



Privacy Management Programme

**From Compliance
to Accountability**

28 May 2014



Agenda

1. Background
2. *“Privacy Management Programme: A Best Practice Guide”*
3. Key steps to setting up a Privacy Management Programme



Background



Day to Day Management

- Budget ✓
- Customer service ✓
- Public relations ✓
- Staff ✓
- Environmental impact ✓
- Privacy and data protection?



How data protection are managed?

Generally ARE

- Reactive
- Remedial
- Handled by legal and compliance staff
- Minimalist approach

Should

- Proactive
- Preventive
- Top management involvement
- Part and parcel of corporate governance



Privacy Management Programme (“PMP”)

Not a requirement under the Personal Data (Privacy) Ordinance (the “**Ordinance**”)

A strategic shift from compliance to accountability

An interim substitute of Data User Return Scheme (“**DURS**”) (Part IV of the Ordinance)



Notification requirement under the Ordinance

- Specified organisations are obliged to notify to the Commissioner "prescribed information":
 - kinds of personal data they control
 - purposes for which the personal data are collected, held, processed or used

July 2011: PCPD issued a consultation document

The initial phase is proposed to cover:

public sector

banking

telecommunications

insurance

Absence of general support



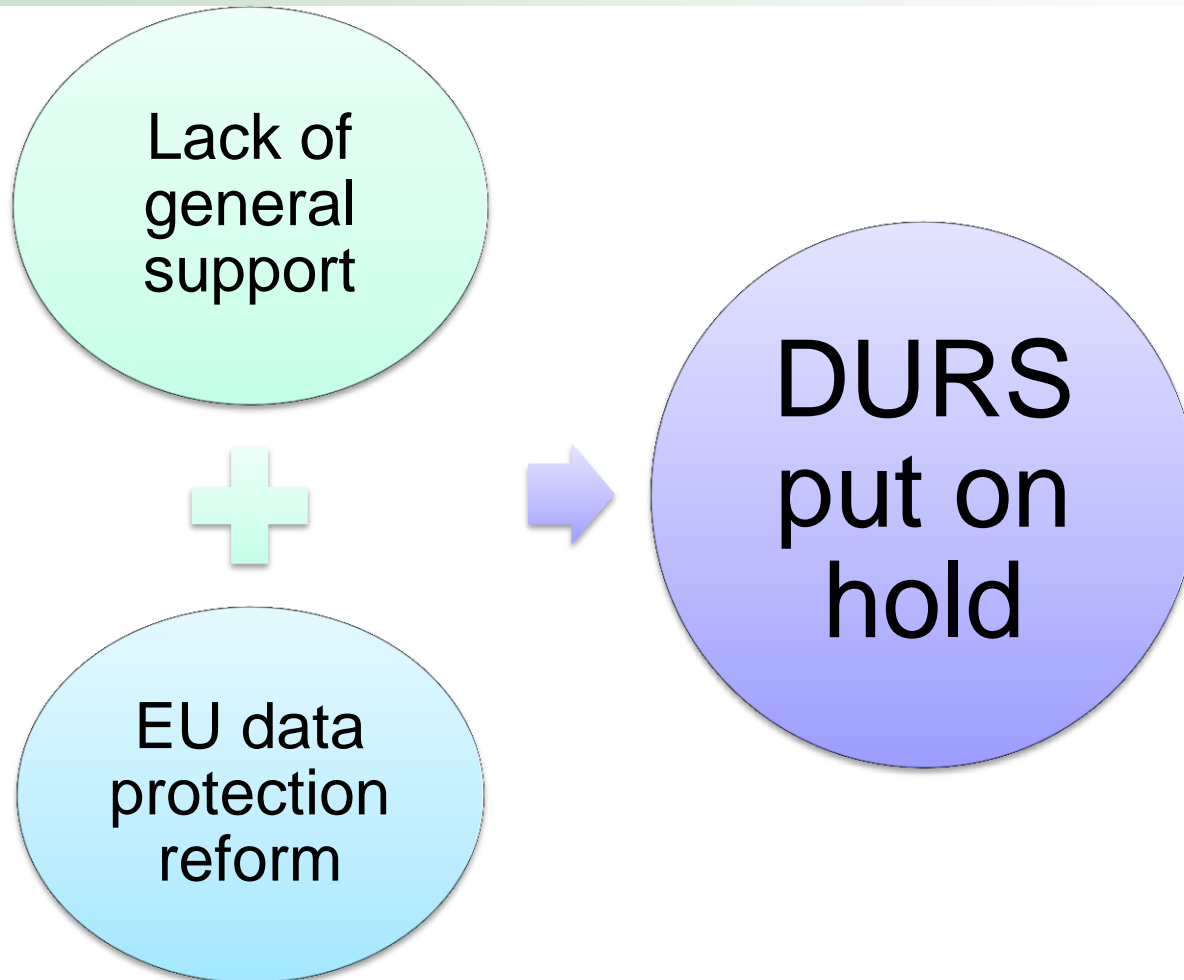
Notification requirement - EU Data Protection Reform

EU data protection reform proposed to:

- abolish notifications (upon which DURS was based)
- mandatory appointment of a data protection officer in
 - public authorities and bodies
 - private enterprises that process data of more than 5,000 persons in any consecutive 12 months



