following table explains how PCI participants are divided into four levels based on annual transaction volumes, and the compliance requirements associated with each level.

<b>Level 1:</b> More than 6 million transactions annually	<ul style="list-style-type: none"> <li>• Annual onsite audit by a QSA</li> <li>• Quarterly network security scan</li> </ul>
<b>Level 2:</b> 1 million to 6 million transactions annually	<ul style="list-style-type: none"> <li>• Annual self assessment questionnaire</li> <li>• Quarterly network security scan</li> </ul>
<b>Level 3:</b> 20,000 to 1 million transactions annually	<ul style="list-style-type: none"> <li>• Annual self assessment questionnaire</li> <li>• Quarterly network security scan</li> </ul>
<b>Level 4:</b> Up to 20,000 transactions annually	<ul style="list-style-type: none"> <li>• Annual self assessment questionnaire</li> <li>• Quarterly network security scan</li> </ul>

### PCI Enforcement and Penalties

There are three types of penalties that can be levied as the result of non-compliance:

- ▶ **Financial:** depending on the severity of the breach and the degree of malfeasance, penalties can range from \$10K - \$100K/month
- ▶ **Processing privileges:** loss of ability to process card transactions
- ▶ **Oversight:** escalated auditing and validation requirements

Beyond official sanctions, organizations subject to PCI standards face the risk of litigation from damaged parties as a result of failure to meet the standards.

### Vulnerability Management and PCI Compliance

Because PCI DSS was developed to secure data at rest in complex networks and in transit between many entities, full compliance will necessarily require a broad spectrum of security technologies including physical access controls, identity management, user authentication, encryption, and vulnerability management. Vulnerability management is essential because it creates a stable platform to support all the other security tools and processes. This paper focuses on PCI standards relating to vulnerability management.

*This document is provided strictly as a guide. No guarantees can be provided or expected.*

## Solution Brief:

### Shavlik Security Suite for PCI DSS

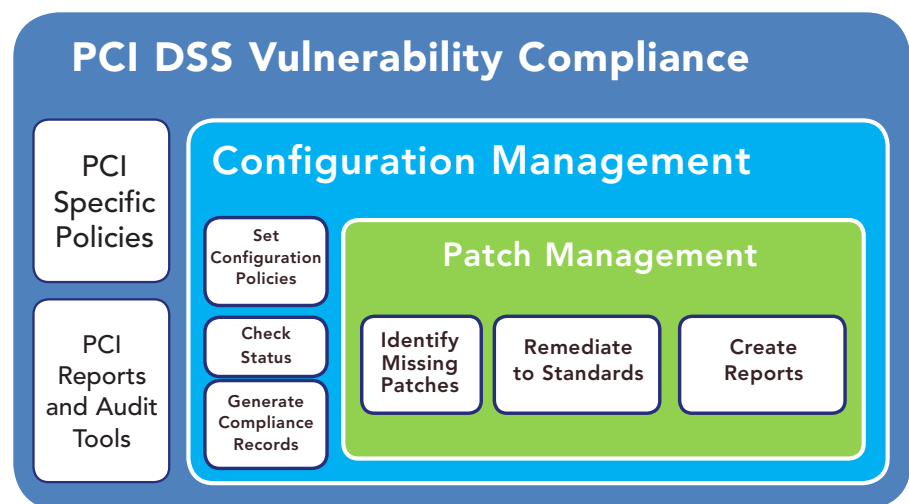
Vulnerability management systems identify and fix potential security problems on servers and PCs, and then maintain the machines at a “gold standard” state. Vulnerability management encompasses two processes: patch and configuration management. Patch management ensures that the device operating system and commercial application software are at the current release with all security patches applied. Configuration managers check that the operating system has been properly configured for the required level of security.

Both patch and configuration management systems generate reports that alert administrators and auditors if systems have drifted away from compliance with stated policies. The PCI DSS standard is just one of any number of regulatory requirements relating to vulnerability management that might apply to a given organization.

The following diagram illustrates that patch and configuration management are critical components of any PCI DSS compliance program. Nevertheless, generic patch and configuration management systems by themselves do not guarantee or provide proof of compliance with PCI vulnerability standards. Organizations subject to PCI will need PCI-specific report and audit modules to “translate” patch and configuration updates into useful compliance documents.

