出國報告（出國類別：開會）

出席 2019 歐盟網路安全法國際會議

（2019 international Conference on the EU Cybersecurity Act）

服務機關：國家通訊傳播委員會
姓名職稱：簡任技正 蘇思漢
科長 陳坤中
派赴國家：比利時布魯塞爾
出國期間：108 年 11 月 16 日至 22 日
報告日期：109 年 1 月 20 日

摘　要

歐盟為確保電子通信網路安全，繼網路和信息系統安全性指令（NIS 指令），及新電信規則（New EU telecoms rules），又於 2019 年 4 月 17 日通過網路安全法（Cybersecurity Act），並自 2019 年 6 月 27 日生效。歐盟網路安全法除授權成立一常設之歐盟網路安全專責機構-歐盟網路與資訊安全局（European Union Agency for Cybersecurity，ENISA），以進一步落實 NIS 指令（包括為基本服務提供者及數位服務提供者使用之網路資訊系統提供網路安全防護建議、指導及最佳實踐等），並責成其協助制定 ICT 產品／服務／流程之資通安全驗證方案相關政策及協助各國實施，同時要求各會員國至少指定一個該國國家級的資通安全認證機構，以提升 ICT 產品／服務／流程的安全性及信任度，俾促進歐盟數位經濟之永續發展。

目前， 歐盟存在許多 ICT 產品的安全驗證方案。 但是，如果沒有適用於整個歐盟範圍內的資通安全認證通用框架，歐盟單一市場中出現分散和壁壘的風險就會增加。歐盟資通安全驗證方案是基於歐盟級別的協議，針對在歐盟範圍內之 ICT 產品／服務／流程，所議定的一套全面性規則、技術要求、標準及程序，用於評估其資通安全屬性。且鑑於 ICT 產品／服務／流程的多元性及多樣性，歐盟資通安全驗證方案將對不同領域的 ICT 產品／服務／流程量身訂做一基於風險的歐盟資通安全驗證方案，且具體描述其【涵蓋的產品和服務的類別】、【資通安全要求】、【評估類型】及【安全保證級別】。ICT 產品／服務／流程經歐盟資通安全驗證方案驗證合格者，可通行全歐盟會員國，除助於供應商跨境營運外，更助於消費者識別擬選購之產品或服務的安全功能。惟此項計畫為自願性，即供應商可以自行決定是否對其產品進行認證，且相關【資通安全要求】將盡可能依賴國際標準，以避免產生貿易壁壘或技術互操作性問題。

此外，歐盟委員會每 5 年將審視所採取的歐盟資通安全驗證方案執行情形，並評估是否透過歐盟其他法規，強制特定場域或全面實施歐盟資通安全驗證方案，以確保 ICT 產品／服務／流程維持一適當資通安全水準，並改善內部市場的運作。我國應把握其契機，適時調和歐盟資通安全驗證方案，以提升我國 ICT 產品等資通安全防護能量及市場競爭力。

目　　錄

壹、 目的

歐盟為加強網路安全結構、增強對數位技術的掌控及確保網路安全應當遵守之法律規範，已於 2019 年 4 月 17 日通過網路安全法（Cybersecurity Act），並自 2019 年 6 月 27 日生效（部分條款自 2021 年 6 月 28 日生效）。該法除成立一永久性之歐盟網路安全專責機構-歐盟網路與資訊安全局（European Union Agency for Cybersecurity，ENISA），以進一步落實 NIS 指令（包括為基本服務提供者及數位服務提供者使用之網路資訊系統提供資通安全防護建議、指導及最佳實踐等），並責成其協助制定 ICT 產品／服務／流程之資通安全驗證框架相關政策及協助各國實施，同時要求各會員國至少指定一個該國國家級的資通安全認證機構。

ICT 產品／服務／流程之資通安全驗證方案雖屬自願性認證，但該法並授權及要求各會員國於其國內法規中明定違反歐盟資通安全認證相關處分。目前歐盟部分會員國雖已施行資通安全驗證方案（包括資通安全要求及評估標準），但處於發展初期的【歐盟網路安全法】最終將其整合並建立一個廣泛且獨立於歐盟網路安全法規體系，並作為"單一數位市場"目標之一部。