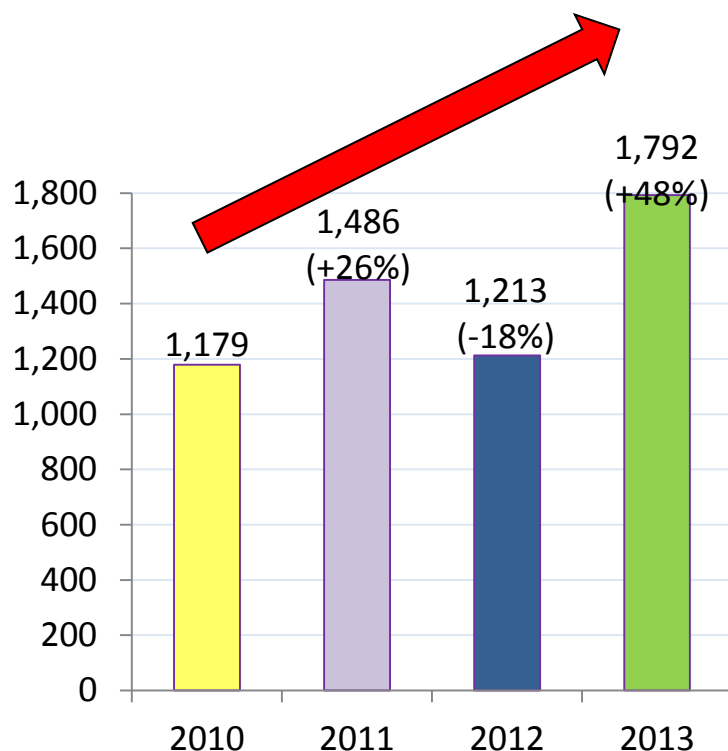
Notification requirement - Put on hold



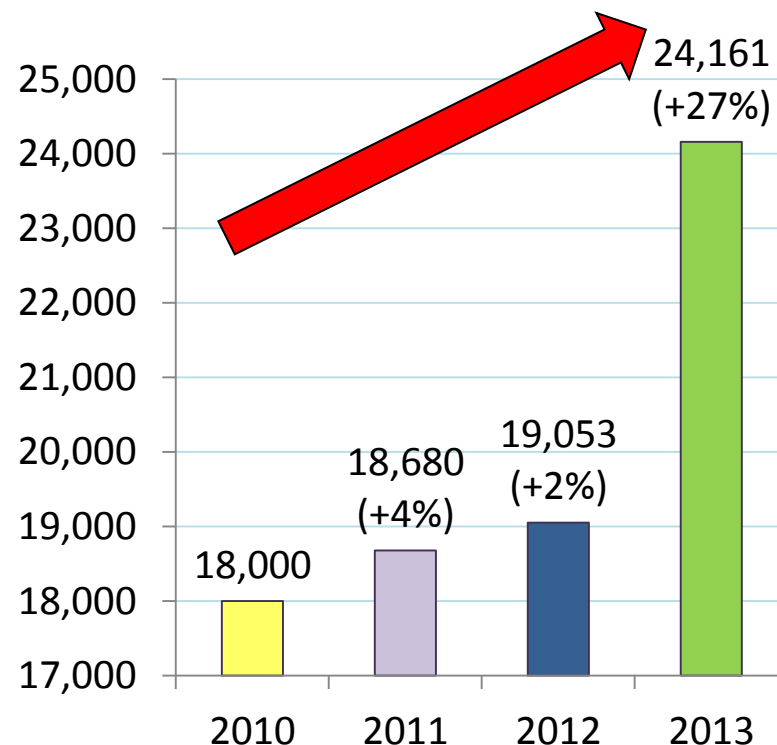


Growing public awareness of data privacy protection

Number of complaints received



Number of enquiries received





PMP

“to meet the high public expectation for protection of personal data privacy in the four sectors concerned, I have advocated to these sectors in the past 12 months to adopt a strategic shift from compliance to accountability”

- Mr Allan Chiang, Privacy Commissioner for Personal Data (January 2014)



Major organisations pledge to implement PMP

As of 18 February 2014, the following organisations pledge to implement PMP:

HKSAR
Government

25 insurance
companies

9 telecom
companies

5 organisations
from other
sectors



Something new?

Based on the Accountability principle

Accountability is not new

- OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)
- APEC Privacy Framework (2004)
- Canada's Personal Information Protection and Electronic Documents Act (2000)

PMP


- introduced in “Part Three. Implementing Accountability” of the revised OECD Guidelines (2013)
- “Getting Accountability Right with a Privacy Management Program” (April 2012) compiled by the Office of the Privacy Commissioner of Canada, and the Offices of the Information & Privacy Commissioners of Alberta and British Columbia, Canada
- “Accountable Privacy Management in BC's Public Sector” (June 2013) by Office of the Information & Privacy Commissioner for British Columbia



Privacy Management Programme: A Best Practice Guide (“BPG”)



Introduction



Embrace personal
data privacy
protection as part
of corporate
governance
responsibilities

Apply them as a
business
imperative
throughout the
organisation



Introduction (Cont')

Not a “one-size-fits-all” solution

Not constitute a Code of Practice under s.12 of the Ordinance

Not provide direct guidance for compliance with specific provisions of the Ordinance

No specific legal liability will be incurred directly



PMP – At a Glance

Part A: Baseline Fundamentals

1. Organisational Commitment

a) Buy-in from the Top	b) Data Protection Officer/ Office	c) Reporting
------------------------	---------------------------------------	--------------

2. Programme Controls



a) Personal data inventory	b) Policies	c) Risk Assessment Tools
d) Training & Education	e) Breach Handling	f) Data Processor Management
g) Communication		

Part B: Ongoing Assessment and Revision



1. Oversight & Review Plan

2. Assess & Revise Programme Controls where necessary



1) Organisational Commitment





a) Buy-in from the Top

- Top management commitment
- Top management or its delegated authority should:
 - appoint the Data Protection Officer(s) (“**DPO**”)
 - endorse the programme controls
 - report to the Board, as appropriate, on PMP

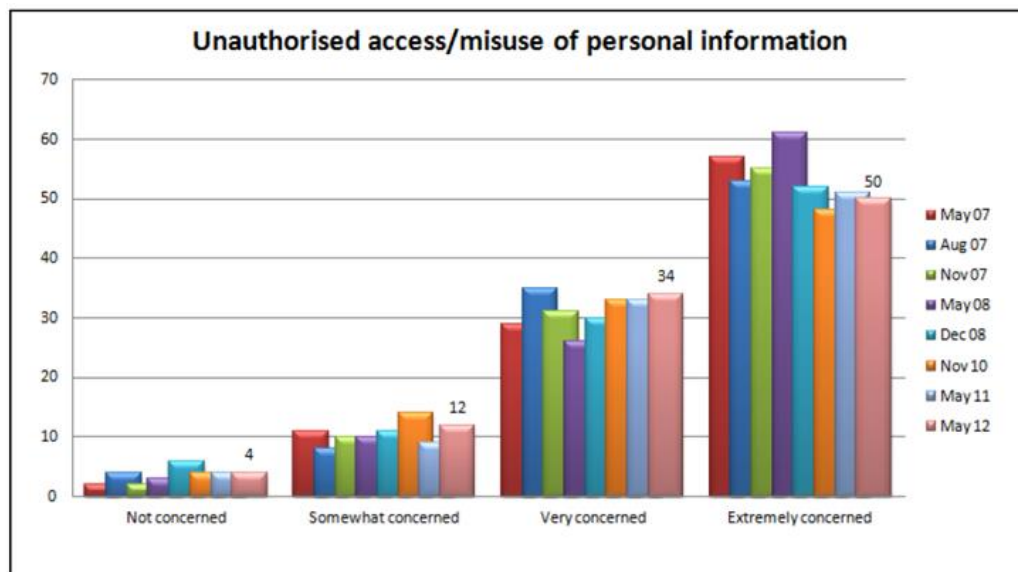


a) Buy-in from the Top - Why matters?