*This document is provided strictly as a guide. No guarantees can be provided or expected.*

### PCI Vulnerability Management and PCI Compliance





## Solution Brief:

### Shavlik Security Suite for PCI DSS

## Shavlik Security Suite Ensures PCI compliance....Simply!

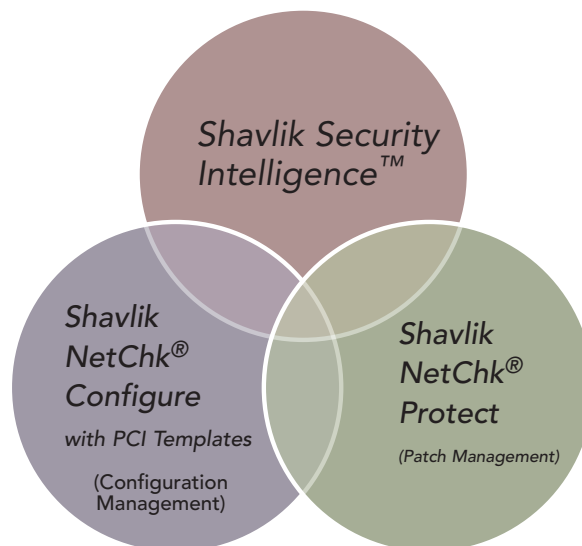
**Shavlik Security Suite** is a full-featured PCI vulnerability compliance management system that combines sophistication with simplicity. Comprised of three carefully integrated products - Shavlik Security Intelligence, Shavlik NetChk Protect and Shavlik Netchk Configure - the Shavlik Security Suite automates all aspects of PCI vulnerability compliance.

**Shavlik NetChk Protect**, an award-winning leader in patch management, perfectly complements Shavlik Netchk Configure, a powerful tool for security configuration management and audit ready reports. Both of these products interoperate with Shavlik Security Intelligence, a next generation analytics product that measures risk and policy compliance across the enterprise, displaying the results in a customizable web-based dashboard. With the addition of Shavlik's PCI DSS templates, the Shavlik Security Suite provides the most direct, best value solution for PCI vulnerability compliance.

## The Shavlik Security Suite Capabilities

Easy and swift to implement, Shavlik Security Suite does not require special expertise and is designed to deliver customized reports that demonstrate compliance with PCI requirements and satisfy the most stringent auditor.

*This document is provided strictly as a guide. No guarantees can be provided or expected.*




**Solution Brief:**

### Shavlik Security Suite for PCI DSS

Shavlik Security Suite will enable organizations of any size to breeze through quarterly ASV scans and to prove PCI compliance when undergoing annual QSA audits. The benefits flowing to organizations from a “best of breed” compliance program such as Shavlik Security Suite were documented in a 2007 survey done by the Aberdeen Group<sup>1</sup> that showed:

- ▶ 56% decreased the number of security-related incidents in the last 12 months
- ▶ 58% decreased the number of false positives
- ▶ 53% decreased the number of non-compliance incidents
- ▶ 28% decreased the time required to complete an audit
- ▶ 86% increased the number of systems requiring updates, patches, and configuration changes actively being managed
- ▶ 77% increased the number of systems generating logs actively being managed

### Shavlik Security Suite Ensures PCI DSS Compliance

	PCI DSS Control Requirement	Shavlik Security Suite Functionality	Sub-Sections Directly Impacted
1.	Install and maintain firewall configurations to protect cardholder data	Shavlik Netchk Configure verifies built-in Windows firewall utilization on targeted systems. Custom checks can be used to monitor firewall configuration settings that are written to the Windows registry.	
2.	Do not utilize default vendor user names, passwords, and system configurations	1) Use Netchk Configure to develop and enforce a security baseline to ensure systems containing cardholder data are properly hardened. 2) Use Netchk Configure to audit and enforce existing password policies. 3) Use Netchk Configure to identify and manage all systems running on those systems that contain cardholder information.	2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function  2.2.3 Configure system security parameters to prevent misuse  2.2.4 Remove all unnecessary functionality such as, scripts, drivers, features, subsystems, file systems, and unnecessary web servers

