Privacy Awareness Week 2015

#PRIVACY MATTERS
#私隱關我事

Privacy by Design
- building on standards

PRIVACY AWARENESS WEEK 關注私隱運動
MAY 3-9 五月 2015

Henry Chang, IT Advisor
Office of the Privacy Commissioner for Personal Data, Hong Kong
7 May 2015

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy by Design - building on standards

Benefits of International Standards:

- Efforts saving – No need to reinvent the wheel
- Clear communications – Common language for all parties
- Faster recognition – Minimum achievement assured
- Uniform application – Needed by MNCs to ensure there is no blind spots

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy by Design - building on standards

Some Relevant International Standards:

- ISO/IEC 27000 – Family on Information security management systems
  - 27001/27002 – ISMS Requirements and Code of Practice for Information Security Controls
  - 27081 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29100 – Information technology — Security techniques — Privacy framework

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy by Design - building on standards

Some Relevant International Standards:

- **ISO/IEC 27000 – Family on Information security management systems**
  - **27001/27002** – ISMS Requirements and Code of Practice for Information Security Controls
  - **27081** – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29100 – Information technology — Security techniques — Privacy framework

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy by Design - building on standards

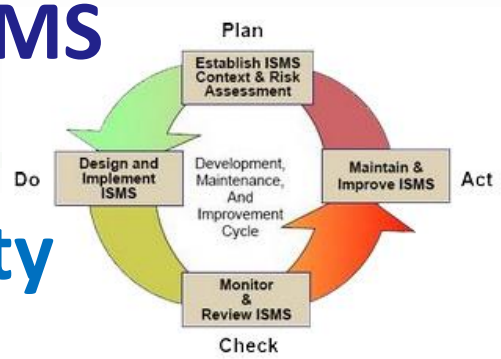
Some Relevant International Standards:

- ISO/IEC 27000 – Family on Information security management systems
  - **27001/27002 – ISMS Requirements and Code of Practice for Information Security Controls**
  - 27081 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29100 – Information technology — Security techniques — Privacy framework

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

ISO/IEC 27001/27002 ISMS



ISO/IEC 27001 – Information Security Management System:

- Covering people, processes and systems through risk management processes
- Certification proves that formal governance exists for
  - Context,
  - Leadership,
  - Planning,
  - Support,
  - Operation,
  - Evaluation and
  - Improvement

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

ISO/IEC 27001/27002

ISO/IEC 27002 – Code of practice for information security controls:

- 35 objectives (grouped under 14 areas) which may be achieved by looking at 114 controls
- For each objective/control, organisation has to decide if it is applicable and to what degree it is applicable

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

ISO/IEC 27001/27002 ISMS

You may be certified to ISO/IEC 27001 but you can only conform to ISO/IEC 27002

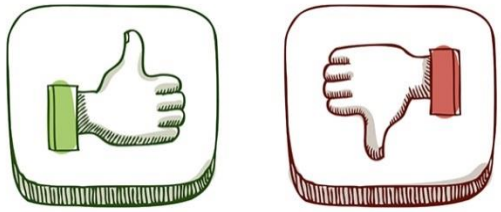
- Certified to ISO/IEC 27001 means you have a minimum and formal way to manage IT security and you have considered all major areas

- Conformed to ISO/IEC 27002 means you have considered all major areas

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

ISO/IEC 27001/27002 ISMS



Advantage:

- A comprehensive template to guide the development of a IT security management system

Disadvantage:

- The actual level of control is determined by the organisation so compliance to the standard means compliance to the levels set internally by the organisation

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy by Design - building on standards

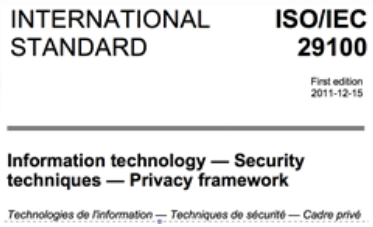
Some Relevant International Standards:

- ISO/IEC 27000 – Family on Information sec management systems
  - 27001/27002 – ISMS Requirements and Code of Practice for Information Security Controls
  - 27081 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **ISO/IEC 29100 – Information technology — Security techniques — Privacy framework**

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

ISO/IEC 29100 Privacy framework


INTERNATIONAL STANDARD

ISO/IEC 29100

First edition 2011-12-15

Information technology — Security techniques — Privacy framework

Technologies de l'information — Techniques de sécurité — Cadre privé

ISO/IEC 29100 – Privacy Framework:

- **Covering 11 principles of privacy protection governance:**
  1. Consent and choice
  2. Purpose legitimacy and specification
  3. Collection limitation
  4. Data minimization
  5. Use, retention and disclosure limitation
  6. Accuracy and quality
  7. Openness, transparency and notice
  8. Individual participation and access
  9. Accountability
  10. Information security
  11. Privacy compliance
- **Useful as a 'neutral' privacy framework for MNCs, on which jurisdictional difference can be built**

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

ISO/IEC 29100 Privacy framework

Advantage:

- Helps MNCs to develop a cross-jurisdicational privacy framework that is not biased towards a location

Disadvantage:

- Not a replacement of national privacy compliance programme
- Often sets the lowest common denominators and not the highest water marks

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy by Design - building on standards

Some Relevant International Standard

- ISO/IEC 27000 – Family on Information management systems
  - 27001/27002 – ISMS Requirements and Code of Practice for Information Security Controls
  - **27081 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**
- ISO/IEC 29100 – Information technology — Security techniques — Privacy framework

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

ISO/IEC 27018 CoP for Cloud Providers

ISO/IEC 27018 – Built on 27002 and 29100:

- Main body (based on ISO/IEC 27002)
  - Provide specific guidance on each applicable controls for cloud providers

- Annex A (based on ISO/IEC 29100)
  - Provide specific guidance on each of the 11 principles for cloud providers

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

ISO/IEC 27018 CoP for Cloud

Advantage:

- A comprehensive tailor-made guide to public cloud providers on data protection

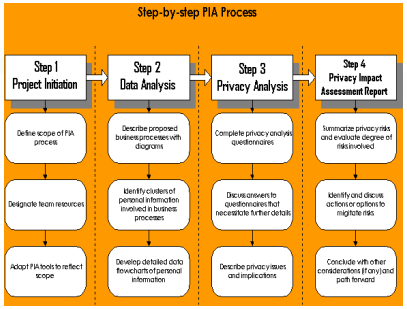
Disadvantage:

- Effectiveness and certification criteria need to be tested
- Customer-involvments are still required in terms of storage location decision, minimum security measures, sub-contracting arrangements, data breach etc.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy by Design - building on standards



Coming "soon":

- **ISO/IEC 27134 – Privacy Impact Assessment - Methodology**
  - **How to carry out a PIA**
  - **What a PIA report should contain**

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy by Design - building on standards

Take away:

- Must know what each standard is good at and weak on;
- Must know the level of measurement (the benchmark);
- Must understand customer involvement;
- Must know how it can be abused.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy Awareness Week 2015

Privacy by Design

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

PRIVACY AWARENESS WEEK
關注私隱運動

MAY
3-9 五月
2015

#PRIVACY MATTERS
#私隱關我事

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

保障資料主任聯會
DATA PROTECTION OFFICERS' CLUB