5G 網路亦屬 ICT 產品／服務／流程之一部，鑑於德國、義大利、芬蘭、英國、瑞士、愛沙尼亞等歐盟會員國均已提供 5G 服務，且我國亦已規劃於今（108）年年底前釋出 5G 頻段，並期許於明年釋出 5G 特許執照。為確保我 5G 網路安全、強韌及可信賴，實有對其資通安全驗證方案深入瞭解，並汲取其經驗，以促進我國產業轉型與發展，奠定數位經濟發展之基礎。

貳、 行程表

2019 歐盟網路安全法國際會議係於 11 月 18 日及 19 日假比利時布魯塞爾酒店召開，本會出席人員係 11 月 16 日 出發，21 日搭機返國，相關行程如下：

日期		行程
Day 1	11/16	**20：10** 搭乘**泰航 TG 635** 由桃園機場(第一航站)出發
		23：05 抵達曼谷蘇汪納蓬國際機場
Day 2	11/17	**00：30** 搭乘**泰航 TG 934** 由曼谷蘇汪納蓬國際機場出發
		07:05 抵達布魯塞爾機場
Day 3	11/18	參加 2019 歐盟網路安全法國際會議第一日
Day 4	11/19	參加 2019 歐盟網路安全法國際會議第二日
Day 5	11/20	整理會議資料及私人行程
Day 6	11/21	**13：10** 搭乘**泰航 TG 935** 由布魯塞爾機場出發
Day 7	11/22	06：10 抵達曼谷蘇汪納蓬國際機場
		08：15 搭乘**泰航 TG 632** 由曼谷蘇汪納蓬國際機場出發
		12：45 抵達台灣桃園國際機場第一航站

參、 會議議程

表 1第一天議程

<table>
<tr><td>08:00-09:00</td><td colspan="2">REGISTRATION</td></tr>
<tr><td>09:00-10:30</td><td colspan="2">PLENARY KEYNOTE SESSION
09:00
Conference Plenary Keynote Address (P10a)
Juhan Lepassaar, Executive Director, European Union Agency for Cybersecurity (ENISA)

09:50
Conference Welcome Presentation: The Cybersecurity Act is Here, But What Does This Mean? (P10b)
Sergio Lombán Lage, VP, Digital Trust Services, SGS Group, Spain</td></tr>
<tr><td>10:30-11:20</td><td colspan="2">NETWORKING BREAK</td></tr>
<tr><td rowspan="2">11:20-12:30</td><td colspan="2">TRACK SESSIONS 1</td></tr>
<tr><td>Panel Discussion
12:00
Certification for Critical Infrastructures (P11a)
Moderator: Jacques Kruse Brandao, Head of Advocacy Digital Trust Services, SGS Group, Germany
Panelists: John Boggie, Director Head of Certification, NXP Semiconductors UK, United Kingdom; Sergio Lombán Lage, VP, Digital Trust Services, SGS Group, Spain; Julian Meyrick, Managing Partner & Vice President, Security Strategy Risk & Compliance, Security Services, IBM, United Kingdom; Eva Schultz-Kamm, Head of Global Government Affairs, Siemens, Germany</td><td>Industry Alignment
12:00
ETSI Security Evaluation Standardization Initiatives (A11a)
Sonia Compans, Technical Officer, ETSI, France

12:30
Lessons Learnt in the Commercial Use of Security Certification—From Setting Standards to an Innovator's Perspective (A11b)
Boris Balacheff, HP Fellow & VP, Chief Technologist for Security Research and Innovation, HP Labs Security Lab, France</td></tr>
</table>

12:30-13:50	LUNCH BREAK	
13:50-16:00	TRACK SESSIONS 2	
	Public Policy	Industry Alignment
	14:00 **Update on ENISA Operations and CSA Implementation** (B12a) Slawomir Górniak, Security Tools and Architecture Expert, European Union Agency for Network and Information Security (ENISA), Greece	14:00 **Vendor Self-Assessment—The Good, The Bad, and the Ugly** (A12a) Helmut Kurth, Chief Scientist and Laboratory Director, atsec information security, Germany
	14:30 **European Cybersecurity Certification Framework, State of Play** (B12b) Aristotelis Tzafalias, Policy Officer, Cybersecurity and Digital Privacy, European Commission, Belgium	14:30 **ISCI WG (International Smartcard Initiative) Who Are We? What Do We Do? How Do We Do It? And How Do We Contribute to The EU Cyber Act?** (A12b) Rachel Menda-Shabat, Director of Security Solution Certification Division, ISCI WG sub-chair, Winbond, Israel
	15:00 **ECSO's Outlook on the EU Cybersecurity Act** (B12c) Roberto Cascella, Senior Policy Manager, ECSO, Belgium	15:00 **Update on The EU Cybersecurity Act: Is The Feared Balkanization of Common Criteria Being Reversed?** (A12c) Martin Chapman, Senior Director, Standards Strategy and Policy EMEA, Oracle, Ireland
	15:30 **Security Needs to be Consistent—The Role of Process in the Cybersecurity Act** (B12d)	15:30 **The Certification Landscape and What Industry Needs** (A12d) John Boggie, Director Head of Certification, NXP Semiconductors UK, United Kingdom