- Customers demand it
 - 89% of US internet users say they avoid companies that do not protect their privacy
 - 84% of HK residents are very or extremely concerned about unauthorised access to or misuse of their personal information

Source:

- <http://www.truste.com/us-consumer-confidence-index-2014/>
- Unisys





a) Buy-in from the Top - Why matters?

- Data breach hits the top and bottom line
 - Average per capita cost/breach: US\$136
 - Abnormal churn rates ranged from 2.4%-4.4%
- Reputation

Source: https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf



a) Buy-in from the Top - Example: Octopus

[Get Your Octopus](#)[Easy Reloading](#)[Earn & Redeem Reward\\$](#)[Latest Promotions](#)[Octopus for Businesses](#)[Caring for the Community](#)

[How Does It Work?](#)[Where to Earn & Redeem](#)[How Do I Join?](#)[Members' Corner](#)[Octopus Rewards Stations](#)[Member Info Update](#)

Earn and Redeem Reward\$



Reward\$ as good as cash
With Octopus Rewards, you can earn and redeem Reward\$ outlets, regardless of your payment means.

[Join Octopus Rewards now!](#)



How it works
You earn Octopus Reward\$ every time you "dood" and make any purchase at our partners. You get cash value that can be applied toward future purchases - not points!





a) Buy-in from the Top - Example: Octopus

PAST

Data Protection = Legal Compliance

Card issuer's chief executive apologises two weeks after denial

Octopus sold personal data of customers for HK\$44m

Phyllis Tsang and Ng Kang-chung

Two weeks after it denied selling the personal data of cardholders to third parties, the Octopus Card Issuer said yesterday it had made HK\$44 million in the past 4½ years by selling the data.

Making the disclosure at a special hearing conducted by the privacy commissioner, Octopus Holdings chief executive Prudence Chan Bik-wah said she wished to "sincerely apologise" to affected cardholders.

A lawmaker who has vowed to launch a Legislative Council inquiry called on her to resign.

Chan said that since the Octopus Rewards scheme - operated by two subsidiaries, Octopus Rewards and Octopus Connect - was launched 4½

years ago, it had sold the data of 1.97 million customers to its six partners in the scheme. As a result each cardholder had been contacted on average 1.7 times.

The revenue received amounted to HK\$44 million, which is 31 per cent of the HK\$140 million total revenue of the two companies combined in that period. Chan said. But taking into account investment and operating expenses the two had reported a combined loss of more than HK\$30 million, she said.

Unionist lawmaker Wong Kwok-hing, calling on Chan to step down, said: "Obviously, what she says now contradicts what she said earlier this month in a press conference her company convened."

"Cheating the public is a very serious

matter and the legislature must not just sit back."

Wong said the privacy commissioner's investigation focused only on privacy concerns. "For the Legislative Council, we shall look into the sale of Hong Kong people's personal data by a company that is controlled by a public utility."

Wong said it was not a criminal offence for Octopus to sell the personal information of customers without their consent, but customers could consider suing the company for compensation in civil proceedings.

According to the Personal Data (Privacy) Ordinance any person who obstructs, hinders or resists the privacy commissioner in performing his function, or makes a false statement to mislead the commissioner, com-

mits an offence subject to a maximum penalty of a HK\$10,000 fine and six months' imprisonment.

Chan said at a press conference on July 7 that the company did not sell the data and did not pass on clients' data without their permission, which was obtained when they signed up for the rewards scheme.

Yesterday, she was asked by Wilson Lee, principal investigator of the Office of the Privacy Commissioner, whether the company had passed the credit card numbers of cardholders to one of its partners, Card Protection Plan (CPI). She replied only that no customers had given permission for this to be done before 2005.

Octopus Cards is wholly owned by Octopus Holdings, whose

• CONTINUED ON A2

Cheating the public is a very serious matter and the legislature must not just sit back

Lawmaker Wong Kwok-hing calls on Prudence Chan to quit

SCMP (27 July 2014)



於法有據
但於情不合

By courtesy of South China Morning Post



a) Buy-in from the Top - Example: Octopus

NOW

“Our Rule of Thumb

Organisational commitment – top-down directives and bottom-up processes

*We need to do **not just legal, but what is right**”*

Presentation by Mr Sunny CHEUNG, CEO, Octopus Holdings Limited, Hong Kong
(2014)

Source: http://www.pcpd.org.hk/privacyconference2014/files/10_cheung_presentation.pdf



a) Buy-in from the Top - Example: Microsoft

- Memo from Bill Gates to employees worldwide (2002)
 - The company's highest priority was *"building trust into every one of our products and services"*
 - Privacy would be a key pillar of Trustworthy Computing initiative
- Chief privacy officer was appointed back in early 2000
- Single internal Microsoft Privacy Standard to help employees integrate privacy and safety into all parts of Microsoft's business

