



Hong Kong Computer Society
Room 1915, 19/F,
China Merchants Tower, Shun Tak Centre,
168 Connaught Road Central, Hong Kong

Tel: 2834 2228
Fax: 2834 3003
URL: <http://www.hkcs.org.hk>
Email: hkcs@hkcs.org.hk



HKCS RESPONSE

COMMONLY ACCEPTED AUDIT OR ASSESSMENT MECHANISM TO CERTIFY INFORMATION SECURITY STANDARDS

6th October 2004



HKCS RESPONSE - COMMONLY ACCEPTED AUDIT OR ASSESSMENT MECHANISM TO CERTIFY INFORMATION SECURITY STANDARDS



Table of Contents

Executive Summary	3
Introduction.....	4
Scope of Review	4
Professional Organizations/Associations.....	4
Information Technology	4
Industry Sector	5
Investment Barriers to Entry	6
Information Security Certification Audit Mechanisms.....	7
Benchmarking	7
Audit/Assessment Mechanisms	7
International Development.....	9
International Standards Organisation.....	9
United States	10
Korea.....	10
Japan	11
Proposed Approach.....	12
Conclusion	12

Executive Summary

The major theme adopted throughout this response is aimed to achieve a harmonised approach towards information security capable of being understood by all organisations and industry sectors. In summary, the HKCS:

- (a) supports the concept of developing and promoting information security standards for application throughout Hong Kong;
- (b) feels that the underlying Security Bureau principles expressed within the invitation may be too reliant upon Professional Organizations/Associations and too narrowly focused on information technology;
- (c) of the opinion that customers, business partners, stakeholders, shareholders and the Government equally should perform important roles when determining information security concerns;
- (d) does not believe the benefits of having to adopt a silo approach whereby individual industry sectors are required to develop their own information security standards will prove beneficial both to the industry sector in general, and more importantly, to individual organisations, the majority of which are made up of small-medium enterprises (SME);
- (e) is concerned that restricting the applicability of information security standards to only those areas that rely on “information technology” may be too narrowly focused;
- (f) prefers to not look at security of technology in isolation of the broader business security issues (e.g. personnel, physical security, business continuity etc...) as such an approach only provides a partial view of the overall required information security solution;
- (g) supports an approach whereby information security assurance can be utilised as an enabler in allowing organisations to achieve greater business opportunities in a global environment and not just being restricted to Hong Kong;
- (h) on a short-term basis supports the Government in not mandating an information security accreditation scheme, however, feels the Government could undertake immediate steps to enable such schemes, where present, to be better recognised;
- (i) on a long-term basis would be supportive of a mandated information security accreditation scheme, should such a scheme be established;
- (j) supports an information security management systems standards approach (e.g. in accordance with ISO 17799) to specify a framework for organisations to manage information security; and
- (k) encourages an organisation’s use of internationally recognised standards as the basis to clearly demonstrate publicly to other parties that organisation’s ability to manage information security on a continuous improvement basis for its information and information systems within an established framework (regardless of their industry sector).



Introduction

Thank you for allowing the Hong Kong Computer Society (HKCS) the opportunity to provide a response to your consultation paper entitled **“Recommendation of Inter-departmental Working Group on Computer Related Crime – Commonly accepted audit or assessment mechanism to certify information security standards”**, issued on 1 December 2003.

The HKCS appreciates the invitation from the Security Bureau to be actively involved in the formulation of information security standards tailored to the needs of the Hong Kong community and to assist in the establishment of audit/assessment mechanism(s) to certify compliance with such standards.

Acceptance of our contribution towards the formulation of applicable information security standards capable of enabling further improvement in the existing regime of information security protection, detection and response, as set forth within the recommendations of the HKSAR Government Inter-departmental Working Group report on Computer Related Crime (2000-2001), is very much welcome.

Scope of Review

The HKCS feels that the underlying principles of the Security Bureau’s invitation may be too reliant upon Professional Organizations/Associations, be too narrowly focused on information technology and not be fully beneficial in its approach towards being reliant upon industry sectors.

As part of its commitment to the evolution and advancement of the Hong Kong community the HKCS would like to offer the following thoughts to enable this important review to be more successful and applicable to the advancement of the Hong Kong community.

