國際新知

●最新個人資訊管理系統（PIMS）國際標準

勞動部資訊處副處長 黃國裕

壹、前言

國內各級政府機關已普遍採用 ISO 27001 標準，作為機關資訊安全管理系統（Information Security Management System, ISMS）的認定標準，其公信力已獲得世界各國普遍認可。然而，國際標準組織（International Organization for Standardization, ISO）最新推動的一系列的個人資料保護與管理標準，尚未被各國普遍應用。本文將說明如何應用 ISO 國際標準來推動個人資料保護與管理，實作隱私衝擊評鑑方法，進而實施國際間廣泛認可的個人資訊管理系統（Personal Information Management System, PIMS）驗證（本文所參考的 ISO 國際標準代號標題與現況，詳見表 1）。當您面臨個資管理標準的抉擇時，ISO 個資管理標準將會是您的選項之一。

表 1：ISO 國際標準代號與現況

ISO 標準代號	標題	現況
27000	資訊安全管理系統概述與詞彙 ISMS-Overview and vocabulary	已公布 2018（v5）、CNS、2016（v3）
27001	資訊安全管理系統—要求事項 ISMS-Requirements	已公布 2013（v2）、CNS、2014（v2）
27002	資訊安全管理之作業規範（實務） Code of practice for information security controls	已公布 2013（v2）、CNS、2015（v2）
27005	資訊安全風險管理 Information security risk management（ISRM）	已公布 2011（v2）、改版中 DIS、CNS、2013（v2）
27006	資訊安全管理系統稽核與驗證—要求事項 Requirements for bodies providing audit and certification of ISMS	已公布 2015（v2）
27009	特定領域應用 ISO 27001 -要求事項 Sector-specific application of ISO 27001 -- Requirements	已公布 2016（v1）、改版中 NP

ISO 標準代號	標題	現況
27018	雲端運算之公共雲中作為個人可識別資訊處理者保護個人可識別資訊擴增的資訊安全控制措施 Code of practice for protection of personally identifiable information （PII） in public clouds acting as PII processors	已公布 2014（v1）、CNS、2016（v1）
27550	隱私工程 Privacy engineering	CD
27552	加強 ISO 27001 的隱私管理 – 要求 Enhancement to ISO 27001 for privacy management -- Requirements	CD
29100	隱私權框架 Privacy framework	已公布（v1）2011、CNS、2014（v1）
29101	隱私權架構框架 Privacy architecture framework	已公布（v1）2013、CNS、2017（v1）
29134	隱私衝擊評鑑指引 Guidelines for privacy impact assessment	已公布（v1）2017
29151	個人可識別資訊保護實務 Code of practice for personally identifiable information protection	已公布（v1）2017
29184	線上隱私告知與同意指引 Guidelines for online privacy notices and consent	CD
29190	隱私能力評鑑模型 Privacy capability assessment model	已公布（v1）2015
29191	部分匿名及部分去連結鑑別之要求事項 Requirements for partially anonymous, partially unlinkable authentication.	已公布（v1）2012、CNS、2015（v1）
20889	隱私增強資料去識別化技術 Privacy enhancing data de-identification techniques	DIS

貳、ISO 有關個人資料保護與管理的國際標準發展

ISO 自 2011 年發展出 ISO 29100 隱私權框架後，已陸續發展出 ISO 29191 部分匿名及部分去連結鑑別之要求事項、ISO 29101 隱私權架構框架（Privacy architecture framework），並於 2017 年發展出全球首項適用於一般組織的隱私衝擊評鑑的國際標準「ISO 29134：隱私衝擊評鑑指引」，以及適用於所有類型組織的個資保護控制措施的國際標準「ISO 29151：個人可識別資訊保護實務」，前述標準均可進行特定領域（sector-Specific）的延伸驗證。之後並持續發展相關國際標準，如：ISO 27552 Enhancement to ISO 27001 for privacy management – Requirements，就是因應國際間的個資管理需求（如：歐盟 GDPR[1]）而生（如圖 1）。