Source: <http://www.microsoft.com/en-us/news/features/2012/jan12/gatesmemo.aspx>



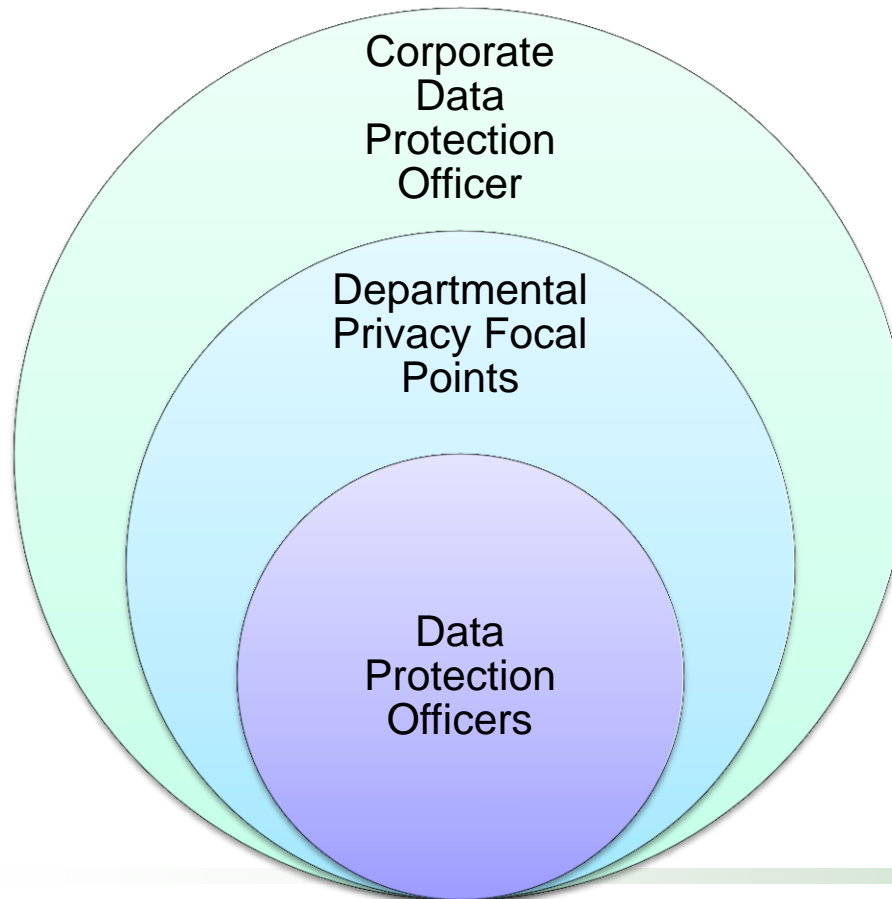
b) Data Protection Officer/Office

- **Role**
 - Establish and implement programme controls
 - Coordinate with other appropriate persons responsible for related disciplines and functions within the organisation
 - Be responsible for the ongoing assessment and revision of programme controls
 - Represent the organisation in the event of an enquiry, an inspection or an investigation by the Commissioner
 - Advocate personal data protection within the organisation itself
- May or may not be a full-time job
- May be supported by dedicated staff (Data Protection Office)



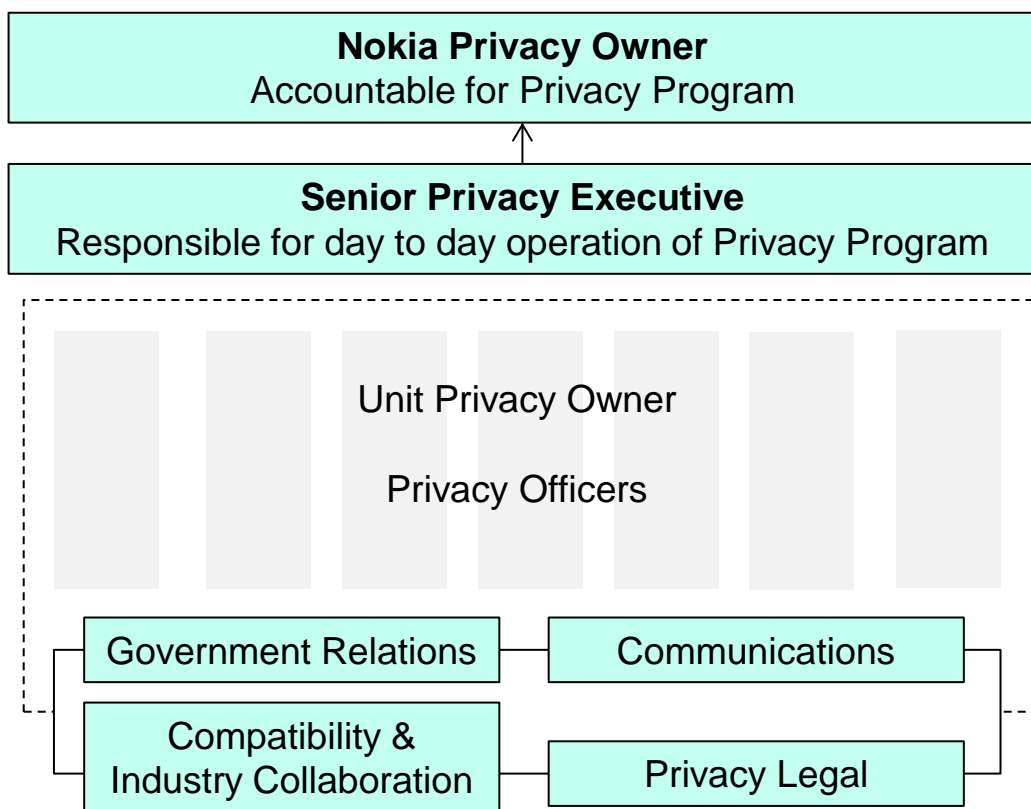
b) Data Protection Officer/Office - Example: CLP

CLP's data protection governance structure





b) Data Protection Officer/Office - Example: Nokia



Nokia Privacy Owner: Ultimate accountability

Senior Privacy Executive: Responsible for day to day operation of Nokia's Privacy Program

Unit Privacy Owners: Accountable for deploying the programme into the Unit

Privacy Officer: Operational privacy expert responsible for proactive privacy work

Global Privacy Counsel: Responsible for privacy legal support across Nokia

Training and Awareness Officer: Develops, drives and oversees training and awareness building

Privacy Leadership Team: Led by Senior Privacy Executive, and consisting of Unit Privacy Owners, Global Privacy Counsel & Industry and Regulatory representatives

Source: http://www.pcpd.org.hk/privacyconference2014/files/6_niva_presentation.pdf



c) Reporting

- Ensure the right people know how PMP is structured and whether it is functioning properly
- Establish internal audit/assurance programmes, e.g.:
 - Customer and employee feedback
 - Third-party verification