Professional Organizations/Associations

The suggestion (in paragraph 6 of the Security Bureau invitation paper) implying that “professional organizations and associations are the most proficient parties in ascertaining ... the information security concerns” of organisations is not necessarily fully supported. The HKCS also believes that customers, business partners, stakeholders, shareholders and the Government all have equally important roles to perform when determining information security concerns.

This position is based on evidence obtained from different countries around the world including Hong Kong. For example, if the above statement were to be true, then why is there a requirement for legislation mandating how selected information pertaining to individual persons must be protected, regardless of the industry sector, e.g. Chapter 486 - Personal Data (Privacy) Ordinance?

Information Technology

Whilst the HKCS agrees with the statement included in paragraph 6 of the Security Bureau’s invitation which states:



HKCS RESPONSE - COMMONLY ACCEPTED AUDIT OR ASSESSMENT MECHANISM TO CERTIFY INFORMATION SECURITY STANDARDS



“...we have considered that for any organization that relies on information technology in its day to day operation, ensuring the security of both the information systems as well as the information itself should be part and parcel of its organizational strategy.”

it is felt that the suggestion of restricting the applicability of information security standards to only those areas that rely on “information technology” may be too narrowly focused. In fact, information can exist in many other non-technology forms including (e.g. spoken, written, body language etc...) and it is felt that equal importance needs to be placed on the protection and security of all information equally, including that information which is in some way associated with information technology.

It is evident through the efforts of the HKSAR Government in the establishment of the “Office of the Government Chief Information Officer” on 1st July 2004, that information technology is only a component of the overall requirement to deliver and protect information in today’s environment.

The HKCS is of the opinion that the Security Bureau should additionally consider all facets of information security, which includes information technology security, in order to provide a more complete and sensible approach towards allowing a top-down culture of information security governance throughout all industry sectors. Reasons supporting this top-down process includes:

- (a) This approach is becoming a more commonly adopted practice throughout a larger number of countries (see below for international reference examples);
- (b) Allowing organisations to address the complete picture of information security protection (i.e. from a management perspective) rather than just focusing on a sub-component (e.g. information technology), which could potentially lead to large weaknesses in organisational security (e.g. poor personnel recruitment practices), thus undermining the efforts to successfully implement information technology security;
- (c) Allows the likelihood of successful implementation to be far greater as top organisational management support will be an integral part of the process of adopting good information security management practices; and
- (d) Overcome the difficult process of stretched information technology budgets competing security against information technology related projects.

Industry Sector

Throughout the world the application of information security has generally not been treated based on an industry by industry sector basis.¹ The formulation of information security standards specifically tailored for the industries under the purview of organizations/associations is deemed to not be the most effective method of addressing this important area due to the following reasons:

¹ An exception potentially applies here to selected high risk industry sectors including defence, finance and Government.



HKCS RESPONSE - COMMONLY ACCEPTED AUDIT OR ASSESSMENT MECHANISM TO CERTIFY INFORMATION SECURITY STANDARDS



- (a) Potentially involves a reinvention of near identical “standards” on a repeated basis;
- (b) Selected industry sectors in Hong Kong are not sufficiently proficient in the area of information security;
- (c) Some Associations in Hong Kong cover greater than one industry sector (e.g. the Hong Kong Computer Society is not biased to any particular industry sector and has a current membership consisting of representatives from just about every industry sector);
- (d) Some industry sectors are present in every industry (e.g. all organisations are in some way involved in finance);
- (e) Potentially unnecessary commitment of workloads and resources (e.g. financial) on the part of a single organisation in having to comply with multiple industry sector standards. For example there is no single common cross-industry specific Standard that establishes a “baseline” for all Industry Sectors. Without such a cross-industry sector information security standard organisations in different industry sectors will be impaired in their ability to efficiently and effectively determine the trustworthiness of an organisation’s information security arrangements. For example when interconnection of IT systems is being planned (i.e. having to conform to multiple information security standards).

