



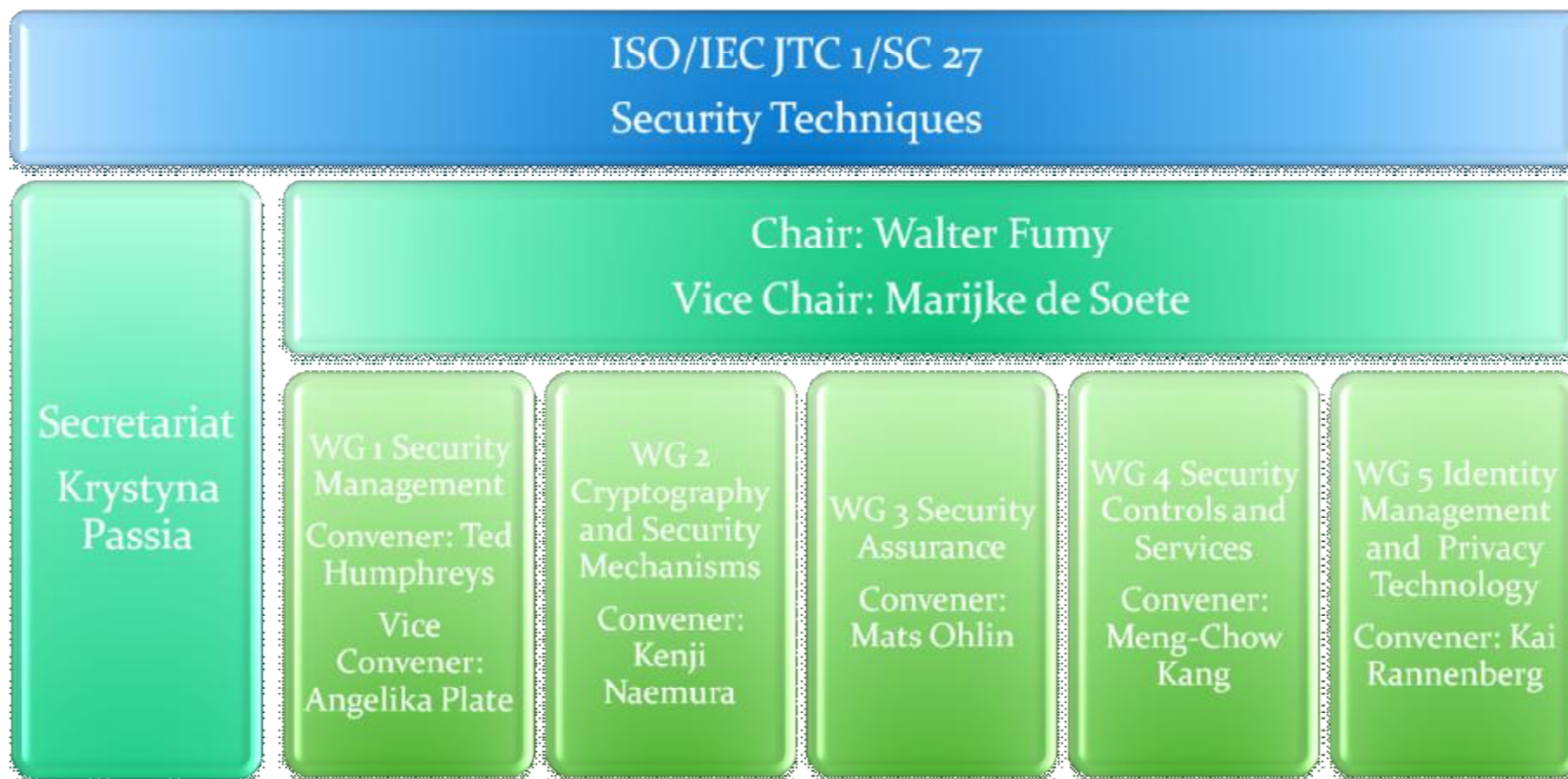
# ISO國際資訊安全標準現況

簡報人：資策會 劉培文副處長



# ISO JTC1 SC27架構

B





# ISO JTC1 SC27 WG1現況

- ISO 27000系列標準
  - *ISO/IEC 27000 – Overview and vocabulary (Final Committee Draft)*
  - *ISO/IEC 27001:2006 – ISMS requirements;*
  - *ISO/IEC 27002:2005 – Code of practice for information security management;*
  - *ISO/IEC 27003 – ISMS implementation guidance (Final Draft International Standard);*
  - *ISO/IEC 27004 – Information security management measurements (Final Committee Draft);*
  - *ISO/IEC 27005:2008 – Information security risk management;*
  - *ISO/IEC 27006:2007 – Accreditation requirements;*
  - *ISO/IEC 27007 – ISMS auditing guidance (Working Draft);*
  - *ISO/IEC 27011:2008 (ITU-T X.1051) – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*



