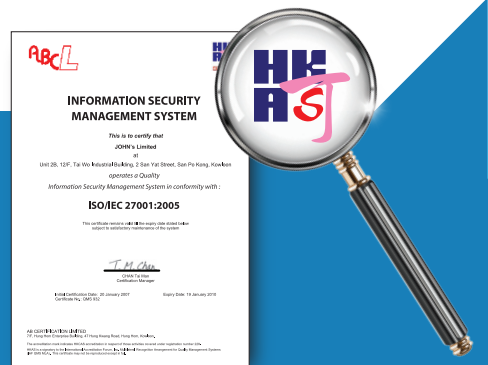
What is HKAS Accreditation?
什麼是香港認可處的認可?

Accreditation gives you quality assurance. The Hong Kong Accreditation Service (HKAS), a government organisation, grants accreditation to certification bodies under the Hong Kong Certification Body Accreditation Scheme (HKCAS). Application for accreditation is open and voluntary. Only competent certification bodies that meet the requirements of the relevant international standards (e.g. ISO/IEC 17021 and ISO/IEC 27006) can achieve accreditation for ISMS certification. Users of certification service should look for accredited service to protect their interests.

HKAS introduced accreditation service for ISO/IEC 27001 certification in November 2011. HKAS-accredited certification bodies providing ISO/IEC 27001 certification service, once available, will be announced at HKAS's website (www.itc.gov.hk/en/quality/hkas/hkcas/cb_no.htm).

認可服務提供品質保證。香港認可處是政府機構，根據「香港認證機構認可計劃」向認證機構發出認可資格。申請認可資格是公開及屬於自願性質。只有符合相關國際標準(如ISO/IEC 17021和ISO/IEC 27006)要求的機構，才能獲發ISMS認證的認可資格。用戶應尋找已獲認可的認證服務，以保障他們的利益。

2011年11月，香港認可處推出ISO/IEC 27001認證的認可服務。當有認證機構獲香港認可處認可提供ISO/IEC 27001認證服務，將會在香港認可處網站(www.itc.gov.hk/ch/quality/hkas/hkcas/cb_no.htm)公布。



Hong Kong Council for Testing and Certification
香港檢測和認證局

The Government of the Hong Kong Special Administrative Region set up the Hong Kong Council for Testing and Certification (HKCTC) in September 2009 to advise the Government on the overall development strategy of the testing and certification industry. The vision of HKCTC is to develop Hong Kong into a testing and certification hub in the region.

香港特別行政區政府於2009年9月成立香港檢測和認證局，就檢測和認證業的整體發展策略向政府提供意見。該局的願景是將香港發展為區內的檢測和認證中心。

For more information,
please visit the following websites
如要了解詳情，請瀏覽下列網頁

Hong Kong Council for Testing and Certification
香港檢測和認證局
www.hkctc.gov.hk

Hong Kong Accreditation Service
香港認可處
www.hkas.gov.hk

Tested in Hong Kong, Certified in Hong Kong
香港檢測•香港認證

Understanding Information Security Management System (ISMS) Certification
認識資訊安全管理系統認證

What is Information Security Management System (ISMS)?
什麼是資訊安全管理系統(ISMS)?

Information security continues to be a big concern territory-wide nowadays. Organisations with poor or inadequate information security measures are often prone to unauthorised attacks and intrusion, thereby undermining the confidence of their clients and the public at large.

Information Security Management System (ISMS) is a part of the overall management system, based on the approach of controlling business risks, to establish, implement, operate, monitor, review, maintain and improve information security.

ISO/IEC 27001 is an international standard published by the International Organisation for Standardisation to specify the normative requirements for the development and operation of ISMS.

The purpose of implementing ISMS is to assist an organisation to achieve its business objectives, such as to raise productivity, to enhance reputation, or to attract more investors and clients, through treating and managing information security risks against its risk acceptance levels through a risk assessment.