Information security standards have generally been designed throughout various different standards setting forums to be consistently applied regardless of the organisational industry sector, e.g. at a management level.² It is this generic non-industry sector specific approach that the HKCS is encouraging the Security Bureau to place greater emphasis on when considering the best solution suited to the Hong Kong environment.

Investment Barriers to Entry

It is recognised that the Security Bureau understands (i.e. paragraph 6 Security Bureau invitation) the importance of barriers causing resistance for organisations to adopt information security, i.e.:

“that investment by organizations in Hong Kong in information security measures has yet to be universally accepted as an essential operating cost of a commercial concern. We also observe the existing situation that conformance to information security standards is largely self-initiated and monitored through internal audit or external independent assessors”.

Whilst examples exist in Hong Kong of mandated security measures that need to be regularly measured, for example, the Hong Kong Monetary Authority “Guidance Note on Independent Assessment of Security Aspects of Transactional E-banking Services”³, our view is that looking at security of technology in isolation of the broader business security

² An example of this non-industry specific application (i.e. certification against) of information security standards can be obtained by looking at the variety (i.e. from just about every industry sector) of organisations that have achieved certification against BS7799-2 – see www.xisec.com

³ See: http://www.info.gov.hk/hkma/eng/guide/circu_date/20000926.htm



HKCS RESPONSE - COMMONLY ACCEPTED AUDIT OR ASSESSMENT MECHANISM TO CERTIFY INFORMATION SECURITY STANDARDS



issues (e.g. personnel, physical security, business continuity etc...) is providing only a partial view of the overall required solution.

Under the Personal Data (Privacy) Ordinance all organisations, regardless of industry sector, have a requirement to protect personal data, but to date guidelines or standards specifying how such security controls need to be applied to enable an organisation to satisfy this Ordinance could be more consistently delivered in a manner consistent with international requirements i.e. of the European Union. This is critical given the tendency of information technology to reduce the barriers associated with the free flow of information across-national borders.

Information Security Certification Audit Mechanisms

The HKCS supports the efforts of the Security Bureau to call for proactive suggestions designed to ensure the Hong Kong environment continually protects its information assets at a level consistent with international best information security practices.

Benchmarking

The HKCS is encouraged by the prior recognition of the Security Bureau that information security assurance contributes to the effective and successful achievement of an organization's objectives. This is definitely a positive and true statement.

Information security assurance can also potentially be an enabler in allowing organisations to achieve greater business opportunities in a global environment and not just being restricted to Hong Kong. This is currently a proven example in the approach being adopted by a number of outsourcing companies in India who are currently demonstrating on a world stage that they have the ability to protect and secure information assets, at least the equivalent of, if not better than, organisations based in other countries. This is one area Hong Kong, as the World City, needs to consider and potentially align its practices with to ensure it is not placing its organisations at an international disadvantage.

Providing organisations with the ability to benchmark (i.e. assess, measure and improve) their level of information security preparedness among their industry peers in accordance with selective commonly accepted mechanisms (e.g. ISO/IEC 17799) is a view strongly supported by the HKCS.

Audit/Assessment Mechanisms

Exploring the feasibility of a commonly accepted audit or assessment mechanism to certify against information security standards is an area that is becoming more increasingly applied throughout the world.

On a short term basis the HKCS supports the Hong Kong SAR Government approach of not mandating an accreditation scheme with respect to the audit or assessment of information security standards. However, the HKCS also feels that the Hong Kong SAR Government could undertake selected steps designed to enable such schemes, where present, to be better recognised.



HKCS RESPONSE - COMMONLY ACCEPTED AUDIT OR ASSESSMENT MECHANISM TO CERTIFY INFORMATION SECURITY STANDARDS



For example, the establishment of (or extension of the powers of an existing body, where one exists) a formal official authority in Hong Kong, the equivalent to JAS-ANZ (Joint Accreditation Service for Australia and New Zealand) and UKAS (United Kingdom Accreditation Service), that is capable of recognizing (i.e. by way of formally recognizing through accreditation) certification bodies with respect to their efforts aligned with promoting information security standards.

The establishment of such an extension of accreditation powers locally in Hong Kong is expected to be welcomed by existing certification organisations as this locally recognised body should reduce resource requirements incurred as a result of having to comply with an overseas accreditation body (e.g. accredited by UKAS in the United Kingdom), which may or may not be suited to the local Hong Kong environment.