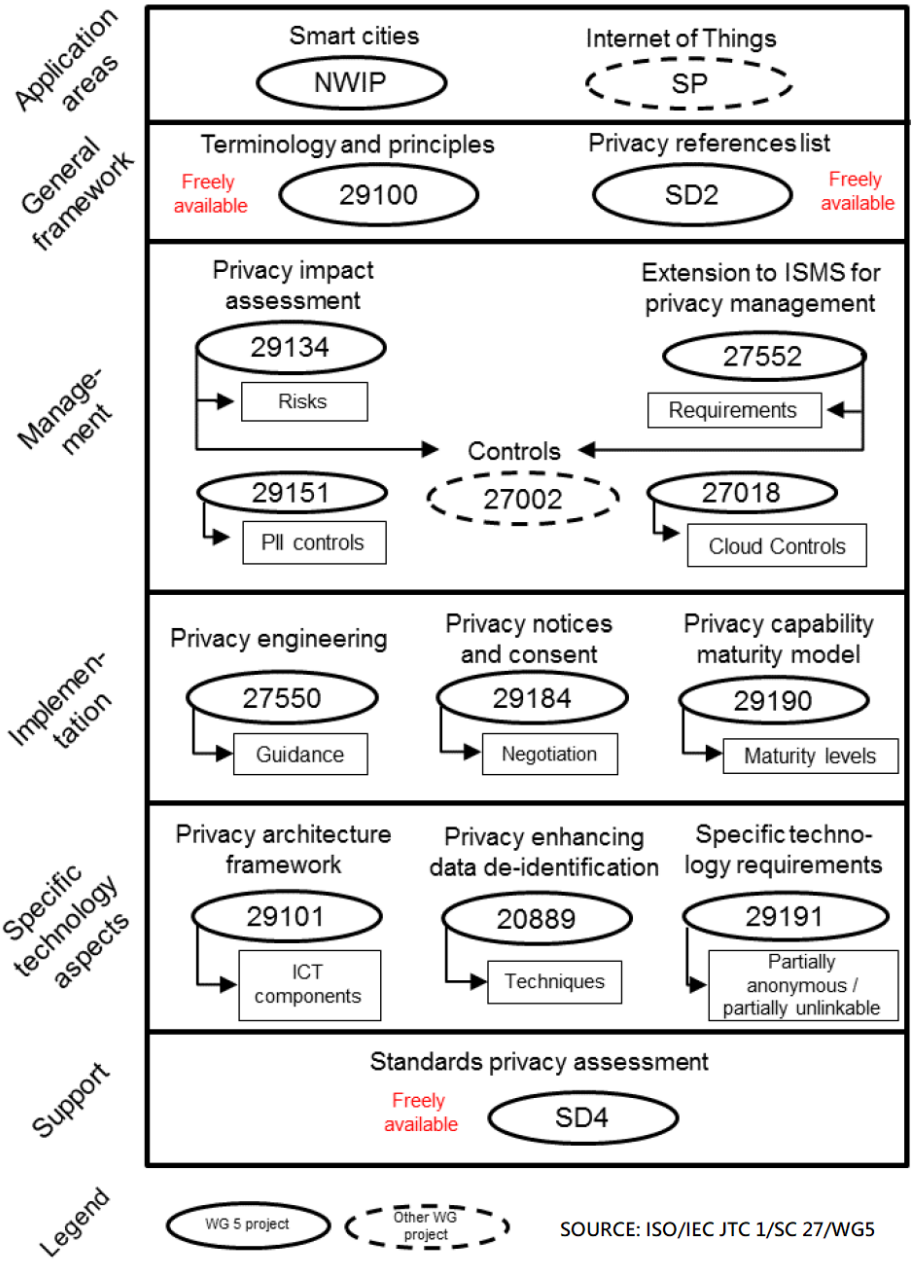

圖 1：ISO 推動的個人資訊保護與管理國際標準

[1] General Data Protection Regulation，歐盟資料保護規範。

參、ISO 對 PIMS 與 ISMS 結合的建議

為利於各類型組織將個人資料保護與管理與組織內的 ISMS 整合，ISO 建議以 ISO 27001 及 ISO 29100 為基礎，建立一套個人資訊管理系統，以共同使用單一管理系統，其中資訊安全風險的識別與管理採用 ISO 27005（可與 ISO 31000 互相校準）、個人資訊隱私風險評鑑則加入 ISO29134 隱私衝擊評鑑指引、風險處理選用 ISO 27002（資訊安全）及 ISO 29151（個資保護）的控制措施與實作指引，以符合組織的風險接受準則（如圖 2）。若組織有特別的考量，ISMS 與 PIMS 仍可個別存在運行，但可使用共同的方法並相互連結。