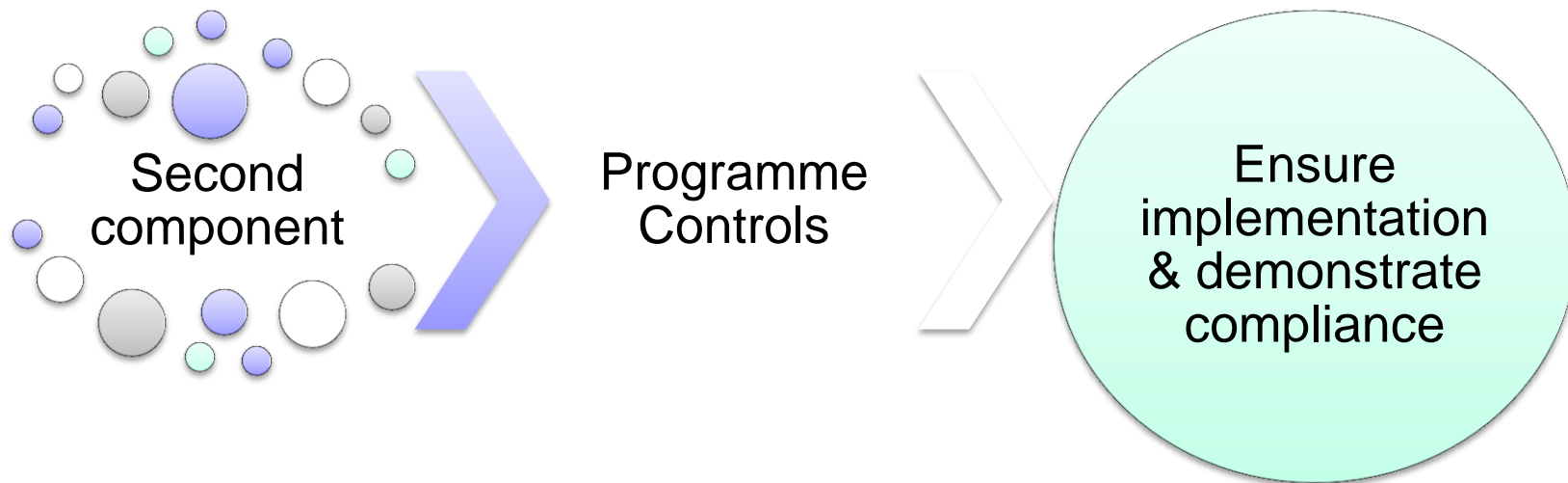


c) Reporting

- Define and explain to employees how and when to escalate a personal data issue
- An effective reporting programme:
 - clearly defines its reporting structure on compliance activities, in the event of a complaint or breach
 - tests and reports on the results of its internal reporting structures
 - documents all its reporting structures



2) Programme Controls





a) Personal Data Inventory

Every organisation should

- be clear about:
 - what kinds of personal data it holds
 - where it is held
 - why it is collecting, using or disclosing personal data
- and document the above



a) Personal Data Inventory

- What kinds of personal data?

Customers

- Name
- Contact information (address, phone number, email, etc.)
- Purchase history
- Voice recording of telephone calls
- Etc.

Employee

- Name
- Gender
- Contact information
- HKID copy
- Salary
- Job title
- Medical benefits and MPF
- Appraisal



a) Personal Data Inventory - Where it is held?

- Within the organisation?
- Who is the owner?
- Held by a data processor?



a) Personal Data Inventory

- Why it is collecting, using or disclosing?

Consumers

- Provision of services
- Marketing
- Complaint/enquiries handling
- Processing application
- Open / Maintain / Terminate an account
- Conduct customer survey / research and perform statistical analysis
- Legal proceedings, including collecting overdue amounts

Employee

- Recruitment and HR management:
 - appointment
 - employment benefits
 - termination
 - performance appraisal
 - discipline
- Administration
- Tax



a) Personal Data Inventory - Benefits

- Decide the type of consent required
- Decide how the data is protected
- Easier to meet data access & correction obligations

Tips:

- Maintain documentation on the consent required under Part 6A of the Ordinance is important when facing complaint / enquiry raised by the data subjects



b) Policies

Policies should cover 6 Data Protection Principles

DPP1: Collection of personal data

DPP2: Accuracy and retention of personal data

DPP3: Use of personal data including the requirements for consent

DPP4: Security of personal data

DPP5: Transparency of organisations' personal data policies and practices ("Privacy Policy Statement")

DPP6: Access to and correction of personal data



b) Policies

- Personal data compliance requirements should also be incorporated in other policies, e.g.
 - contract management policies
 - procurement policies
 - human resources policies
 - policies dealing with the disclosure of personal data to regulatory bodies, law enforcement agencies and other government bodies
- Documented in writing
- Readily available to internal staff



c) Risk Assessment Tools

When to conduct a risk assessment?

- Periodically
- Where there is material change to regulatory requirements relating to personal data
- Before any material change to the data user's existing personal data process
- Before introducing any new personal data process



c) Risk Assessment Tools

What may be considered as a material change?

- New types of personal data will be collected
- Significant changes will be made in the way personal data is used or disclosed
- System access is being changed so that new groups of individuals will be access to personal data
- Management or security of personal data will be outsourced to a service provider
- Retention period for personal data will be changed



c) Risk Assessment Tools - Privacy Impact Assessment

PIA

- Evaluate a proposal in term of its impact upon personal data privacy

Objective

- Avoid or minimise adverse impact

Generally include:

- Data processing cycle analysis
- Privacy risks analysis
- Avoiding or mitigating privacy risks
- Reporting



Privacy Impact Assessment - Resources

- PCPD's Information Leaflet – Privacy Impact Assessments
(http://www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf)
- Information Commissioner's Office (UK) – Privacy Impact Assessment Handbook
(http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf)
- Office of the Australian Information Commissioner – Privacy Impact Assessment Guide
(http://www.oaic.gov.au/images/documents/migrated/oaic/repository/publications/guidelines/Privacy_Impact_Assessment_Guide.pdf)
- Privacy Commissioner (NZ) – Privacy Impact Assessment Handbook
(<http://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf>)



c) Risk Assessment Tools - Privacy assessment/audit

- Review of an organisation's compliance with its privacy policies and procedures, and requirements under the Ordinance
- May rely on
 - subjective information, such as employee interviews/questionnaires, complaints received, or
 - Objective standards, such as information system logs, training attendance and test score
- Can be conducted internally or externally by third parties