# ISO JTC1 SC27 WG1 現況

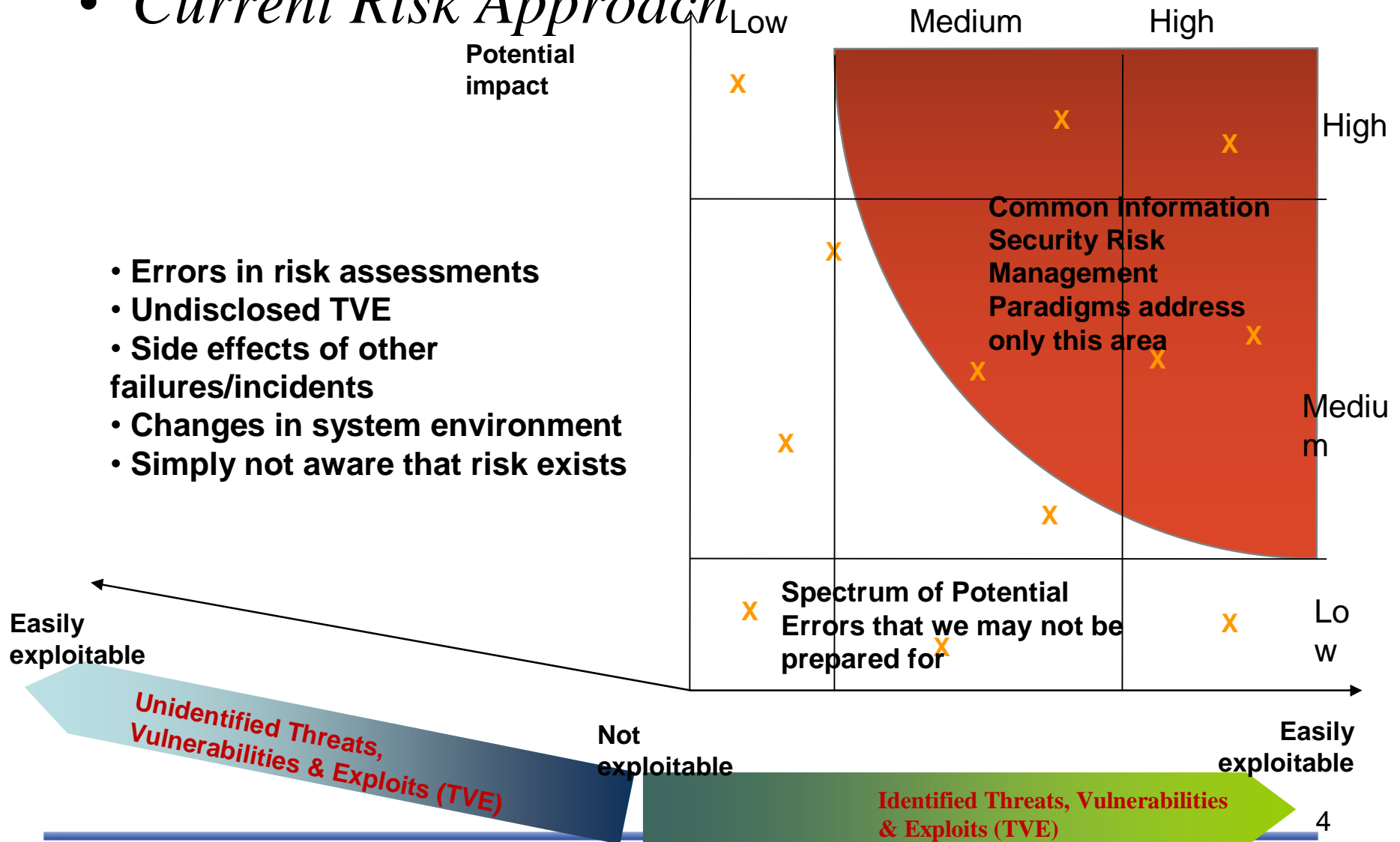
- 新的研究項目及專案建議
  - 資訊安全治理
    - *Information security governance (Study Period)*
  - 特定產業之資訊安全管理體系標準-- 世界彩券協會
    - *Sector-Specific ISMS Standards for the World Lottery Association (Study Period)*
  - 特定產業之資訊安全指引 -- 關鍵基礎建設
    - *Information security for Critical Infrastructure – Sector-specific guidance (Study Period)*
  - 電子化政府資訊安全管理指引
    - *ISM guidelines for e-government services (New work item proposal)*
  - 資訊安全管理：跨政府與產業互動及交流
    - *Information security management: sector to sector interworking and communications for industry and government (New work item proposal)*。詳細資料請參考附件文件 N6620rev1。
  - 稽核員資訊安全管理控制
    - *Guidance for auditors on ISMS controls (New work item proposal)*。



