國土及公共治理季刊

整合資安與個資管理系統的國際標準－ISO／IEC 27701 簡介與應用

黃明達　淡江大學資訊管理學系教授
梁日誠　ISO／IEC JTC1／SC27 委員、TCIC 環奧驗證公司全球營運總經理

壹、前言

自 2019 年 8 月公告開始，ISO／IEC 27701：2019（簡稱 ISO 27701）（註 1）便成為各方關注的焦點，期待 ISO 27701 整合了資訊安全管理與個資管理的特性能帶給目前日益翻新的新興科技與新興應用一個可供治理的共通基礎，使得數位社會的可信賴度（Trustworthiness）得以有效地建立。ISO 27701 是隱私資訊管理系統（Privacy Information Management System, PIMS. 本文依本地習慣用語譯為個資管理系統）的國際標準，為 ISO 27001（註 2）與 ISO 27002（註 3）於個資管理的延伸標準，完整地含括了可供驗證的 ISO 27001 各項要求及提供實作指引的 ISO 27002，且附加或微調個資管理的要求與實作指引。不僅整合資訊安全管理系統（ISMS）與個資管理系統（PIMS），也提供國際間所有不同型態與規模的機構，可用於驗證的 PIMS 國際標準。ISO 27701 除含括了 ISO 27001 與 ISO 27002 外，亦整合了 ISO 27018 公用雲個資處理者控制措施（註 4）、ISO 29151 個資控制者控制措施（註 5）、ISO 29134 隱私衝擊評鑑（註 6）、ISO 29100 隱私框架（註 7）等現有個資相關標準，是一個設計發展時即已考量整合概念（亦稱為整合設計 Integration by Design）的國際標準。

貳、ISO 27701 的資訊安全與個資保護整合應用

資訊安全著眼於資產的機密性（Confidentiality）、完整性（Integrity）與可用性（Availability），個資保護則涵蓋了同意及選擇、目的適法性及規定、蒐集限制、資料極小化、利用持有與揭露限制、準確性及品質、公開透明及告知、個人參與及存取、可歸責性、資訊安全、隱私遵循等 11 個隱私原則，採用基於資訊安全的個資保護方法便成了最佳的實作與法遵展現的考量，以歐盟一般資料保護規則 GDPR（註 8）為例，便於其中的 Article 32 要求處理的安全（Security of Processing），ISO 27701 緣因 GDPR 而生，也循資訊安全管理系統（ISMS）於個資管理的延伸（如表 1）而形成了個資管理系統（PIMS）。

表 1　資訊安全與個資保護相關標準的延伸關係

資訊安全相關標準	延伸事項	個資保護相關標準	類別
ISO 27001 第 4 ～ 10 章	個資管理系統要求	ISO 27701 第 5 章	要求
ISO 27002	個資控制措施	ISO 27701 第 6 章	指引
ISO 27002	個資控制者的額外控制措施	ISO 27701 第 7 章	指引
ISO 27002	個資處理者的額外控制措施	ISO 27701 第 8 章	指引
ISO 27001 Annex A	個資處理者的控制目標與 控制措施	ISO 27701 Annex A	要求
ISO 27001 Annex A	個資處理者的控制目標與 控制措施	ISO 27701 Annex B	要求

資料來源：作者整理

於建置 PIMS 時，可參考表 1 的要求與指引類別來建立或增修相關管理系統所需文件（如管理手冊、政策、程序書等），於進行 PIMS 驗證時，則應針對表 1 的要求類別進行合規展現，要求類別包含 ISO 27701 與 ISO 27001。以資通安全管理法子法－資通安全責任等級分級辦法（註 9）所要求的「初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性」為例，ISO 27701 的驗證恰與「以上效果」吻合，更增加了內含個資的核心資通系統的驗證有效性，同時展現了資訊安全與個資保護的合規性。