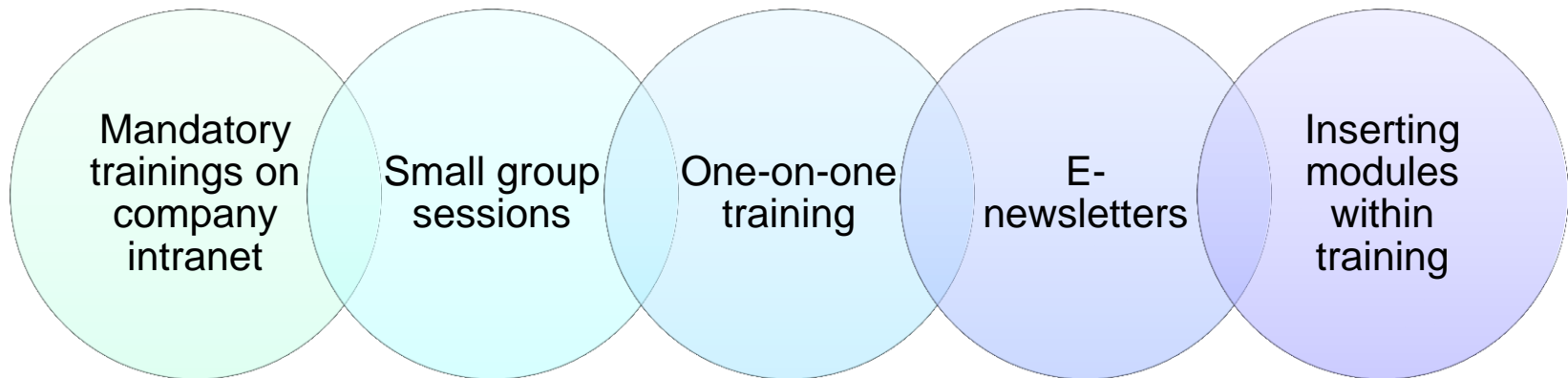


d) Training and Education

- Tailored to specific needs of all relevant employees (i.e. those handling personal data)
- Be given to new employees in its induction programme and periodically thereafter
- Cover organisation's policies and procedures
- Be delivered in an appropriate and effective manner
- Circulate essential information to relevant employees as soon as practical if an urgent need arises
- Monitor attendance



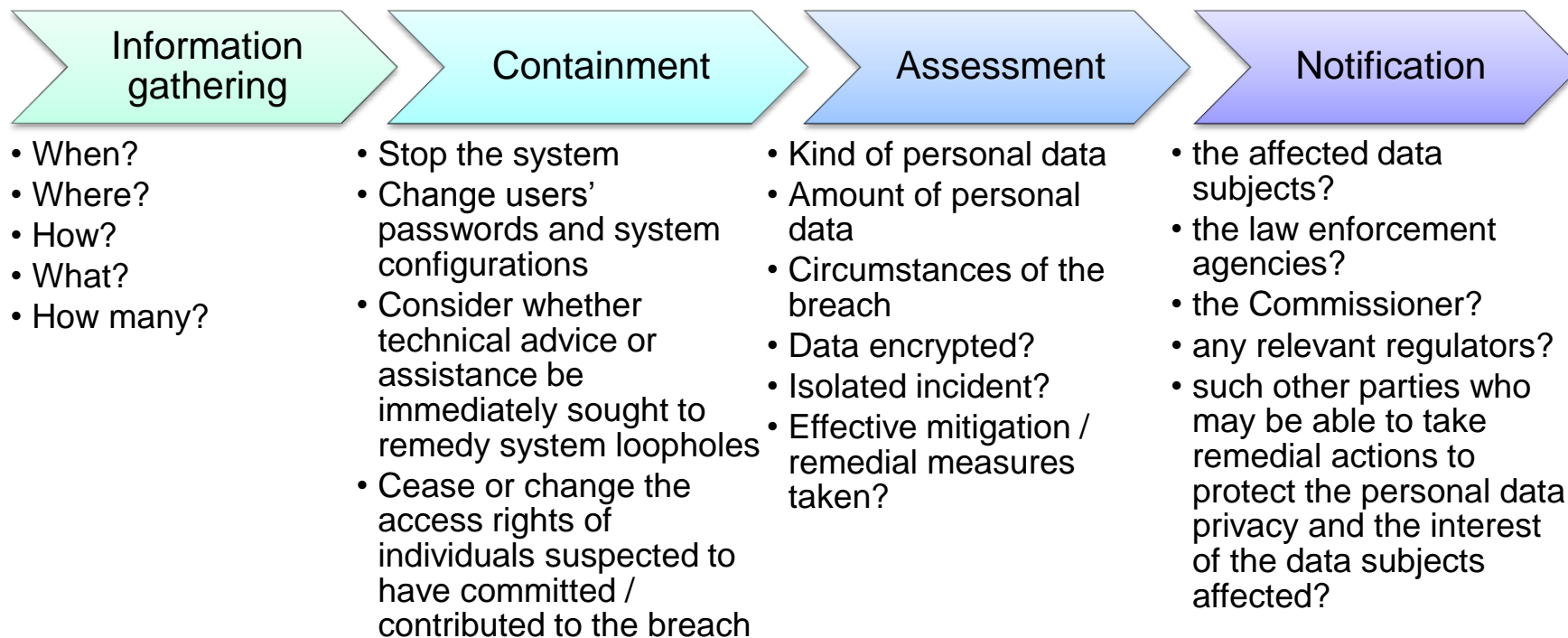
d) Training and Education - Various ways





e) Breach Handling

- Breach handling procedure in place



- Designate an officer/a team to manage a breach



f) Data Processor Management

- Data processor:
“a person who
 - (a) processes personal data on behalf of another person; and*
 - (b) does not process the data for any of the person’s own purposes”*
- Must adopt contractual or any other means to prevent
 - personal data transferred to the data processor from being kept longer than is necessary for processing of the data (DPP2(3))
 - Unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (DPP4(2))



f) Data Processor Management

Obligations to be imposed on data processor by contract

- Security measures to be taken by the data processor
- Timely return, destruction or deletion of the personal data no longer required
- Prohibition against other use and disclosure
- Prohibition (absolute or qualified) against sub-contracting to other service provider
- Reporting of irregularity
- Measures to ensure contract staff's compliance with the agreed obligations

Through other non-contractual means

- Select reputable data processors
- Data processors have robust policies and procedures in place
- Data users have the right to audit and inspect