*This document is provided strictly as a guide. No guarantees can be provided or expected.*

<sup>1</sup> Aberdeen Group “Sustaining Compliance: How I Learned to Stop Worrying and Love the Security Audit”


**Solution Brief:**
**Shavlik Security Suite for PCI DSS**

	PCI DSS Control Requirement	Shavlik Security Suite Functionality	Sub-Sections Directly Impacted
3.	Protect stored cardholder data	This requirement generally speaks to encryption of data and access level file control. Encryption is not covered by Netchk Configure, but uses custom check to assess permissions on cardholder data stores and files and can create a check to ensure an encryption service is running. This solution can also track and enforce restrictions of access to I/O devices like USB ports.	
4.	Encrypt transmission of cardholder data, and sensitive information across public networks	Netchk Configure has the ability to enforce certain encryption standards through built-in and custom checks.	
5.	Use regularly updated antivirus software	Custom checks for determining how current an antivirus application or data file can also be used to meet this requirement.	5.2 Ensure that all antivirus mechanisms are current, actively running, and capable of generating audit logs.
6.	Develop and maintain secure systems and applications	Use Netchk Configure to help control access to workstations and servers via the built-in "account inspection and management" capability. This allows for identification, disabling and enabling of accounts. Monitor and maintain secure systems using security baselines or specific checks to manage security on these systems. In addition, IIS checks can help with web server requirements.  Through integration with Shavlik's Security Intelligence (SSI), users can create thresholds and alerts for circumstances related to patch, configuration and spyware events. By utilizing Shavlik's NetChk Protect solution it is possible to maintain up-to-date system patches and provide reporting as to when patches were applied to specific machines. Reporting capabilities are very extensive, providing both static reports and real-time ad hoc query capabilities, trending and dashboards.	6.3.1 Testing of all security patches and system and software configuration changes before deployment  6.3.2 Separate development, test and production environments  6.5.9 Denial of service  6.5.10 Insecure configuration management
7.	Restrict access to cardholder data by business function and need-to-know	Use Netchk Configure to restrict and manage access to systems containing payment card data with built-in "account inspection and management" capability. Custom checks can assess specific user rights or file/folder permissions related to cardholder data.	7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.  7.2 Establish a mechanism for systems with multiple users that restricts access based on a users need to know and is set to "deny all" unless specifically allowed.

*This document is provided strictly as a guide. No guarantees can be provided or expected.*

 **Solution Brief:**

Shavlik Security Suite for PCI DSS

	PCI DSS Control Requirement	Shavlik Security Suite Functionality	Sub-Sections Directly Impacted
8.	Assign unique IDs to all persons with access to cardholder data	1) Use Netchk Configure to help control access to workstations and servers via the built-in "account inspection & management" capability. This allows for identification, disabling and enabling of accounts. 2) Use Netchk Configure to create a policy that will govern user access (password age, logon attempts, etc).	<p>8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects</p> <p>8.5.4 Immediately revoke access for any terminated users</p> <p>8.5.5 Remove inactive user accounts at least every 90 days</p> <p>8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed</p> <p>8.5.8 Do not use group, shared, or generic accounts and passwords</p> <p>8.5.9 Change user passwords at least every 90 days</p> <p>8.5.10 Require a minimum password length of at least seven characters</p> <p>8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she used</p> <p>8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts</p> <p>8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID</p> <p>8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate</p>
9.	Restrict physical access to cardholder data	A policy can be created with Netchk Configure to provide password required screensaver protection.	

*This document is provided strictly as a guide. No guarantees can be provided or expected.*