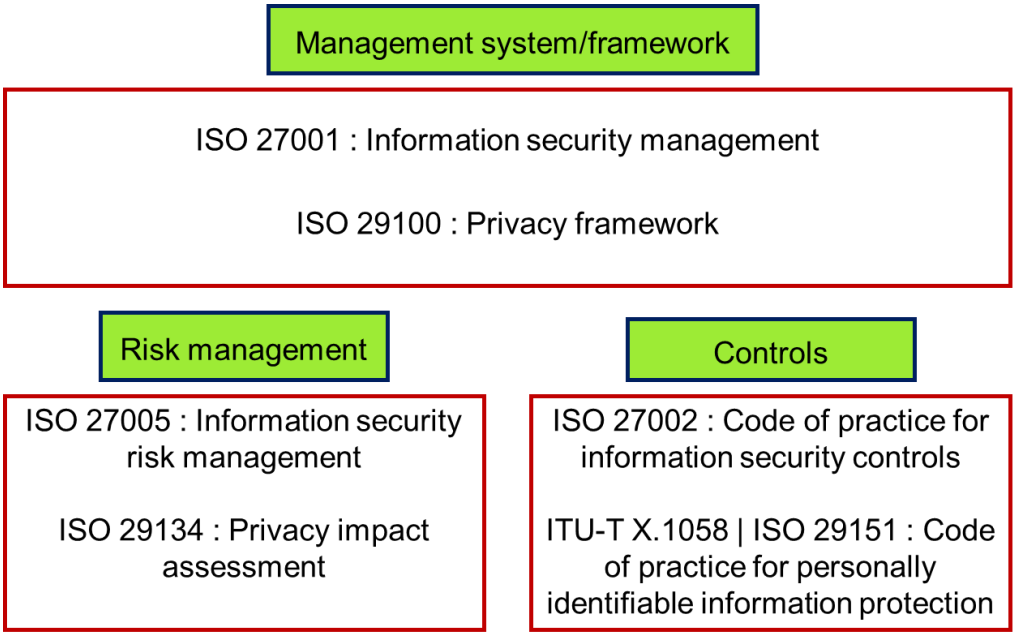

圖 2：個人資訊管理系統的架構

肆、PIMS 的驗證機制

關於 PIMS 的驗證機制，ISO 建議是以 ISO 27001 延伸驗證的方式實施，ISO 27001 延伸驗證除了補強原先 ISO 27001+ISO27002 的不足外（如圖 3），亦可有效加強組織對於資訊安全實作的深度及廣度（如圖 4）。ISO 27001 延伸驗證依據 ISO 27009 Sector-specific application of ISO 27001-Requirements 特定領域應用 ISO 27001 的要求，PIMS 的驗證即為個人資料特定領域（PIMS-Specific）的延伸驗證。

ISO 27001:2013 標準附錄 A 中，所列各項控制目標及控制措施並未完全列出有關個人資料保護部分，確實需要額外之控制目標及控制措施。因此，ISO 以 ISO 29151 標準識別個人資料風險及其對應個人資料保護的控制措施。另外，在 ISO 27006:2015 標準有關 ISMS 驗證機構認證規範中也已揭示經鑑別適用之特定標準，亦可列入驗證文件，顯示出 ISO 對於以 ISO27001 為基礎的特定領域延伸驗證（依據 ISO27009），已有完整的佈局。