	David Martin, Head of International Assurance, NCSC, United Kingdom	
16:00-16:30	NETWORKING BREAK	
16:30-18:00	TRACK SESSIONS 3	
	Standards for Success 16:30 **CEN-CENELEC JTC13 WG3 Security Evaluation Standardization Initiatives** (S13a) Miguel Bañon, Global Technology Leader for Cybersecurity, Epoche and Espri (a DEKRA company), Spain 17:00 **Comparing National Lightweight Methodologies around Europe** (S13b) Javier Tallon, CoFounder and COO, jtsec Beyond IT Security SL, Spain 17:30 **Implementing and Maintaining a Cybersecurity Program—The Role of Standards** (S13c) Raymond Romero, Deputy Director, Board of Governors of the Federal Reserve Systems, United States	Cloud and GDPR Frameworks 16:30 **Toward the European Cloud Security Certification Scheme: The CSPCERT Final Public-Private Recommendation** (C13a) The European Cloud Service Provider Certification Working Group, Saurabh Ghelani, EMEA Strategic Trust Leader, Google Cloud, et al. 17:00 **The EU-SEC Framework** (C13b) Lefteris Skoutaris, Research Analyst, Cloud Security Alliance, Greece 17:30 **Addressing GDPR Requirements Using the ISO/IEC 27701 Standard. Is the CSA Looking At It?** (C13c) Willy Fabritius, Global Portfolio Champion for Information Resiliency, BSI Group, United States
18:00	ADJOURN	

表 2 第二天議程

	TRACK SESSIONS	
09:00-11:00	IoT Challenges 9:00 **Embedded Systems for IoT Products: What is the Current Certification Offer?** (I20a) Dr. Claire Loiseaux, CEO, Internet of Trust, France; Alexander Schasse, IT Security Consultant bei TÜV Informationstechnik GmbH – TÜViT, Germany 09:30 **SESIP: A Practical, Operational, Lightweight CC Methodology** (I20b) Wouter Slegers, CEO, TrustCB, Netherlands 10:00 **EUROSMART IoT Security Certification Scheme (eIoT SCS)** (I20c) Roland Atoui, Managing Director, Red Alert Labs/EUROSMART, France; and Ayman Khalil COO & Managing Partner Red Alert Labs 10:30 **X-Gateway as a Modular Part of IoT** (I20d) Markus Bartsch, Business Development, TUViT, Germany	Industrial Strategies 09:00 **Foundations and Perspectives of the EU's 2019 Cybersecurity Act Certification Legislation for the Industrial Automation and Control Systems** (T20a) Paul Theron, Advisor & Cyb'Air Research Chair, Thales, France 09:30 **Beyond the Theory of the Cybersecurity Act** (T20b) Stefano Bracco, Knowledge Manager, European Union Agency for the Cooperation of Energy Regulators, Italy 10:00 **IEC62443 and NIS Directive: Needs and Opportunities** (T20c) Maria Fravventura, Security Evaluator, Brightsight, Netherlands 10:30 **Building Trust and Hope in 5G Instead of Selling Fear** (T20d) Mika Lauhde, Global Vice-President, Cybersecurity & Privacy, Global Public Affairs, Huawei, China
11:00-11:30	NETWORKING BREAK	