近年來，資訊保安持續備受廣泛關注。資訊保安措施欠佳或不足的機構，往往容易受到黑客攻擊或入侵，因而打擊客戶及普羅大眾對他們的信心。

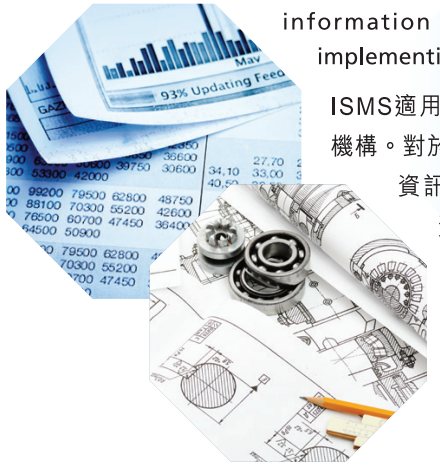
資訊安全管理系統(Information Security Management System，簡稱ISMS)是整體管理系統的一部分，基於控制業務風險的方針，建立、實施、運行、監控、審查、維護和改進信息安全。

ISO/IEC 27001是國際標準化組織發布有關ISMS的國際標準，為系統的開發與運作提供規範性的要求。

實施資訊安全管理系統的目的，在於協助機構透過風險評估，因應其風險接受程度有效地應對及管理資訊保安風險，從而達到業務目標，例如提升工作效率、提高聲譽，或吸引更多投資者及客戶。

Who should Implement ISMS?
誰應實施ISMS?

ISMS is applicable to organisations of all sizes and in all business sectors. In particular, organisations storing and/or handling information that is personally sensitive, or information that is of a commercially sensitive nature and value (e.g. product design) or information that is business critical (i.e. information that needs to be accurate and its integrity assured). The processing of such information will benefit from implementing ISMS.



ISMS適用於各行各業、不同規模的機構。對於需要儲存或處理個人敏感資訊、敏感及具價值的商業資訊(如產品設計)、或關鍵性業務資訊（即需要保證其準確性和完整性的資訊）的機構而言，實施ISMS尤其有用。

What are the Benefits of Getting ISMS Certification?
獲得ISMS認證有何好處?

Certification is an attestation issued by a third-party body, through a formal conformity assessment process, that specified requirements (e.g. ISO/IEC 27001) are fulfiled.

Certification of ISMS to ISO/IEC 27001 allows an organisation to demonstrate that its information assets are adequately protected against information security risks. It gives greater confidence to its business partners, authorities and other interested parties.

認證是通過一個正式的合格評定程序，由第三方發出證明，表示已滿足某些特定的要求(如ISO/IEC 27001)。

獲得ISO/IEC 27001 ISMS認證，可讓機構更能確保本身的資訊資產受到充分保護，免受資訊保安風險影響，從而為業務夥伴、規管當局及其他相關人士帶來信心。

Where can I Obtain ISMS Certification Services?
我在哪裡可以取得ISMS認證服務?

Some local certification bodies have already been providing ISO/IEC 27001-based ISMS certification services.

部分本地認證機構已開展ISO/IEC 27001 ISMS認證服務。

Major Steps of Establishing and Implementing ISMS to ISO/IEC 27001
建立和實施ISO/IEC 27001 ISMS的主要步驟

ISO/IEC 27001 adopts a "Plan-Do-Check-Act" model for establishing, implementing, maintaining and continually improving an ISMS:

ISO/IEC 27001採用「規劃—實施—檢查—處置」的模式以建立、實施、保持和持續改進ISMS：

1. Define the scope, boundary and policy of ISMS
   確定ISMS的範圍、邊界和方針
2. Define the risk assessment approach of the organisation
   確定機構的風險評估方法
3. Identify and evaluate risks and options for the relevant treatment
   識別和評估風險及其處理方法的方案
4. Select appropriate control objectives and controls for the treatment of risks
   為處理風險選擇合適的控制目標和控制措施
5. Obtain management approval of the proposed residual risks
   獲得管理層批准建議的殘餘風險
6. Obtain management authorisation to implement and operate the ISMS
   獲得管理層授權實施和運行ISMS
7. Monitor, review, maintain and improve the ISMS continuously
   不斷地監視、評審、保持和改進ISMS