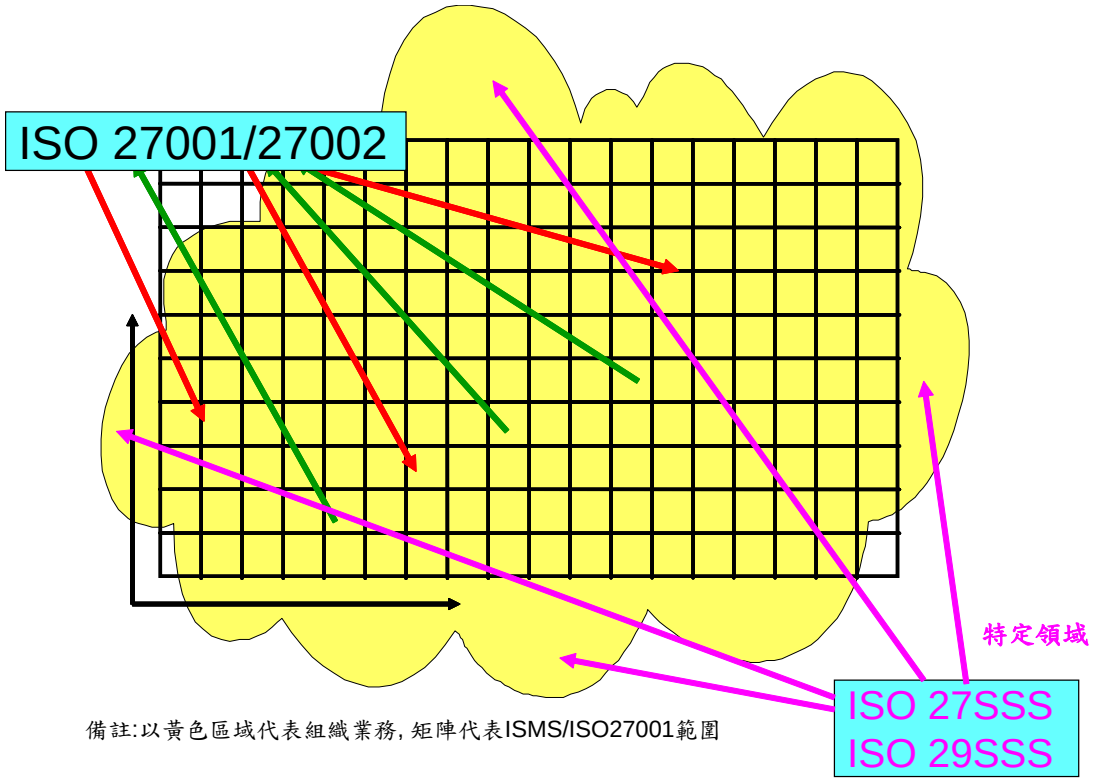

圖 3：特定領域的 ISMS

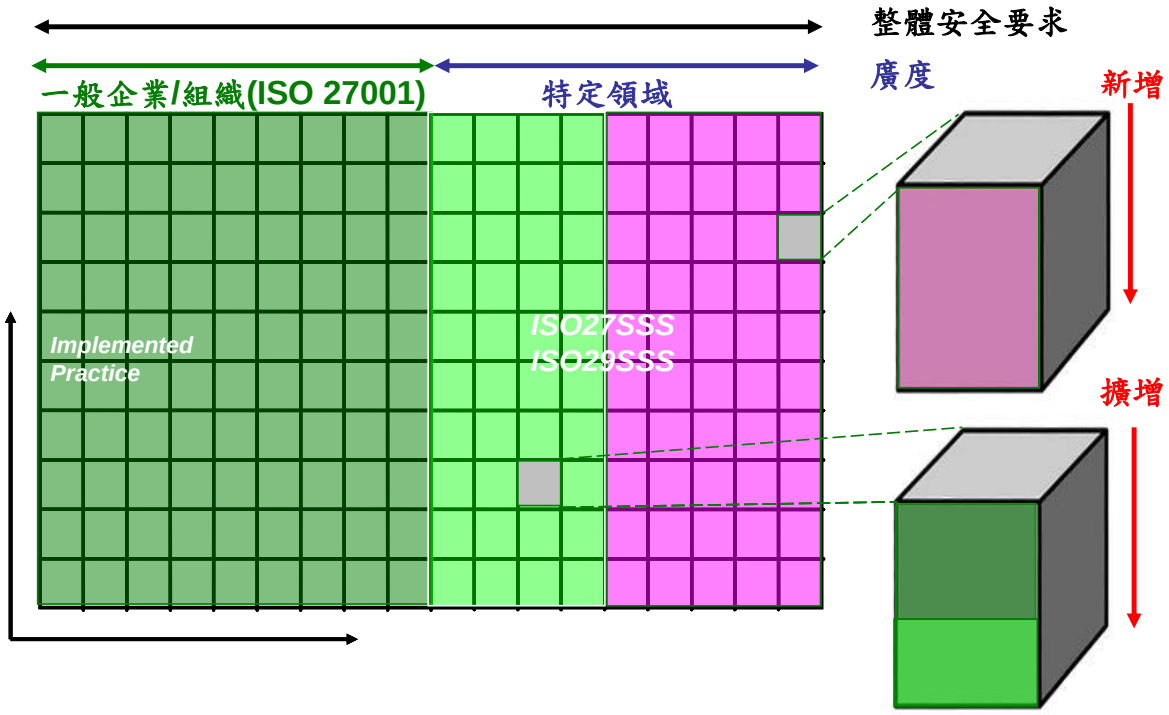

圖 4：一般與特定領域可選擇的 ISMS 實作方案

伍、如何從 ISMS 到 PIMS

對於已經運用 ISO 27001 標準建立 ISMS 的各級政府機關而言，以 ISO 29151 標準為依據，推動 PIMS 設立是最有效率的選擇。對於尚無建立 ISMS 的機關，亦可同時選擇以 ISO 相關標準建立 ISMS 與 PIMS 並通過驗證。ISMS 驗證標準為 ISO 27001（CNS 亦有相對應的標準）、PIMS 的驗證標準為 ISO29151，其中 PIMS 如有對外提供服務尚需增加 ISO 27018 驗證標準（適用於對外服務，CNS 亦有相對應的標準），各標準的交互關係如圖 5。