# ISO JTC1 SC27 WG4現況

## • Current Risk Approach

- Errors in risk assessments
- Undisclosed TVE
- Side effects of other failures/incidents
- Changes in system environment
- Simply not aware that risk exists

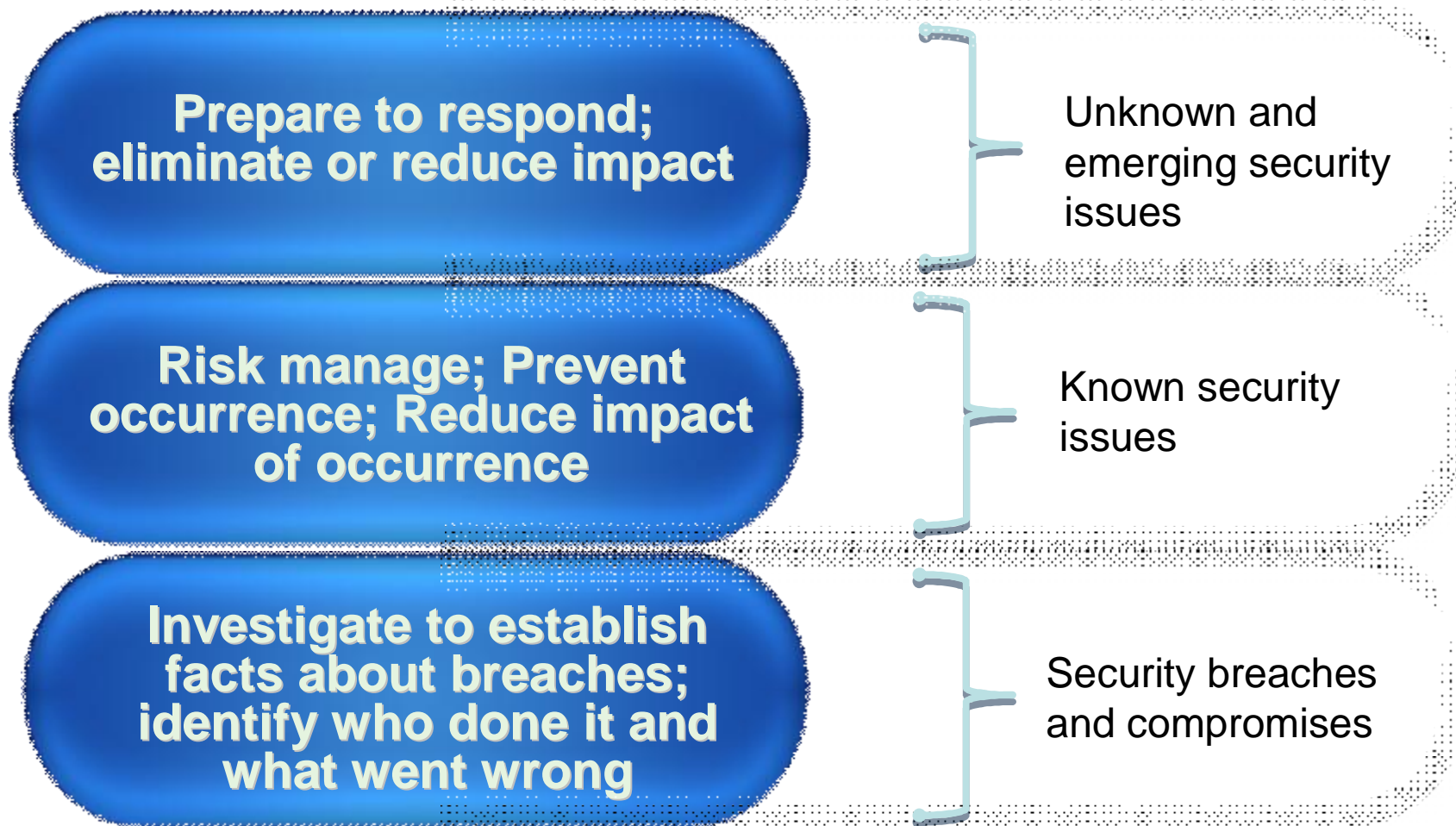




# ISO JTC1 SC27 WG4現況

B

- *Roadmap Framework*



5



# ISO JTC1 SC27 WG4現況

- *Standards for Unknown and emerging security issues*
  - **ISO/IEC 27031 – Guidelines for ICT readiness for Business Continuity (Working Draft);**
  - *ISO/IEC 24762:2008 – Guidelines for ICT disaster recovery services;*
  - *ISO/IEC 18043:2006 – Selection, deployment and operations of intrusion detection systems (IDS);*
  - *ISO/IEC TR 18044:2002 – Information security incident management. In the April 2008 meeting, the working group has further proposed that this technical report be revised and elevated to become an IS; and*
  - **ISO/IEC 27032 – Guidelines for cybersecurity (Working Draft)**



# ISO JTC1 SC27 WG4現況

- *Standards for Known security issues*
  - *ISO/IEC 18028:2005/6 – Network Security (parts 1 to 5)*, 此標準目前正在修改，未來會公布為*ISO/IEC 27033 (parts 1 to 7)*標準
  - *ISO/IEC 27034 – Application security*，此標準係由組織使用者的觀點來看應用程式之安全管理需求
  - *ISO/IEC TR 14516 (ITU-T X.842) – Guidelines on use and management of Trusted Third Party services (TTP)*
  - *ISO/IEC 15945 (ITU-T X.843) – Specification of TTP services to support the application of digital signatures*
  - *ISO/IEC 15816 (ITU-T X.841) – Security information objects for access control*
  - *ISO/IEC TR 29149 – Best practice on the provision of time-stamping services (new project starting in Oct 2008)*