Whilst consistent with the Security Bureau view that “conformance to information security standards is largely self-initiated and monitored through internal audit or external independent assessors”, the HKCS feels that the HKSAR Government can further encourage the adoption of best practice information security practices at an organisational management level in such a non-mandatory manner. Such an approach should be aimed at enabling more culturally aware best information security practices to be integrated throughout an organisation, regardless of that organisations dependence on information technology or the industry sector in which that organisation belongs. Some examples that may enable this organisation culture change to occur in a non mandatory manner include:

- (a) Establishing a consistent HKSAR Government approach when issuing and inviting organisational responses for tenders that clearly allows these responding organisations to demonstrate (i.e. in alignment with international best practices) how they meet good information security governance requirements in protecting government information assets (i.e. demonstration through willingness to subject the organisation to independent certification of their information security practices). It is potentially too much of a burden on organisations (especially SMEs) to have to provide prior demonstration of being in compliance with (for example) the ITSD Security Baseline as this is a good example of a specific industry sector approach whereby any one organisation must demonstrate compliance with multiple security protection schemes;
- (b) Implement some form of government assistance body specifically designed to encourage and assist organisations address information security (i.e. beyond the information technology specific bodies already established by the HKSAR Government);
- (c) Implementing some form of government rebate scheme to encourage organisations, especially SMEs, to adopt better information security practices. This will assist in the perceived financial burden a lot of SMEs may face when considering the adoption of information security best practices; and



HKCS RESPONSE - COMMONLY ACCEPTED AUDIT OR ASSESSMENT MECHANISM TO CERTIFY INFORMATION SECURITY STANDARDS



- (d) Greater active participation by the Hong Kong Government in international standards setting bodies (e.g. ISO)⁴, and subsequently encouraging greater public participation in information security standards setting bodies (e.g. in Hong Kong) to support these international efforts.

On a longer-term basis, the HKCS is of the opinion that mandating information security accreditation schemes should be seriously considered and encouraged. Where implemented, such an accreditation scheme would be beneficial in allowing a greater level of international recognition of Hong Kong as a jurisdiction seriously approaching the topic of information security protection. Mandating some form of information security compliance through an accreditation scheme would also be consistent with various international efforts, including the United States (Sarbanes Oxley) the European Union (Data Protection Legislation) and a number of other countries.

Where the Hong Kong SAR Government undertakes to consider such a mandated information security accreditation option, the HKCS welcomes the opportunity to further participate and contribute to supporting the Government's efforts.

International Development

International Standards Organisation

The HKCS notes that the International Standards Organisation (ISO) has actively within its international standards setting forum commenced preparations to develop/adopt an international standard for Information Security Management Systems (ISMS) based on the British Certification Standard BS 7799-2⁵.

As of the time of preparing this response, ISO has concluded that a proposed international standard for an ISMS:

- ❖ Offers significant value to a wide range of organisations (large and SME) across a wide range of industry and government sectors;
- ❖ Is of considerably greater value than national or regional standards currently adopted throughout some countries;
- ❖ Is complementary to and capable of enhancing a number of existing ISO and ISO/IEC standards;
- ❖ Can be adopted in a manner that avoids overlap and conflict with other standards;
- ❖ Fills a void for organisations seeking to be better recognised internationally for protecting their information assets;
- ❖ Permits a more level playing field in SMEs by allowing them to demonstrate their ability to successfully adopt and maintain an ISMS;

⁴ It is noted that over the past 3-4 years China has significantly increased its participation (in terms of number of active participants) in the ISO standards setting committee dedicated to information security (ISO JTC SC27).

⁵ Current timetable expectations expect that ISO will have available, for international publication, an equivalent international version of BS 7799-2 by 2006.



HKCS RESPONSE - COMMONLY ACCEPTED AUDIT OR ASSESSMENT MECHANISM TO CERTIFY INFORMATION SECURITY STANDARDS



- ❖ Provides greater world harmonisation in protecting on-line information assets (e.g. e-commerce); and
- ❖ Assists organisations in meeting current and emerging regulatory and legislative requirements.