11:30-12:30	TRACK SESSIONS	
	IoT Challenges 11:30 **Common Criteria as Backbone of IoT Security Certification** (I21a) Georg Stütz, Principal Security Certification Expert, NXP Semiconductors, Austria 12:00 **OWASP IoT Project: A Great Ally for the IoT Candidate Schemes** (I21b) Jose Alejandro Rivas Vidal, Security Lab Manager, Applus+ Laboratories, Spain	Panel Discussion 11:30 **Standardization and the EU CSA** (P21a) Discussion on standardization efforts under various national frameworks. **Panelists:** Sonia Compans, Technical Officer, ETSI, France; Philippe Magnabosco, Policy Advisor for External Standards, ANSSI, France; David Martin, Head of International Assurance, NCSC, United Kingdom[60 Minutes]
12:30-13:30	LUNCH BREAK	
13:30-15:30	TRACK SESSIONS	
	Outlook/Opportunities 13:30 **SOGIS View on the Cybersecurity Act** (L22a) Bernd Kowalski, Chairman, SOG-IS, Germany 14:00 **Overview of Current and Future NIAP and US Government Certification Initiatives** (L22b) Mary Baish, Director, NIAP, United States 14:30 **BSI View on the EU Cybersecurity Act** (L22c) Speaker TBA, BSI, Germany	Innovations in Assurance 13:30 **Addressing the Continuity of Software Security for Embedded Devices** (N22a) Jasmina Omic, Product Manager Services, Riscure, Netherlands 14:00 **Updating Certified Products** (N22b) Gabor Hornyak, CTO, CCLab, Hungary 14:30 **Agile Assurance: Modernizing IT Product Certification** (N22c)

		Lachlan Turner, Director Consulting, Lightship Security, Canada
	15:00 **The ROI of Security Evaluations** (L22d) Dirk-Jan Out, CEO, Brightsight	15:00 **Making Evaluation Schemes Scale Up: the Tensegrity of Process and Product** (N22d) Tony Boswell, Senior Principal Consultant, DNV GL Technical Assurance Laboratory, United Kingdom
15:30-16:00	NETWORKING BREAK	
16:00-17:00	CLOSING PRESENTATION, SUMMARY PANEL DISCUSSION 16:00 **Panel Discussion: Looking Ahead to the Next Generation of Industry Assurance** (P23a) **Moderator:** Chris Gow, Director, EU Public Policy, Government Affairs, Cisco, Belgium **Panelists:** Michael Cooper, Manager, Security Testing, Validation and Measurement Group, National Institute of Standards and Technology (NIST), United States; Slawomir Górniak, Security Tools and Architecture Expert, European Union Agency for Network and Information Security (ENISA), Greece; Jonathan Sage, Government and Regulatory Affairs, IBM, United Kingdom; Aristotelis Tzafalias, Policy Officer, Cybersecurity and Digital Privacy, European Commission, Belgium	
17:00	ADJOURN	


2019 INTERNATIONAL CONFERENCE
EU CYBERSECURITY ACT
PLATINUM SPONSOR
SGS
PRESENTING SPONSOR
ECS

圖 1 出席人員大會留影

肆、 會議重要內容紀要

一、開幕式及主題演講（Conference Welcome Presentation）

開幕式及主題演講係由 ENISA 執行董事（Executive Director）Juhan Lepassaamr 與本次會議最大贊助商 SGS 集團-數位服務副總裁 Sergio Lombán Lage 擔綱。

(一) ENISA 執行董事 Juhan Lepassaar 演講

Juhan Lepassaar 於今年 10 月 16 日就任，在接任執行董事之前，於歐盟執委會服務 6 年，並曾任歐盟副主席 Andrus Ansip 團隊數位單一市場事務主管。本次研討會 Lepassaar 以網路安全法為題，闡述未來歐盟在網路與資訊安全治理的變革：

1. 提升 ENISA 在歐盟網路與資訊安全治理的能量及角色

為強化歐盟在網路安全治理上的專業能力及促使 ENISA 可更有效的協助歐盟執委會及網路資訊安全協作小組（NIS Cooperation Group）處理歐盟境內的網路安全事宜，網路安全法已將 ENISA 由一臨時性的任務編組，提升至歐盟執委會下的官方組織。

另為因應 5G 網路布建衍生的設備安全威脅，ENISA 也遵循執委會於今年 3 月發布之「5G 網路安全建議書」（Recommendation on Cybersecurity of 5G networks）要求，協助歐盟會員國評估所屬 5G 基礎網路建設所涉資通安全風險及威脅，並綜整各會員國 5G 基礎網路建設所涉資通安全風險及威脅之評估結果，於今年 10 月 6 日提出歐盟層級的 5G 網路安全風險評估報告（EU coordinated risk assessment of the cybersecurity of 5G networks）。具體描述當前歐盟會員國對於 5G 網路風險來源的看法，並劃分 10 類風險情境（risk scenarios）。以 10 種風險情境之一「缺乏接取控制措施（lack of access controls）」為例，組織如缺乏足夠的接取控制措施，懷有惡意且具備網路管理員權限的分包商即有可能得以破壞受保護資訊的機密性、完整性、可用性。接下來，ENISA 將