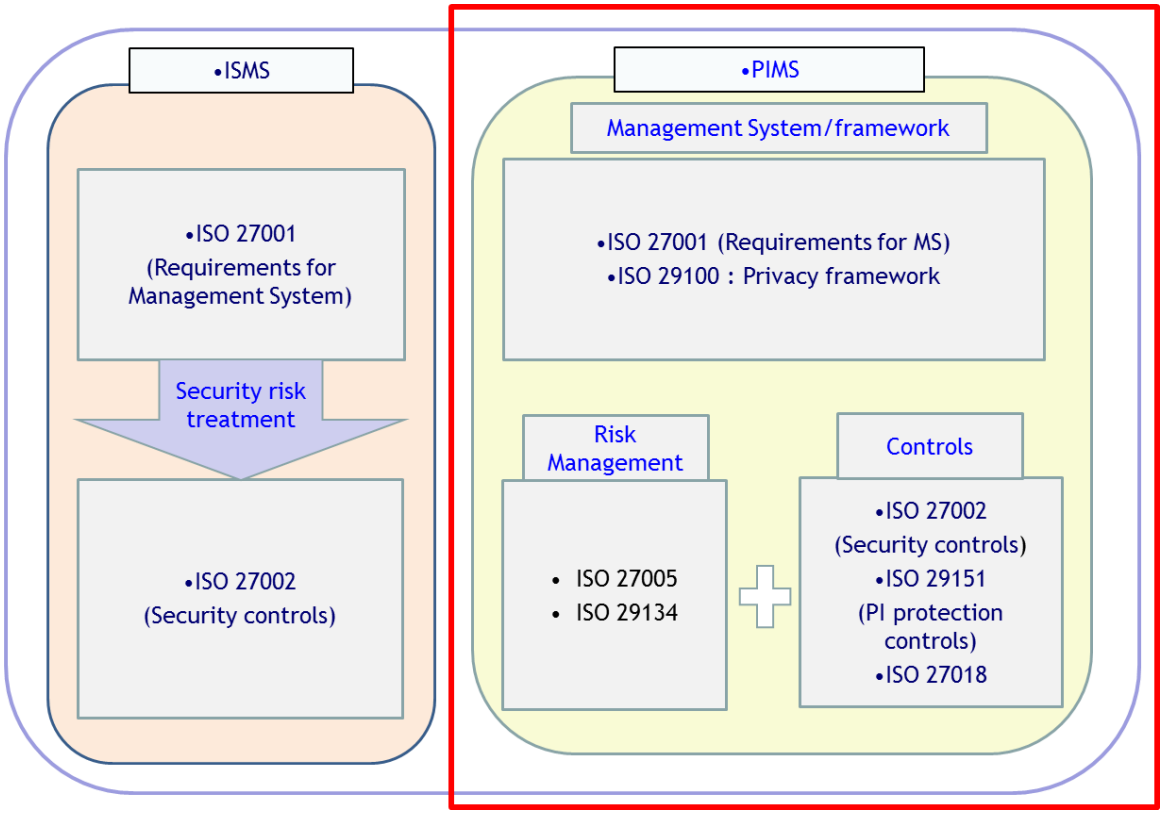

圖 5：ISMS 與 PIMS 關係

各機關以往遵循個人資料保護法及施行細則[2]時，在沒有適用的 ISO 國際標準情況下，會退而求其次採用英國或德國標準，但能否符合我國個人資料保護法及施行細則要求，或與其他國家互通，目前仍有爭議。個人資料保護與管理的 ISO 國際標準可應用在個資法及施行細則的法規遵循展現，政府機關對於內部的資訊安全及所持有個人資料保護是責無旁貸的，目前歐盟除了採用 ISO 29134 做為 GDPR DPIA[3]個人資料保護衝擊評鑑的標準外，亦已確認發展中的 ISO 27552 可直接做為 PIMS 的驗證標準，並鼓勵以認驗證機制（Article 40~43）來展現 GDPR 的法規遵循，包括英國標準學會（British Standards Institution; BSI）、德國標準化協會（Deutsches Institut fur Normung; DIN）與法國資訊與自由全國委員會（Commission Nationale de l'informatique et des libertés. CNIL）都正積極推動。

[2] 例如：第 12 條，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。

[3] General Data Protection Regulation - Data Protection Impact Assessment.

無論是現階段 ISO 27001+ISO 29151+ISO 27018 或是正在推動的 ISO 27001+ISO 27552 的 PIMS，以及因應歐盟 GDPR DPIA 的要求，都是以實施隱私衝擊評鑑為基礎工作，以 ISO 29134：隱私衝擊評鑑指引，在組織內建立 ISO 標準為基礎的隱私衝擊評鑑方法，除了可以與現有的制度接軌外，亦有助於建立以 ISO 標準為基礎的 PIMS，使我國在推動相關業務時，增進與各國間互認與接軌的基礎，也是鞏固既有制度並兼顧組織永續發展。

陸、參考文獻

梁日誠（2017）。「個人資料保護與國際資安新標準」。個資保護新紀元研討會。臺北市：臺灣數位鑑識發展協會。

臺灣網路防護協會（2018）。2018 年第 1 季資訊安全管理系統標準化系列討論會-GDPR 之驗證與個人資訊管理系統要求事項的組織證據標準化-根基於 ISO/IEC TC 1/SC 27 之進程。臺北市：臺灣網路防護協會。

European Union General Data Protection Regulation （http://eur-lex.europa.eu/）（accessed Feb 2018）

ISO, 2011, ISO 27005:2011 Information security risk management, Second edition, Switzerland, ISO.

ISO, 2011, ISO 29100:2011 Privacy framework, Switzerland, ISO.