The proposed purpose of the ISMS Standard is to specify a framework for organisations to manage information security aspects of their business, which may also be used to demonstrate to other parties their ability to manage information security. It will provide tools for continuous improvement of information security.

The scope of the proposed standard is intended to set forth requirements for establishing, developing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security within the context of the organization's overall business needs and risks.

It is important to note that organisational implementation of an ISMS in accordance with the proposed ISO international standard will have the ability to provide publicly an internationally recognised way for that organisation to demonstrate to other parties its ability to manage the security of its information and information systems within an established framework (regardless of their industry sector).

There are numerous examples throughout different national countries whereby information security standards have been proactively developed by Governments and steps taken by these Governments to have these standards adopted by local organisations. Outlined here is a very brief introduction to the approach being adopted in Korea, Japan and the United States.

United States

The United States proceeded down a regulatory path and has introduced a range of legislation mandating all organisations need to protect all forms of information. Specific legislation includes: Sarbanes Oxley, HIPAA, etc...

Through the National Institute of Standards and Technology (NIST) the United States has been very proactive over the years (particularly in the past 2 years) in the development of information security standards. Whilst the US has not formally mandated compliance to selected international security standards it is believed that the United States is more moving towards such adoption and recognised of information security Standards such as ISO/IEC 17799 through their active participation in the relevant ISO Technical Committee assigned to this Standard.

Korea

Korea has moved forward with the establishment of the Korea Information Security Agency⁶ specifically to provide a consistent approach to Information Security and Information Security Standards. Korea takes a very proactive approach within International Standards setting bodies (e.g. ISO) and in the further development of information security management standards.

⁶ See: www.kisa.or.kr

Japan

Japan is one country which has established a dedicated Division within a Government Agency (JIPDEC)⁷ specifically for the purposes of promoting and encouraging Japanese organisations to adopt and be certified against recognised information security standards pertaining to information security (i.e. based on ISO/IEC 17799 and BS 7799-2). Japan has further created a number of roles to ensure the protection of information security through the establishment of:

- (a) Office of IT Security Policy, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry,
- (b) IT Security Office Information and Communications Policy Bureau, Ministry of Public Management, Home Affairs, Posts and Telecommunications

Evidence of the success of the Japanese approach is clearly evident in that 500 organisations, from a variety of different industry sectors, have been certified against a common information security standard⁸ recognised internationally. Additionally Japan takes a very proactive approach within International Standards setting bodies (e.g. ISO) and in the further development of information security management standards in an international forum. The following chart clearly demonstrates the growth of information security management certifications in Japan.