**Solution Brief:**

## Shavlik Security Suite for PCI DSS

	PCI DSS Control Requirement	Shavlik Security Suite Functionality	Sub-Sections Directly Impacted
10.	Track and monitor all access to network resources and cardholder data	Netchk Configure performs validation checks on system auditing settings which include failed attempts to access file systems and data stores on workstations and servers. Should changes be made to password related baselines (e.g. password length, failed attempts, history, age and more), Shavlik can report, alert or remediate these deviations from policy. Compliance checks for event log management and auditing allow for proper tracking of events related to access.	<p>10.2.1 All individual user accesses to cardholder data</p> <p>10.2.2 All actions taken by any individual with root or administrative privileges</p> <p>10.2.3 Access to all audit trails</p> <p>10.2.4 Invalid logical access attempts</p> <p>10.2.5 Use of identification and authentication mechanisms</p> <p>10.2.7 Creation and deletion of system-level objects</p>
11.	Regularly test security systems and processes	<p>By using the Shavlik Security Suite of software applications (including NetChk Protect, Shavlik Security Intelligence and Netchk Configure) it is possible to easily validate and remediate gaps in the security posture. It is also easy to provide evidence that these routine checks have occurred.</p> <p>Using Netchk Configure, a wide variety of checks can easily be created to suit individual environments and needs. These checks take literally minutes to create. Using custom checks combined with hundreds of built-in checks create and use baselines to test, remediate, and maintain security.</p>	
12.	Maintain a policy, which addresses information security	Use Netchk Configure and the PCI Policy Template as a means to translate written policy into technical controls which can also be customized. Use Netchk Configure as a security configuration policy repository, which can be easily referenced in support of any audit requirements.	

*This document is provided strictly as a guide. No guarantees can be provided or expected.*



## Solution Brief:

### Shavlik Security Suite for PCI DSS

## Key advantages of Shavlik NetChk Security Suite

### Continuous Proof of PCI DSS Vulnerability Compliance

- ▶ View details of each security setting including local security policy information
- ▶ PCI-specific alerts, dashboard, and reports provide compliance assurance
- ▶ Security auditing based on PCI DSS security controls
- ▶ Scheduled scanning and policy enforcement
- ▶ Integrated data backend enables comprehensive reporting
- ▶ Custom checks wizard enables administrators to quickly add new checks as necessary to comply with changing requirements

### Ease of use

- ▶ Get up and running in hours, not days or weeks
- ▶ Automated policy baseline development and enforcement
- ▶ Rationale explaining why a security measure is recommended
- ▶ Find, compare or enforce security settings on multiple systems

### Superior protection

- ▶ Settings recommendations based on real-world security experience
- ▶ Policy dashboard provides a comprehensive view of the state of the organization's security configuration posture
- ▶ Knowledge base of information to secure operating systems, databases and web servers
- ▶ Combination of both agent and agentless scanning gives unrivaled perspective on network status

*This document is provided strictly as a guide. No guarantees can be provided or expected.*

