

RISK ADVISORY SERVICES

PCI ADVISORY SERVICES

WHAT IS PCI AND DOES IT APPLY TO ME?

IF YOUR COMPANY ACCEPTS CREDIT CARDS TO CONDUCT BUSINESS, ARE YOU AWARE OF THE MANDATORY REQUIREMENTS OUTLINING HOW YOU MUST STORE AND PROTECT THIS INFORMATION?

Use of credit cards has become a more accepted and prevalent method of payment, but in the process of authorizing a transaction, you must ensure confidential information is adequately protected against today's risks. If you store, process, or transmit card holder information, these controls apply to you and you must be compliant.

The Payment Card Industry is comprised of five major credit cards brands and they have established requirements to reduce the risk of exposure, which must be implemented and assessed on a regular basis. Failure to meet these requirements could result in penalties or possibly revocation in the ability to accept credit cards. Depending upon the number or amount of credit card transactions you process, the requirements that apply to you are different.

What are the PCI requirements?

PCI DSS (Data Security Standards) define high level areas such as:

- Building & Maintaining a Secure Network
- Maintaining a Vulnerability Management Program
- Monitoring and Testing Networks
- Protecting Cardholder Data
- Implementing Strong Access Controls
- Maintaining Information Security Policy

These PCI requirements and risks are only applicable to credit card information, and

with today's efforts to reduce the corporate technology footprint to lower costs through system consolidation, it can be challenging to ensure the identification, segregation, and protection of this information meets PCI standards. In the event you experience a breach that exposes card holder data, it can seriously damage your company image and possibly require you to protect the cardholders placed at risk.

Our team of IT professionals in the Technology Risk and Security practice can help you:

- Understand and document the flow of card holder information, and evaluate the method used to segment your PCI sensitive information from the rest of your corporate infrastructure.
- Perform a PCI readiness assessment to identify and prioritize gaps that may exist in meeting PCI requirement criteria. We will provide recommendations to address each identified gap and help establish a plan to prioritize remediation activities and achieve PCI compliance.
- Review your vulnerability management program to ensure it is designed to meet PCI requirements and address PCI security events in a timely manner.
- Develop a framework to ensure your solution remains current and addresses the PCI DSS needs on a continual basis.



CONTACT BDO

National

Sam Khoury
416 369 6030
skhoury@bdo.ca

Central Canada

Carlo Mariglia
416 369 3078
cmariglia@bdo.ca

David Knott
416 815 3016
dknott@bdo.ca