以個人資料保護法要求的適當安全維護措施（註 11）為例，參考臺灣士林地方法院小額民事判決 107 年度湖小字第 401 號個資法判例法院對於被告敗訴的判決書中指出「更乏資料可認被告於本事件發生前，已於公司內部就經手客戶資訊之員工建置完善、嚴格之管理制度。故難推認被告已就其所取得客戶（包含本件原告在內）個人資料，已善盡防護工作，以避免遭不法蒐集、處理、利用」，可見有效的個資管理系統（或稱制度）的建置、維運、稽核或驗證與持續改善機制於個資法遵循所扮演的關鍵角色。對於歐盟 GDPR 的適用單位而言，ISO 27701 提供一個合規展現的國際性方法，ISO 27701 Annex D 則 提 供 ISO 27701 與 GDPR 的對應表，此對應表的重要貢獻者之一便是 GDPR 的主責機構 European Data Protection Board（EDPB），EDPB 透過與 ISO ／ IEC JTC1 ／ SC27 ／ WG5 的緊密合作，於 ISO 27701 的發展到公告過程中代表歐盟全程參與，也正因如此，ISO 27701 也被各界期望成為泛歐的 GDPR 驗證標準的選項或部分選項之一。

表 2　個資相關專案的角色與個資保護要求事項對應表

專案角色 / 個資角色	委託機關	受託者	複委託者
個資控制者	V	☆（受託者因處理專案的個資而成為個資控制者）	☆（複委託者因處理專案的個資而成為個資控制者）
個資處理者	V	V	V
專案的個資保護要求事項	ISO 27701：管理系統、Annex A & B	ISO 27701：Annex B（專案要求）	ISO 27701：Annex B（專案要求）
因處理專案的個資而成為個資控制者的要求事項		☆ ISO 27701：管理系統、Annex A	☆ ISO 27701：管理系統、Annex A

資料來源：作者整理

ISO 27701 包含了個資控制者與個資處理者的要求事項，這也與個人資料保護法（註 10）中的委託機關與受託者、複委託者的關係架構吻合，委託機關可使用 ISO 27701 做為對受託者與複委託者的個資保護要求事項（如表 2）。以智慧城市為例，城市政府機構（委託機關）對於各個智慧應用（如智慧醫療、智慧教育、智慧金融支付等）專案的承接者（受託者或複委託者）便可應用表 2 進行個資與資安治理相關工作。

參、ISO 27701 於金融業的應用

於金融業的業務流程與資訊中，均高度包含個人資料，也因此資訊安全與個資保護作業是建立金融單位與客戶間互信關係所不可或缺的因素。金融監督管理委員會於金融業訂定了「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」（註 12），能同時展現對資訊安全與個資保護要求合規的 ISO 27701 便是最佳的選擇。在金管會於 2019 年 07 月 30 日公布純網路銀行許可設立名單（註 13）時，進一步說明了強化對純網銀之監理的面向，其中包含了「應於開業後 1 年內，通過並取得資安標準（如：ISO 27001）及個資保護標準（如：BS10012、TPIPAS）等認證」，於 2019 年 08 月 05 日公布的 ISO 27701 國際標準恰可做為整合資安標準與個資保護標準的合規對應方案。

臺灣正值開放銀行（Open Banking）蓬勃發展之際，資安與個資保護議題也成為各界關注的議題，開放銀行的相關利害團體可例舉如圖 1。若以 TSP（Trust Service Provider）業者、財金公司、金融機構三者間建立等同的資安與個資管理要求以展現行業合規為例，可識別出表 3 的相關國際標準列表。

