ISO 27001 certification

Cyber issues are inevitable. However, an independent assessment that attests that your organization is following good security practice not only helps verify your cyber risk management capabilities to you and your clients.

The problem

There are many cyber challenges that companies now face on a daily basis. In an effort to demonstrate that they're taking security seriously, many organizations are seeking to follow good security practice, such as that defined in ISO 27002. While adherence to good practice is a step in the right direction, many organizations are going one step further and are seeking independent verification that they're following good practice appropriately. As a consequence, they're looking for ISO 27001certification.

How can we help?

Our services cover the implementation of the recognized information security standard ISO 27001, as well as the preparation for a certification audit. We review the relevant documentation and, if necessary, we help to amend or improve it. We give you support with the identification of risks and help you develop your risk assessment methodology. We can also organize for you the certification audit itself. In co-operation with you we prepare a statement of applicability for the ISO 27001 standard.

The KPMG approach:

KPMG in Canada has adopted a three phase process for certifying organizations to ISO 27001 compliance. The phases are as follows:

- **Phase 1**
  Certification assessment and documentation review
  This stage is to confirm the effective implementation and compliance with the management system elements of ISO27001.
- **Phase 2**
  Certification audit
  The next stage is to confirm the effective implementation and compliance with ISO/IEC 27001:2013.
- **Phase 3**
  Ongoing surveillance
  The final stage is to confirm ongoing compliance. The criteria for ongoing assessment visits is based on PECB requirements and will be conducted every 12 months, when the ISO27001 certification undergoes a renewal process. Typically there is an initial visit after the first 6 months.

The KPMG advantage

There are many reasons for selecting KPMG in Canada to complete your ISO 27001 certification:

- Our approach to performing ISO 27001 certification audits is effective and is designed to minimize disruption to your business activities. We won't be constantly requesting information and documentation from you outside of onsite fieldwork days.
- We work collaboratively with you and like to ensure that our knowledge and insight is retained in the organization.
- The team we use to conduct our ISO27001 advisory work are information security professionals. The team we will deploy for you are fully qualified ISO27001 lead auditors. The blend of these two teams means that you're getting the right people at the right time to meet your needs.

Why choose KPMG

We have extensive knowledge and experience in performing ISO27001 advisory work and certification audits. Our key credentials that distinguish us as the clear choice for this work are detailed below:

- KPMG is the only ‘Big 4’ firm that is accredited to perform ISO27001 certification audits, and we strive to provide the highest level of assurance through our audits.
- We have the experience of certifying numerous global organizations who have a similarly mature understanding of information security.
- We have a proven methodology and our certification approach is accredited by PECB, a globally recognized accreditation body.
- Our team has extensive experience in providing advice and assurance over IT and security controls. Our people are trained, qualified, and experienced information security professionals, who have chosen a career in information security.
- All deliverables go through our rigorous internal quality assurance review process, so that you can take comfort that we will strive to provide consistency in our findings and always achieve the level of quality that you would expect from us.
- KPMG is an independent firm with an international reputation for high standards, professional ethics and client confidentiality. We are independent of the ISO27001 standard and vendors so you know that our findings are without bias, regardless of the investment or changes that may be required.
- We are able to deliver ISO 27001 certification in multiple jurisdictions, using local resource where appropriate.

KPMG’s Cyber Team works with organizations to help 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 or 1-844-576-4911

CANADIAN Lawyer ★2016–2017★ READERS' CHOICE AWARDS Forensic Accounting

CANADIAN Lawyer ★2016–2017★ READERS' CHOICE AWARDS Cyber Security Consultants

CANADIAN Lawyer ★2016–2017★ READERS' CHOICE AWARDS Litigation Support & E-Discovery Consultants

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^{TM} 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

kpmg.ca/Cyber