# ISO JTC1 SC27 WG4現況

- *Standards for Security Breaches and compromises*
  - 目前此WG 4在這個方面還沒有特定的標準制定工作在進行。僅有馬來西亞National Body正在針對「數位鑑識證據收集程序」進行為期六個月的之研究



# ISO JTC1 SC27 WG4現況

B

## ICT Readiness for Business Continuity (27031)

Reference to ISO/IEC 24762, Vulnerability Mgmt, IDS, & Incident Response related standards

## Cybersecurity (27032)

Anti-Spyware, Anti-SPAM, Anti-Phishing, Cybersecurity-event coordination & information sharing

## Network Security (27033)

ISO 18028 revision; WD for new Part 1, 2, 3, & 4.; New Study Period on Incident Categorization & Classification

## Application Security (27034)

WD for Part 1

## TTP Services Security

New Study Period proposed; Includes outsourcing and off-shoring security

## Forensic Investigation

New Study Period on Evidence Collection & Digital Forensic

9



# ISO JTC1 SC27 WG4現況

- *ISO/IEC 27032 – Guidelines for Cybersecurity (Working Draft)*
  5. *Overview*
    - *Information Security, Network Security, Internet Security, CIIP, Cybersecurity*
  6. *Roles of Users, Organizations, and Service Providers in Cybersecurity*
  7. *Countermeasures against Social Engineering Attack*
  8. *Framework of Information Sharing and Coordination*
  9. *Cybersecurity Readiness*
    - *9.1 Darknet Monitoring*
    - *9.2 Sinkhole Operation*
    - *9.3 Traceback*



# 結論

- *ISO/IEC 27000* 系列標準除27007前還在工作小組草擬階段外，其他都已進入*FCD*或*FDIS*，未來數月內將陸續正式公布，代表27000系列的標準已漸趨成熟。由*WG 1*目前的發展來看，27000系列的標準將偏重技術稽核之作法及特定產業之實作指引
- *ISO JTC 1/SC 27/WG 4*之發展方向已經可以看出大致之輪廓，主要是由*ISO/IEC 27031*到27034之相關標準組成。其中*ISO/IEC 27032*網際空間安全標準之編輯之一為*RAISE*之共同主席*Koji Nakao*，其中相當多之內容均是在*RAISE*會議中討論之議題。
- 我國可透過*RAISE*參與*ISO SC27*資安相關標準之制定，尤其是對*WG4*之研究計畫及標準撰擬之影響