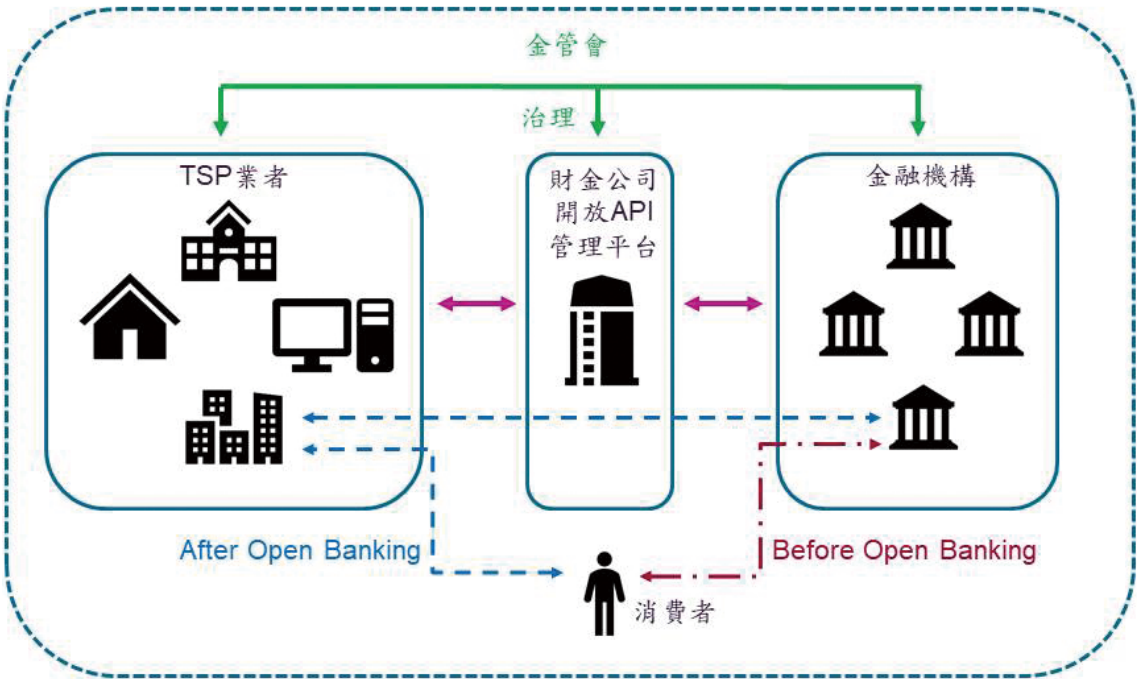

圖 1　開放銀行之相關利害團體關係圖

資料來源：作者整理

表 3　開放銀行之適用國際資安與個資管理標準列表

機構類別 / 相關要求	金融機構	財金公司	TSP 業者
資訊安全管理	V	V	V
個資管理	V	V	V
可適用的管理系統國際標準	PIMS ／ ISO 27701（含 ISMS ／ ISO 27001）	PIMS ／ ISO 27701（含 ISMS ／ ISO 27001）	PIMS ／ ISO 27701（含 ISMS ／ ISO 27001）

資料來源：作者整理

考量不同類別機構的相關資源取得或有難易不同的限制，可採用 ISO 27701 可適度選定 PIMS 範圍的特性，訂定分階段導入與驗證期程，終至等同資安與個資保護的互信架構。值得留意的是，TSP 業者的使用者終端程式（如 APP）自使用者申請帳號與通行碼或會員時即涉及個資的蒐集、處理、利用，也應確保個資法的合規性。對於各類別機構都有可能使用由雲端服務供應商所提供的雲端服務，基於等同資安與個資保護的原則，ISO 27701（PIMS 含 ISMS）也是必要選項，也另須考量雲端安全的相關國際標準如 ISO 27017，使得整體安全更臻完整。

肆、ISO 27701 於特定領域的應用

在整體 ISO 27000 系列資安與個資標準中，包含特定領域（Sector–Specific）適用的標準，可大致識別如圖 2 的關係圖。

以電信事業領域為例，主管機關 NCC 於電信事業資通安全管理手冊（註 14）中鼓勵並要求（部分）電信事業機構通過 TAF 認證之驗證機構的第三方 CNS ／ ISO ／ IEC 27001 驗證與 ISO ／ IEC 27011 增項稽核表驗證，並於國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法（註 15）中要求非公務機關蒐集、處理及利用達五千名用戶之個人資料者，其訂定之本計畫及處理方法內容應包含國內或國際個人資料安全稽核機制之規劃及執行計畫，圖 2 中的 ISO 27701 與 ISO 27011 標準可成為合規的最佳方案。其他主管機關，如經濟部（能源與公用事業）、衛福部（健康照護）、金管會（金融上雲端議題）等，都可使用圖 2 來識別特定領域的行業標準與要求。