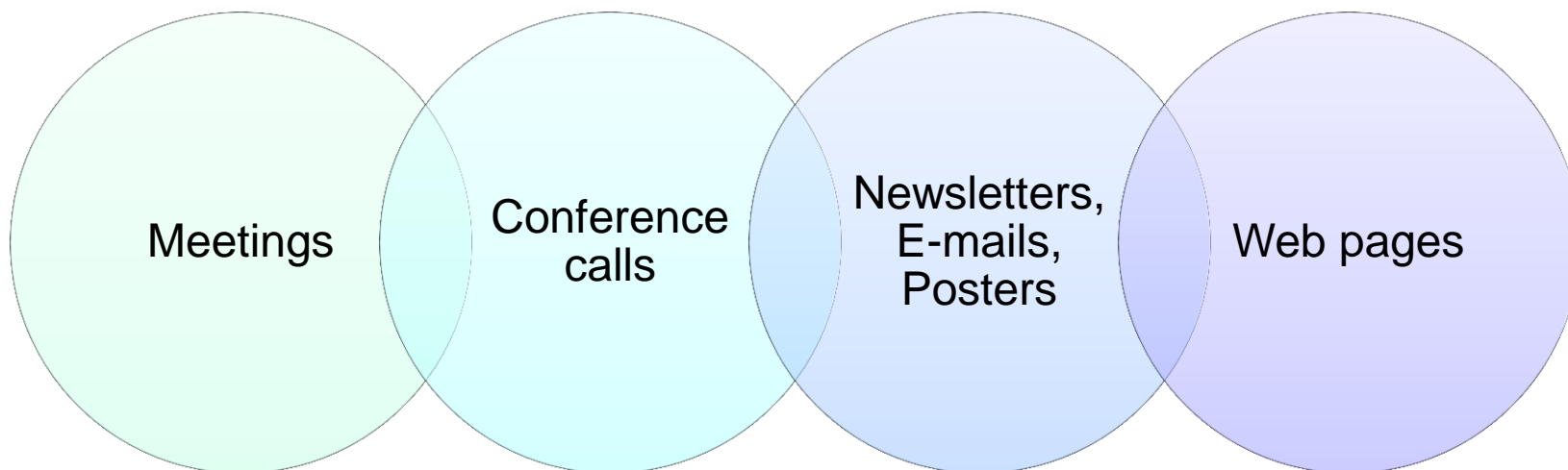
g) Communication

Communication should:

- be clear and easily understandable
- not be simply a reiteration of the Ordinance
- provide enough information on:
 - purpose of collection, use and disclosure of personal data
 - how long it is retained
 - who to contact with questions or concerns
- be easily available



g) Communication





1. Develop an Oversight & Review Plan

- Developed by DPO/Data Protection Office
- On a periodic basis
- Set out how the effectiveness of the organisation's programme controls will be monitored and assessed



2. Assess & Revise Programme Controls

Where necessary,

- Update personal data inventory
- Revise policies
- Treat risk assessment tools as evergreen
- Update training and education
- Adapt breach and incident response protocols
- Fine-tune data processor management
- Improve communication



Key steps to setting up a PMP



Key Steps

Structure the team



Establish the baseline



Plan



Implement



Structure the Team

- Appoint a project lead with sufficient privacy knowledge and authority to manage the project and assess the findings
- Ensure oversight by the management through the project lead
- Involve HR, risk management, internal audit and IT personnel if necessary
- Obtain outside privacy expertise if necessary



Establish the Baseline

- Use BPG as a checklist to evaluate if the components exist
- Obtain and document information to assess current situation, may include:
 - Staff interviews
 - File reviews
 - Policy reviews

Baseline Fundamentals	In place?
Buy-in from the Top	
Data Protection Officer/Office	
Reporting	
Personal Data Inventory	
Policies	
Risk Assessment Tools	
Training & Education Requirements	
Breach Handling	
Data Processor Management	
Communication	



Plan

- Determine what steps need to be taken in order to move from its current state to its desired, future state (Gap Analysis)
 - Core/elective activities
 - Responsible parties
- Determine timeline
- Determine sequence

Source: http://www.pcpd.org.hk/privacyconference2014/files/9_neumann_presentation.pdf



Implement

- Put the activities in place
 - Resources
 - Communicate
 - Execute

Source: http://www.pcpd.org.hk/privacyconference2014/files/9_neumann_presentation.pdf



Ongoing review

- PMP – Not a finished product
- Require ongoing assessment and revision in order to be effective and relevant

Refinements	Updated?
Update personal data inventory	
Revise policies	
Treat risk assessment tools as evergreen	
Update training and education	
Adapt breach and incident response protocols	
Fine-tune data processor management	
Improve communication	



Tool: Privacy Maturity Model (“PMM”)

AICPA/CICA PMM:

- an example of a well-known model used for over 20 years
- can be used to measure progress against established benchmarks
- can be used as the basis for reporting on the status of the organisation’s PMP

Source: <http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/item47888.aspx>

Five maturity level

1. ad hoc	• procedures or processes are generally informal, incomplete and inconsistently applied
2. repeatable	• procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects
3. defined	• procedures and processes are fully documented and implemented, and cover all relevant aspects
4. managed	• reviews are conducted to assess the effectiveness of the controls in place
5. optimized	• regular review and feedback are used to ensure continuous improvement towards optimization of the given process