ISO, 2013, ISO 27001:2013 Information security management systems – Requirements, Second edition, Switzerland, ISO.

ISO, 2013, ISO 27002:2013 Code of practice for information security controls, Second edition, Switzerland, ISO.

ISO, 2013, ISO 29101:2013 Privacy architecture framework, Switzerland, ISO.

ISO, 2013, ISO 29191:2013 Requirements for partially anonymous, partially unlinkable authentication, Switzerland, ISO.

ISO, 2014, ISO 27018:2014 Code of practice for protection of personally identifiable information （PII） in public clouds acting as PII processors, Switzerland, ISO.

ISO, 2015, ISO 27006:2015 Requirements for bodies providing audit and certification of ISMS, Second edition, Switzerland, ISO.

ISO, 2016, ISO 27009:2016 Sector-specific application of ISO 27001 -- Requirements, Switzerland, ISO.

ISO, 2017, ISO 29134:2017 Guidelines for privacy impact assessment, Switzerland, ISO.

ISO, 2017, ISO 29151:2017 Code of practice for personally identifiable information protection, Switzerland, ISO.

ISO, 2018, ISO 31000:2018 Risk management -- Guidelines, Second edition, Switzerland, ISO.

ISO, 2018, ISO DIS 20889 Privacy enhancing data de-identification techniques, Switzerland, ISO.

ISO CD 27552 Enhancement to ISO 27001 for privacy management – Requirements,

Switzerland, ISO.
ISO JTC 1/SC 27 WG 5 SD1 – WG 5 Roadmap, Switzerland, ISO.