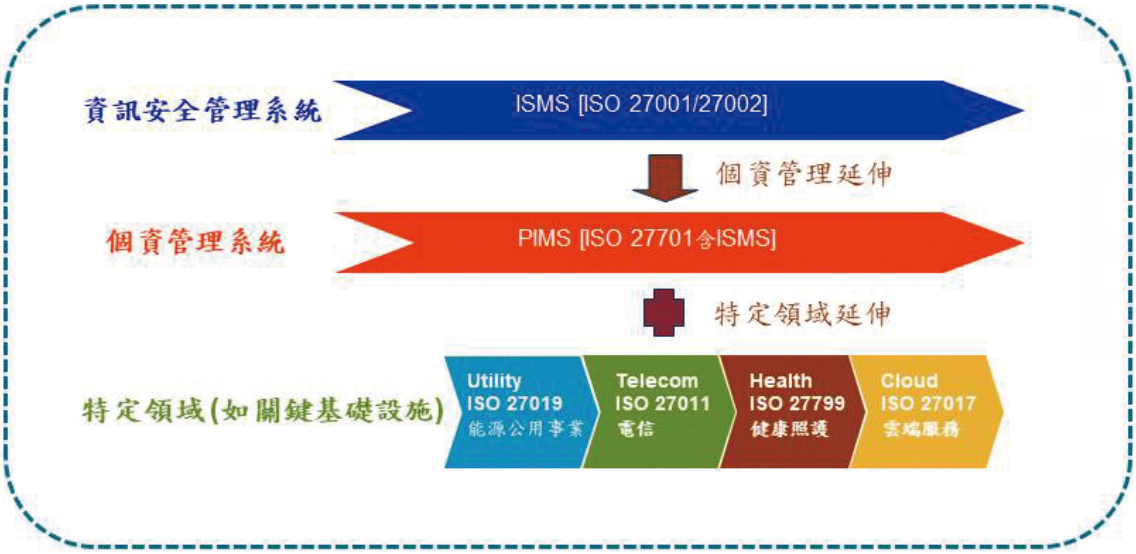

圖 2　特定領域資安與個資標準識別圖

資料來源：作者整理

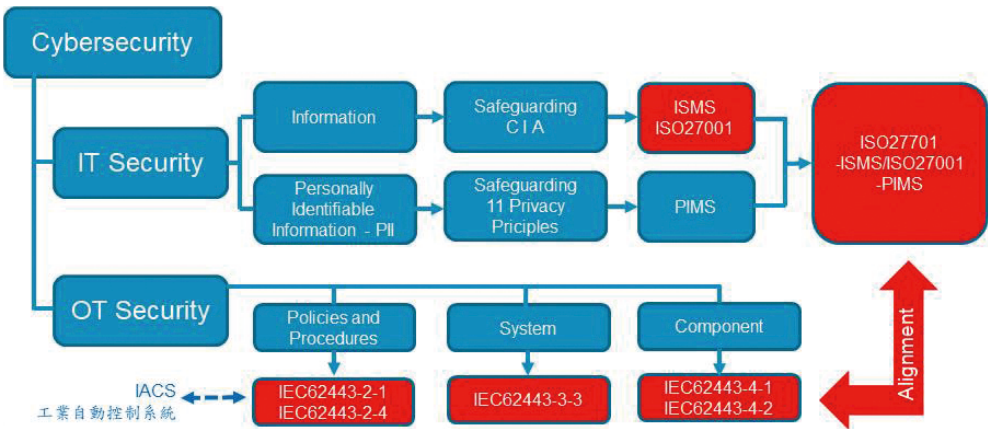

圖 3　組織內的資通安全適用標準分析

資料來源：作者整理

伍、資通安全發展的國際趨勢

資通安全（Cybersecurity）的框架（Framework）（註 16）適用於國家、社會、組織、個人等層面，並包含 IT 安全與 OT 安全兩部分，於組織內的資通安全適用標準分析如圖 3，組織可以採用所識別出的標準進行資通安全實作或驗證。

於國際間，除了歐盟 GDPR 鼓勵認驗證機制與自律規範（含監控）外，歐盟的資通安全法（Cybersecurity Act）（註 17）與聯合國的資通安全共通法規框架草案（A Common Regulatory Framework For Cybersecurity 2018, United Nations [draft]）（註 18）均提出了認驗證的要求。歐盟的資通安全法將針對 ICT Product、ICT Service、ICT Process 建立認驗證體制，聯合國的資通安全共通法規框架草案提出 People、Product、Process 的認驗證要求，認驗證的範圍包含了法規範圍內的組織及其供應商，也意味著若臺灣的設備與服務供應商無法符合國際間的認驗證要求，即無法在某些國際或國家的市場上架，而 ISO 27701 在供應商的 Process 層面對於 Cybersecurity 認驗證合規的展現扮演重要的角色。採用適當的國際標準 ISO 27701 以滿足對資安與個資保護的認驗證合規要求已是不可避免的趨勢，企業也須正視此議題並預做準備。

陸、整合式管理系統的比較分析

不論在臺灣或國際間，因為合規因素或市場要求或互信機制的建立，皆同時需要資訊安全管理與個資管理，ISO 27701 採用整合式方案（ISMS 與 PIMS 於同一管理系統中）管理系統的方法，相較於過去採用分立式方案的資訊安全管理（ISMS）與個資管理（PIMS）二套管理系統（先忽略整合的重工），我們試著進行概略的分析。因不同管理系統的管理系統（Management System, MS）部分均依循 ISO 的管理系統標準（Management System Standard, MSS）（註 19），MS 差異不大，概略視為等同。資訊安