從技術面進一步描繪前述風險及威脅樣態，即針對 5G 網路各關鍵元件，提出潛在的網路安全漏洞。復依「5G 網路安全建議書」要求，於本年 12 月底前提出 5G 網路風險減輕措施工具箱（a common toolbox of mitigating measures），提供各會員國參考。

2. **建立資通安全驗證框架，幫助消費者了解網路安全**

網路安全法施行後的另一項重要變革係為建立適用於全歐盟的 ICT 產品／服務／流程之資通安全驗證框架（cybersecurity certification framework）。歐盟執委會的期望是未來藉由驗證框架的建立，制定各領域的資通安全驗證方案（cybersecurity certification scheme），並搭配市場機制運作，以幫助消費者取得相對安全的 ICT 產品／服務／流程。

ENISA 除將依歐盟滾動式工作項目（The Union Rolling Programme, URWP）及執委會指示，提出驗證框架候選計畫（candidate scheme）外，並將設立專網，發布各項資通安全驗證框架候選計畫之細節，及歐盟官方對於認證一致性（conformity）的聲明。歐盟的一般民眾則可藉此了解資通安全驗證框架的各項細節，藉此強化個人資通安全意識，並於未來選購具有安全認證的 ICT 產品及服務。

3. **加強網路安全相關研究**

在網路安全法提升 ENISA 法律位階及人力、預算後，ENISA 已有更豐富的資源可針對網路安全風險、預防措施強化等研究。以 5G 網路為例，綜整提出歐盟層級的 5G 網路安全風險評估報告及盤點未來 5G 網路在布建與運作上可能存在的網路漏洞與網路威脅，並提出相應的減輕措施等，均係 ENISA 成為歐盟正式官方組織後，得以進行之工作。未來 ENISA 將運用資源，強化相關網路安全研究，進而協助歐盟會員國建立符合自身需求的網路安全防護措施。

(二) SGS 副總裁 Sergio Lombán Lage 演講

SGS 鑑於未來大量物聯網裝置將遍及各行各業，以及 5G 網路興起，

自 2018 起即整合該公司既有資通安全能量，提供【ICT 產品及系統】、【網路通訊及雲端】、【資通安全管理系統、服務與專業認證】及【資料整合】等 4 項數位信任服務（Digital Trust Service）。Lage 為數位信任服務的負責人，於網路安全法草案諮詢期間，曾以專家身份參與並提供相關意見。本次研討會，他以「網路安全法的出現意欲為何（The Cybersecurity Act is Here, But What Does This Mean?）」為題，從業界實務經驗出發，闡述這部法律出現的意義為何？

1. 法規的目的在於建立人民的信任

Lage認為在當前數位時代公司治理的主要議題為取得消費者信任及保護企業聲譽，也因此有遠見的企業無論規模大小均應將一部分利潤投資於資通安全措施，建立良好的資訊安全管理制度，以防禦網路攻擊。此時，歐盟發布網路安全法，並試圖建立全歐盟適用的資通安全驗證框架，提供企業及消費者依循及選擇的基準，並建立對於 ICT 產品及服務的信任感。

資通安全驗證框架為因應消費者使用情境，所提出的基本（Basic）、實質（Substantial）、高級（High）三種安全保證級別（assurance level），雖立意良善，但實務上，目前仍無各方均可接受的共同基準。因此，如何解決共同基準的問題，及相關配套措施將是未來落實網路安全法的重大挑戰。

2. CSA 也可以像 GDPR 一樣成為全球黃金標準

鑑於歐盟市場的性質，網路安全法（CSA）相關要求很可能重現數年前一般資料保護規則（GDPR）成為全球通用標準的情況。不過要達成此一目標，各類驗證標準間的相互承認將成為國際市場的主要課題。此外，優先推動哪些垂直產業（Vertical Industries）的資通安全認證標準、第三方服務的供應鏈管理及市場本身喜好等，都是未來在推動資通安全驗證框架應考量之因素。

二、小組討論

(一) 關鍵基礎設施資通安全認證（Certification for CI）

本場討論主持人為 SGS 數位信任服務推廣主管 Jacques Kruse Brandao，報告人兼與談人為西門子全球治理事務主管 Eva Schultz-Kamm，其餘與談人包括 NXP 資通安全驗證主管 John Boggie、TÜV SÜD 資通安全策略主管 Sudhir Ethiraj、SGS 數位信任部門副總裁 Sergio Lombán Lage 及 IBM 合夥人暨資通安全服務副總裁 Julian Meyrick。討論主題為「信任憲章」（Charter of Trust）在驗證實務上之落實情形。進行方式首先由 Eva Schultz-Kamm 報告「信任憲章」之內容，接著以信任憲章第 2 條及第 7 條原則展開討論。

