PCI DSS consultancy services

If you take credit cards for goods and services, you must be PCI DSS compliant. If you're not compliant, you could be fined or have your ability to take credit cards away from you. Are you compliant?

The problem

The Payment Card Industry Data Security Standard (PCI- DSS) is a mandatory security standard for adoption by organizations that handle credit cards. Dealing with PCI- DSS compliance is a challenge for most organizations that take credit cards, as is identifying when an organization has done enough to successfully achieve compliance.

Most organizations use credit card data in a multitude of different ways, and the way that they process it varies greatly. When combined with the fact that some host the data directly, but others rely on third parties and that credit card data typically exists in both electronic and paper form, the challenge is exacerbated.

So what can be done about it?

KPMG's approach

KPMG have been helping organizations with their PCI DSS compliance requirements for many years.

Depending on your requirements, KPMG will define a customized approach to help you with your compliance requirements, taking into account the specific budgetary and time requirements that you may have.

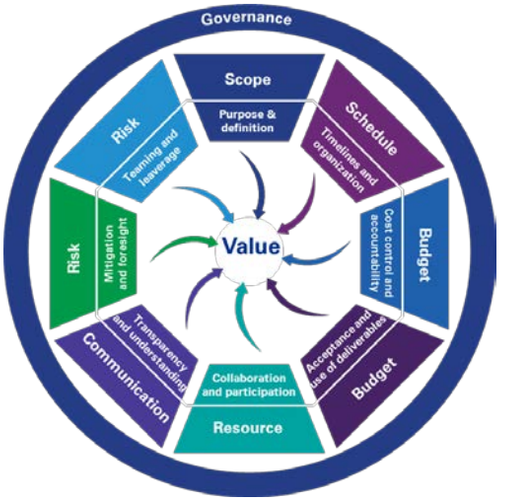
To assist with compliance, we typically take a phased approach splitting the engagement into manageable workstreams. We spend time understanding the characteristics, capabilities, gaps and improvement opportunities for your cyber security posture, as well as how it can impact your ultimate compliance with PCI DSS.

- **Phase 3**: Cyber security risk/threat modelling and evaluation;
- **Phase 4**: Targeted maturity levels identification;
- **Phase 5**: Assessment of current security strategy, together with cyber security program adjustment and re-sequencing.
- **Phase 6**: Issuing the final report and presenting to management.

The overarching principle we adopt is to build on any PCI DSS compliance activities you have already completed, and provide you with the most appropriate compliance strategy for your organization.

The strategy will include a prioritized set of activities, and will include quick-win activities where appropriate. In addition, the strategy can take into account global considerations (for large multi-nationals) and provides appropriate key performance indicators (KPI's) and key risk indicators (KRIs) as metrics to track PCI DSS compliance progress and provide updates to boards and executives.

Further, we are able to interface with your QSA if appropriate, to help ensure that the program achieves its ultimate aim. Although PCI DSS compliance can take some time to achieve (depending on the scope of our activities), we are able to provide guidance on the timeframes and budget required to be successful.



The KPMG PPM Methodology

Key benefits

By using KPMGs PCI DSS Consultancy and compliance services, you are able to benefit from the following:

- A key driver of a successful project is making sure the team is comprised of individuals that understand your requirements and objectives and who have successfully completed engagements of similar scope and complexity. Our team has a thorough understanding of the issues and challenges you face with regards to PCI DSS compliance.
- We have completed many PCI-DSS diagnostic and readiness projects. KPMG's PCI-DSS diagnostic and readiness assistance services are adaptable and flexible for use with organizations of different sizes and complexity.
- Our strategy is to work collaboratively with you to leverage your existing in-house resources and documentation, to provide relevant knowledge, advice, methodology and assistance to the extent required by management.
- KPMG brings together professionals in information protection and business continuity, risk management, privacy, organizational design, behavioral change and intelligence management. These combined skills are used to assess and design your PCI-DSS compliance controls.
- When this deep knowledge is linked to our world-class methodologies and tools to support our security professionals worldwide on other related standards such as ISO 27000, PCI-DSS, NIST, ISF, and SANS, we strive to ensure that our services are delivered in a consistently efficient and effective manner, using the latest techniques, and providing high value to our local and worldwide clients.
- As we are a global organization, we are able to assist you with your PCI DSS compliance challenges in Canada, as well as any other geographic locations that you operate.
- At the heart of KPMG's PCI DSS compliance assessments in the use of the KPMG PPM methodology, This methodology helps to ensure that all activities are executed as efficiently as possible.

KPMG's Cyber Team works with organizations to prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

Have a cyber emergency? Contact our 24/7 Cyber response hotline.

1-844-KPMG-911
1-844-576-4911

KPMG Cyber Security professionals believe cyber security should be about what you can do — not what you can't

An objective, knowledgeable advisor

As a global network of regulated member firms, we have an unwavering commitment to precision, quality and objectivity in everything we do. So you can rest assured that KPMG cyber security assessments and recommendations are based on what's best for your business – not on market hype.

Knowledge of emerging issues

In our I-4 Forum, also known as the International Integrity Institute, we convene leading cyber security professionals from around the world to discuss emerging threats, regulatory challenges and solutions. So we can help you consider possible issues around the corner in financial services, oil and gas, pharmaceuticals, engineering and other industries.

Rated no. 1 In executive management

In fact, in a 2016 Forrester Wave™ study on information security consulting services, companies rated KPMG No. 1 for counseling senior leadership on cyber security. KPMG member firms surpass other professional services firms and technical firms to help board members understand cyber security, make informed decisions that align to the business strategy, and feel assured in their due diligence.

Transforming security across different geographies and cultures

KPMG member firms have deep local knowledge in nearly every market where you do business, so we understand cyber security risks, regulatory impacts, change management, forensic investigations and other factors that may change from one country to the next. We have a global network of more than 3,000 cyber security professionals, plus multi-disciplinary collaboration with 189,000 other professionals in KPMG member firms across more than 152 countries. With that global presence, we can help you drive security transformation across your operations, wherever they may be.

Contact us

Francis Beaudoin
National Leader,
Technology Risk Consulting
T: 514-840-2247
E: fbeaudoin@kpmg.ca

Jean-Francois Allard
Partner
T: 514 840 2645
E: jeanfrancoisallard@kpmg.ca

Yassir Bellout
Partner
T: 514-840-2546
E: ybellout@kpmg.ca

Erik Berg
Partner
T: 604-691-3245
E: erikberg@kpmg.ca

John Heaton
Partner
T: 416-476-2758
E: johnheaton@kpmg.ca

Adil Palsetia
Partner
T: 416-777-8958
E: apalsetia@kpmg.ca

Jeff Thomas
Partner
T: 403-691-8012
E: jwthomas@kpmg.ca