表 4　分立式與整合式方案的比較表

組成 / 方案	資訊安全管理		個資管理	
	管理系統 MS	資安控制措施	管理系統 MS	個資控制措施
分立式	MS	資安控制措施	MS	個資控制措施
整合式（ISO 27701）	MS	資安控制措施	0.2MS	個資控制措施
整合式 – 分立式	0	0	–0.8MS	0

資料來源：作者整理

全管理系統可分析為 MS 加上達成資訊安全的控制措施，個資管理系統可分析為 MS 加上達成個資管理的控制措施。ISO 27701 的 MS 部分由 ISMS ／ ISO 27001 及個資管理延伸部分組成，ISMS ／ ISO 27001 的 MS 約有 59 個要求，個資管理延伸部分約有 12 個要求，約為 0.2 個 MS。分立式與整合式方案的比較如表 4。

由表 4 的分析可知，整合式 ISO 27701 方案相較於分立式方案（ISMS ／ ISO 27001 及另一 PIMS，共二個管理系統）約省了 0.8 個管理系統的投入，於第一年可視為建置成本的降低，於第二年開始可視為維運成本的降低。建立與維運管理系統可視為組織的合規成本，相較於分立式方案，使用整合式管理系統 ISO 27701 能有效的降低短期的建立成本與中長期的維運成本。若原採用分立式方案，也可轉換為 ISO 27701 整合式方案，愈早開始省得愈多。若資安法與個資法主管機關及各中央目的事業主管機關可以於政策面選定適合的國際標準 ISO 27701 並推動對應的國家標準 CNS 27701 的訂定及 ISO 27701 認驗證機制，對各公務與非公務機關在國內與國際間均將有相當的助益。

在新興科技與新興應用的推波助瀾下，數位化組織、數位社會、數位國家正快速的發展成形中，資通安全治理是數位治理不可或缺的一環，且有資通安全管理法與個人資料保護法把守著最後一道防線。當您走出臺灣跨向國際時，國際間的資通安全法規、個資保護法規及相關認驗證機制也同樣的規範著地球村的每一分子，最新的 ISO 27701 國際標準就像是一把新鑰匙，與您開啟著資通安全與個資保護整合管理的大門。

附註

註 1： ISO ／ IEC JTC 1 ／ SC 27, Information security, cybersecurity and privacy protection. 2019. ISO ／ IEC 27701：2019 Security techniques—Extension to ISO ／ IEC 27001 and ISO ／ IEC 27002 for privacy information management—Requirements and guidelines. Geneva ／ International Organization for Standardization.

註 2： ISO ／ IEC JTC 1 ／ SC 27, Information security, cybersecurity and privacy protection. 2013. ISO ／ IEC 27001 ／ 2013 Information technology—Security techniques—Information security management systems—Requirements. Geneva ／ International Organization for Standardization.

註 3： ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2013. ISO ／ IEC 27002 ／ 2013 Information technology—Security techniques—Code of practice for information security controls. Geneva ／ International Organization for Standardization.

註 4： ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2019. ISO ／ IEC 27018 ／ 2019 Information technology—Security techniques—Code of practice for protection of personally identifiable information（PII）in public clouds acting as PII processors. Geneva ／ International Organization for Standardization.

註 5： ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2017. ISO ／ IEC 29151 ／ 2017 Information technology—Security techniques—Code of practice for personally identifiable information protection. Geneva ／ International Organization for Standardization.

註 6： ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2017. ISO ／ IEC 29134 ／ 2017 Information technology—Security techniques—Guidelines for privacy impact assessment. Geneva ／ International Organization for Standardization.

註 7： ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2011. ISO ／ IEC 29100 ／ 2011 Information technology—Security techniques—Privacy framework. Geneva ／ International Organization for Standardization.

註 8： The European Parliament and of the Council. 2016. General Data Protection Regulation. Brussels ／ European Union.