## PCI Summary Report

### Scan Policy Compliance Summary by Item



Report Date: 10/7/2009 1:50 PM

Scan Date	Scan By	Version	Policy Name	Machine Group
10/7/2009 1:04:36 PM	VM-LS-XPP-OFF/Administrator	4.1.232	PCI	My Machine
Policy Check		Machines Compliant	Machines Noncompliant	
<b>PCI DSS 1.1</b> 1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the				
	Windows Firewall (GPO Domain Profile) Status	0%	(0 of 1)	100% (1 of 1)
	Windows Firewall (GPO Standard Profile) Status	0%	(0 of 1)	100% (1 of 1)
	Windows Firewall (Standard Profile) Status	0%	(0 of 1)	100% (1 of 1)
	Windows Firewall Status	0%	(0 of 1)	100% (1 of 1)
<b>PCI DSS 1.1</b> 2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to				
	Alerter Service Status	100%	(1 of 1)	0% (0 of 1)
	Application Layer Gateway Service Status	0%	(0 of 1)	100% (1 of 1)
	Application Management Service Status	100%	(1 of 1)	0% (0 of 1)
	Automatic Updates Service Status	100%	(1 of 1)	0% (0 of 1)
	Background Intelligent Transfer Service Status	100%	(1 of 1)	0% (0 of 1)
	Clipboard Service Status	100%	(1 of 1)	0% (0 of 1)
	COM+ Event Services Status	100%	(1 of 1)	0% (0 of 1)
	COM+ System Application Service Status	100%	(1 of 1)	0% (0 of 1)
	Computer Browser Service Status	100%	(1 of 1)	0% (0 of 1)
	Cryptographic Services Status	100%	(1 of 1)	0% (0 of 1)
	DCOM Server Process Launcher Service Status	100%	(1 of 1)	0% (0 of 1)
	DHCP Client Service Status	100%	(1 of 1)	0% (0 of 1)
	Distributed Link Tracking Client Service Status	100%	(1 of 1)	0% (0 of 1)
	Distributed Transaction Coordinator Service Status	100%	(1 of 1)	0% (0 of 1)
	DNS Client Service Status	100%	(1 of 1)	0% (0 of 1)
	Error Reporting Service Status	0%	(0 of 1)	100% (1 of 1)
	Event Log Service Status	100%	(1 of 1)	0% (0 of 1)
	Fast User Switching Compatibility Service Status	0%	(0 of 1)	100% (1 of 1)
	Fax Service Status	100%	(1 of 1)	0% (0 of 1)
	FTP Publishing Service Status	100%	(1 of 1)	0% (0 of 1)
	Help and Support Service Status	100%	(1 of 1)	0% (0 of 1)
	HTTP SSL Service Status	100%	(1 of 1)	0% (0 of 1)
	Human Interface Device (HID) Access Service Status	100%	(1 of 1)	0% (0 of 1)
	IIS Admin Service Status	100%	(1 of 1)	0% (0 of 1)
	IMAPI CD-Burning COM Service Status	100%	(1 of 1)	0% (0 of 1)
	Internet Connection Firewall (ICF - pre-Vista)/Internet Connection	0%	(0 of 1)	100% (1 of 1)
	IPSEC Services Status	100%	(1 of 1)	0% (0 of 1)
	Logical Disk Manager Administrative Service Status	100%	(1 of 1)	0% (0 of 1)
	Logical Disk Manager Service Status	100%	(1 of 1)	0% (0 of 1)
	Messenger Service Status	100%	(1 of 1)	0% (0 of 1)
	MS Software Shadow Copy Provider Service Status	0%	(0 of 1)	100% (1 of 1)
	Netlogon Service Status	0%	(0 of 1)	100% (1 of 1)
	NetMeeting Remote Desktop Sharing Service Status	0%	(0 of 1)	100% (1 of 1)
	Network Connections Service Status	100%	(1 of 1)	0% (0 of 1)
	Network DDE DSDM Service Status	100%	(1 of 1)	0% (0 of 1)
	Network DDE Service Status	100%	(1 of 1)	0% (0 of 1)
	Network Location Awareness (NLA) Service Status	100%	(1 of 1)	0% (0 of 1)

*This document is provided strictly as a guide. No guarantees can be provided or expected.*



## Solution Brief:

### Shavlik Security Suite for PCI DSS

#### Why customers choose Shavlik:

"ACCENT has been very pleased with the implementation of the Shavlik Security Suite. We recently and successfully completed our first PCI audit. NetChk Protect and NetChk Configure performed exactly as we had hoped, enabling us to quickly bring our Windows servers into compliance as well as develop a program to keep them in compliance. In fact, the auditors commented that it was one of the cleanest first audits they had ever performed. Thank you for helping us confidently demonstrate our compliance. We look forward to continued use of Shavlik's products."

— **Nathan Ziege, Director, Network Services, Information Technology, ACCENT Marketing Services, LLC**

"Shavlik's solution was extremely fast to implement and easy to administer- we were doing full scans of our IT environment within one week of installation... and more importantly, Shavlik Technologies delivered a solution with the capability to automatically map our system configurations directly to PCI compliance requirements. Another big selling point is that NetChk Configure can both scan AND remediate, as a lot of other solutions require manual remediation of each node. We simply don't have the resources to devote to this extra effort. The simplicity and automation of Shavlik has allowed us to assign the management of NetChk Configure to the same full-time employee who also manages our patch and threat management efforts – a significant savings as most of the other solutions we evaluated would have required an additional full-time resource just to manage their single solution."

"Our PCI initiative was accomplished in December 2008 and we are now 100% PCI compliant. The results have been a measurable ROI and auditors acknowledging significant improvement in a short amount of time. We now have the visibility and the confidence that the auditor will simply tell us what we already know."

— **Adrian Butler, Vice President, Information Technology for Accor North America**

This document is provided strictly as a guide. No guarantees can be provided or expected.