PMM Reporting

Figure 1 - Privacy Maturity Report by GAPP Principle

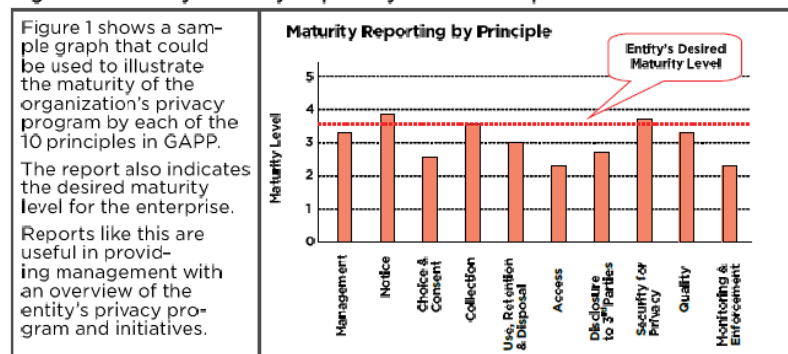


Figure 2 - Maturity Report by Criteria within a Specific GAPP Principle

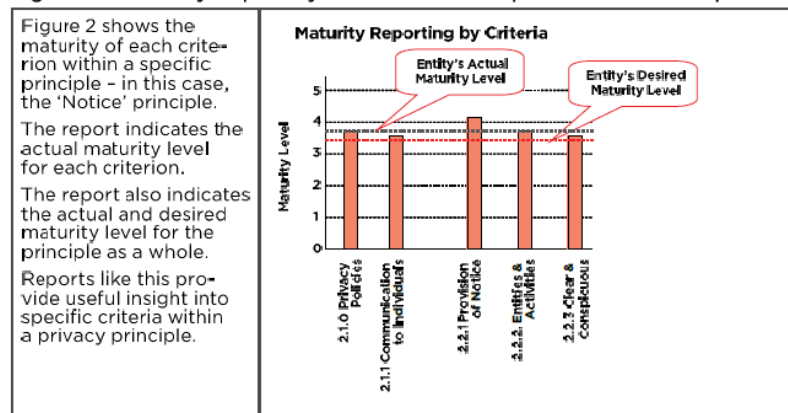
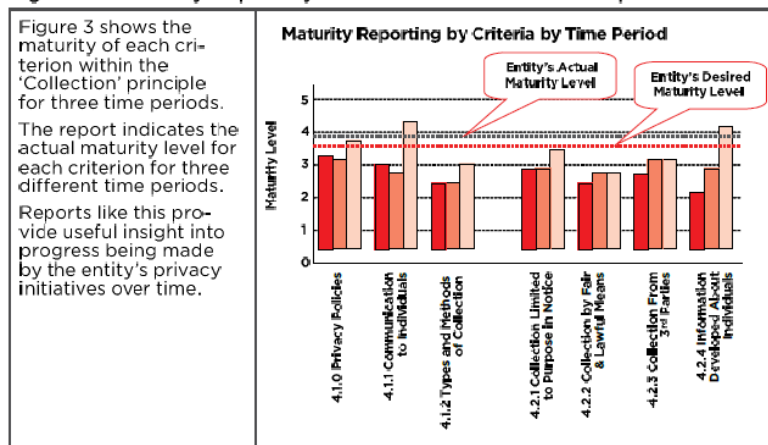


Figure 3 - Maturity Report by Criteria within a GAPP Principle Over Time





Tool: Scorecard

Nymity Data Privacy Accountability Scorecard (Excel based):

- Identify Core and Elective activities
- Create evidence collection questions
- Collect response to the questions
- Calculate score
 - $\% \text{ managed} = \# \text{ of core activities evidenced} \div \# \text{ of core activities}$
 - $\% \text{ advanced} = \# \text{ of elective activities evidenced} \div \# \text{ of elective activities}$
- Update scorecard periodically

Source:

<http://www.scorecard.nymity.com>,

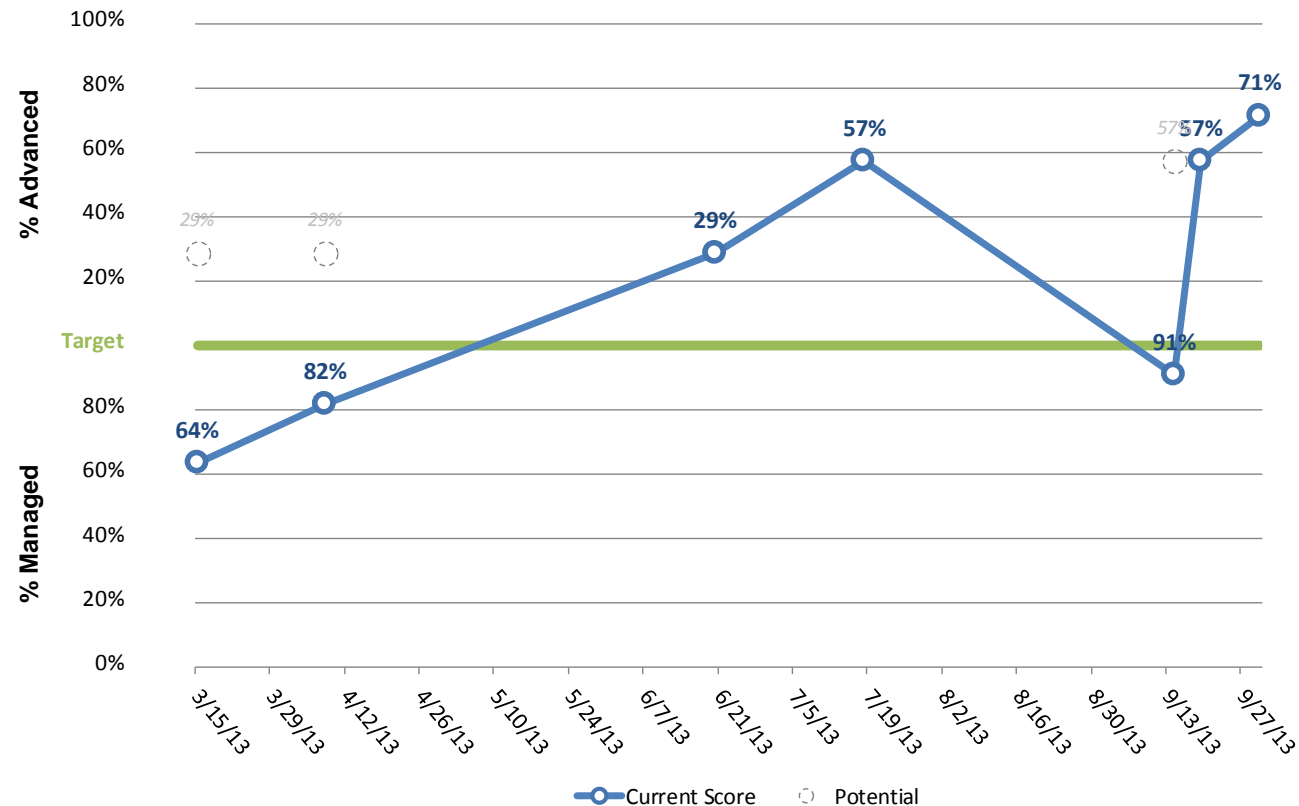
http://www.pcpd.org.hk/privacyconference2014/files/9_booklet_guide.pdf



Scorecard Reporting

NYMITY Data Privacy Accountability Scorecard™

www.scorecard.nymity.com





Thank you!