註 9： 行政院編。2018。資通安全責任等級分級辦法。臺北：行政院。

註 10：行政院國家發展委員會編。2015。個人資料保護法。臺北：行政院國家發展委員會。

註 11：行政院國家發展委員會編。2016。個人資料保護法施行細則。臺北：行政院國家發展委員會。

註 12：行政院金融監督管理委員會編。2016。金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法。臺北。行政院金融監督管理委員會。

註 13：行政院金融監督管理委員會編。2019。純網路銀行許可設立名單。臺北。行政院金融監督管理委員會。

註 14：國家通訊傳播委員會編。2012。電信事業資通安全管理手冊。臺北。國家通訊傳播委員會。

註 15：國家通訊傳播委員會編。2016。國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法。臺北。國家通訊傳播委員會。

註 16：ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2018. ISO ／ IEC TR 27103 ／ 2018 Information technology—Security techniques—Cybersecurity and ISO and IEC Standards. Geneva ／ International Organization for Standardization.

註 17：European Parliament. 2014. EU Cybersecurity Act. Brussels ／ European Union.

註 18：Steering Committee on Trade Capacity and Standards. 2018. Draft proposal for a common regulatory framework on cybersecurity. Geneva ／ United Nations.

註 19：International Organization for Standardization Electrotechnical Commission. 2019. ISO ／ IEC Directives, Part 1, Consolidated ISO Supplement—Procedures specific to ISO. Geneva ／ International Organization for Standardization.

參考文獻

1. 行政院編。2018。資通安全責任等級分級辦法。臺北：行政院。
2. 行政院國家發展委員會編。2015。個人資料保護法。臺北：行政院國家發展委員會。
3. 行政院國家發展委員會編。2016。個人資料保護法施行細則。臺北：行政院國家發展委員會。
4. 行政院金融監督管理委員會編。2016。金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法。臺北。行政院金融監督管理委員會。
5. 行政院金融監督管理委員會編。2019。純網路銀行許可設立名單。臺北。行政院金融監督管理委員會。
6. 國家通訊傳播委員會編。2012。電信事業資通安全管理手冊。臺北。國家通訊傳播委員會。
7. 國家通訊傳播委員會編。2016。國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法。臺北。國家通訊傳播委員會。
8. European Parliament. 2014. EU Cybersecurity Act. Brussels ／ European Union.
9. ISO ／ IEC JTC 1 ／ SC 27, Information security, cybersecurity and privacy protection. 2019. ISO ／ IEC 27701 ／ 2019 Security techniques—Extension to ISO ／ IEC 27001 and ISO ／ IEC 27002 for privacy information management—Requirements and guidelines. Geneva ／ International Organization for Standardization.
10. ISO ／ IEC JTC 1 ／ SC 27, Information security, cybersecurity and privacy protection. 2013. ISO ／ IEC 27001 ／ 2013 Information technology—Security techniques—Information security management systems—Requirements. Geneva ／ International Organization for Standardization.
11. ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2013. ISO ／ IEC 27002 ／ 2013 Information technology Security techniques—Code of practice for information security controls. Geneva ／ International Organization for Standardization.
12. ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2019. ISO ／ IEC 27018 ／ 2019 Information technology—Security techniques—Code of practice for protection of personally identifiable information（PII）in public clouds acting as PII processors. Geneva ／ International Organization for Standardization.
13. ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2017. ISO ／ IEC 29151 ／ 2017 Information technology—Security techniques—Code of practice for personally identifiable information protection. Geneva ／ International Organization for Standardization.
14. ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2017. ISO ／ IEC 29134 ／ 2017 Information technology—Security techniques—Guidelines for privacy impact assessment. Geneva ／ International Organization for Standardization.
15. ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2011. ISO ／ IEC 29100 ／ 2011 Information technology—Security techniques—Privacy framework. Geneva ／ International Organization for Standardization.
16. ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2018. ISO ／ IEC 27000 ／ 2018 Information technology—Security techniques—Information security management systems—Overview and vocabulary. Geneva ／ International Organization for Standardization.
17. ISO ／ IEC JTC 1 ／ SC 27 Information security, cybersecurity and privacy protection. 2018. ISO ／ IEC TR 27103 ／ 2018 Information technology—Security techniques—Cybersecurity and ISO and IEC Standards. Geneva ／ International Organization for Standardization.
18. International Organization for Standardization Electrotechnical Commission. 2019. ISO ／ IEC Directives, Part 1, Consolidated ISO Supplement—Procedures specific to ISO. Geneva ／ International Organization for Standardization.

19. Steering Committee on Trade Capacity and Standards. 2018. Draft proposal for a common regulatory framework on cybersecurity. Geneva ／ United Nations.
20. The European Parliament and of the Council. 2016. General Data Protection Regulation. Brussels ／ European Union.