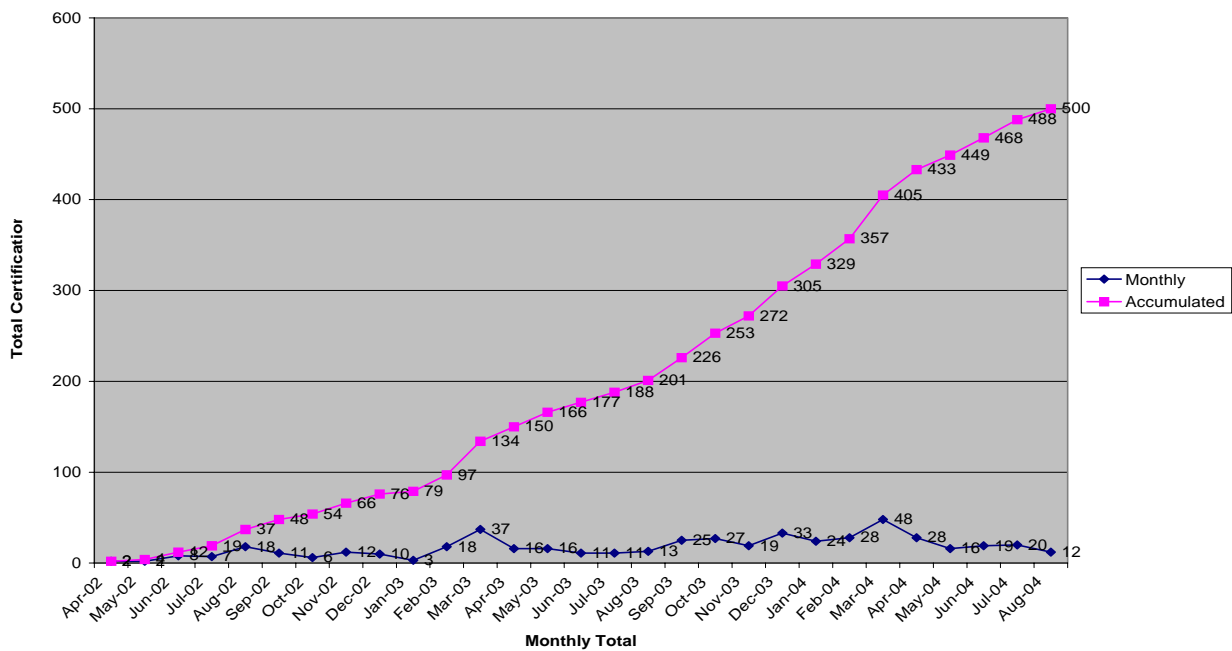


Chart 1 – Japan - BS7799-2 Certifications

⁷ See: <http://www.isms.jipdec.jp/en/>
⁸ As at 7th September 2004



Proposed Approach

The HKCS believes an approach that would allow organisations to determine their own information security requirements in a manner customised to meet its particular needs within an information security management systems framework, would be preferred, particularly with respect to allowing an organisation to:

- ❖ Identify their own information security objectives;
- ❖ Implement suitable strategies to meet these objectives;
- ❖ Measure and record outcomes; and
- ❖ Improve both the protection strategies and the information security management approach over time.

To better allow organisations to undertake this ISMS approach, a suitable internationally recognised standard (e.g. ISO/IEC 17799) is strongly recommended for local adoption throughout Hong Kong.⁹ The adoption of internationally recognised information security standards ISO/IEC 17799 (and also BS 7799-2) is an approach that has been very strongly adopted in a number of countries throughout the world including: Australia, Japan, New Zealand, Singapore, Sweden and United Kingdom.

It is important to note that flexibility needs to exist in the proposed information security standard to enable an organisation to be capable of applying the standard across an entire organisation or parts of an organisation where specific business functions, specific business processes or specific organisational units have particular requirements.

This customization approach would allow small, medium and large sized organisations to undertake a wide range of business activities within industry recognised information security best practices. This approach will also enable internal and external parties to assess an organization's ability to meet its own requirements, as well as any customer, business partner, or regulatory requirements.

Conclusion

A mechanism recognised by the Hong Kong Government for certification of compliance through audit or assessment by relevant authorized certification bodies is deemed to be strongly beneficial to the Hong Kong environment.

Different approaches towards the adoption of information security standards is generally seen as supported by selected industry sectors (e.g. finance, health, government, defence etc.), but is generally not common among other sectors that traditionally include those organisations considered to be small or medium enterprises (SME), and generally these include sectors that would not have any resource capabilities to participate in initiatives such as that offered by this Security Bureau invitation.

The HKCS believes that a more effective approach towards enhancing awareness of the importance of information security standards, and the adoption of a relevant audit mechanism among industries in a sustained and coordinated manner should be generated from within the Hong Kong Government with the support of the various professional

⁹ As discussed in the paragraph 8 of the Annex included with the Security Bureau invitation.



HKCS RESPONSE - COMMONLY ACCEPTED AUDIT OR ASSESSMENT MECHANISM TO CERTIFY INFORMATION SECURITY STANDARDS



organizations and business associations concerned, where a common agreed basis for understanding can be achieved.

The respective standards for common compliance (e.g. ISO 17799 and BS 7799-2) have already been established in an international forum and reinventing the approach based on industry sector is not seen as being economically viable for all industry sectors.

The HKCS supports the concept of BS 7799-2 in its approach towards enabling organisations to be nationally, and more importantly internationally, recognised from the perspective that they have proven on a best practice basis to have successfully developed a managed information security management system to protect the organisation's information assets.