1. 開場簡報：資通安全信任憲章之概述

資通安全信任憲章（Charter of Trust on Cybersecurity）為歐洲網通大廠西門子（Siemens）於 2018 年 2 月倡議的資通安全產業自律規範，共同簽署者，計有 Siemens 、AES 及 AIRBUS 等 16 家跨國企業[1]。信任憲章定有 3 大目標及 10 大原則。3 大目標為【保護個人及公司資料】、【避免損害個人、企業及基礎建設】及【建立數位世界可資信賴的基礎環境】；另 10 大原則分別為網路與資訊安全所有權原則（Ownership of cyber and IT security）、負責任的數位供應鏈原則（Responsibility throughout the digital supply chain）、安全預設原則（security by default）、以使用者為中心原則（User-centricity）、創新與共創原則（Innovation and co-creation）、資通安全教育原則（Education）、關鍵基礎設施驗證及解決方案原則（Certification for critical infrastructure and solutions）、透明及回應原則（Transparency and responses）、法規框架原則（Regulatory framework）、聯合倡議原則（Joint initiatives）。

[1] 16 家企業為 AES、AIRBUS、Allianz、Atos、CISCO、DAIMLER、DELL、IBM、MSC、NXP、SGS、SIEMENS、Deutsche Telekom、TOTAL、TÜV SÜD、Mitsubishi Heavy Industries。

2. **議題討論：**

(1) **信任憲章原則 2-負責任的數位供應鏈原則項下 17 項要求之落實程度**

Eva Schultz-Kamm 與 Julian Meyrick 皆表示此 17 項基準要求只是未來供應鏈生產的基礎要求，Sergio Lomban Lage 亦進一步指出此 17 項基準要求可以說是全球具代表性的企業對於安全的想法，其價值不但在於橫跨多方且也足以符合業界對於效率的要求。

Category	Baseline Cybersecurity Supply Chain Requirements [1]
Data Protection	Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data
	Data shall be protected from unauthorized access throughout the data lifecycle
	The design of products and services shall incorporate security as well as privacy where applicable
Security Policies	Security policies consistent with industry best practices such as ISO 27001, ISO 20243, SOC2, IEC 62443 shall be in effect (including access control, security education, employment verification, encryption, network isolation/ segmentation, operational security, physical security, vendor management)
	Guidelines on secure configuration, operation and usage of products or services shall be available to customers
	Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products and services.
Incident Response	For confirmed incidents, timely security incident response for products and services shall be provided to customers
Site Security	Measures to prevent unauthorized physical access throughout sites shall be in place
Access, Intervention, Transfer, & Separation	Encryption and key management mechanisms shall be available, when appropriate, to protect data
	Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced
Integrity and Availability	Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed
	Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigating risks to service environments
	Business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption, where applicable
	A process shall be in place to ensure that products and services are authentic and identifiable
Support	The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available
	Based on risk, and during the timeframe of support, processes shall be in place for: (1) Contacting Support, (2) Security Advisories, (3) Vulnerability Management, and (4) Cybersecurity related Patch Delivery and Support
Training	A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awareness)

圖 2 原則 2 負責任的數位供應鏈原則所定 17 項基準要求

資料來源：美國 NIST 網站

(2) **信任憲章如何與世界主要國家的資通安全法律協調一致，特別尤其是網路安全法提出建置歐盟資通安全驗證框架，信任憲章的內容如何符合？**

在場的專家皆同意信任憲章目標之一，即是協助政府落實資通安全驗證的工作。網路安全法關注的是政治制度上的調整，而信任憲章則是從產業需求為出發點所建立的數位信任（digital trust）做法，簽訂信任憲

章的企業，也仍處於實踐學習階段。

信任憲章實際上是回應網路安全法的設計初衷，即藉由歐盟資通安全證框架的機制，配合信任憲章的基準要求，盤點當前已有且可用的標準，以制定後續特定領域的資通安全驗證計畫。

(3) 信任憲章原則 7-關鍵基礎設施驗證實務運作及如何支援法規落實

在場專家表示信任憲章提出對於關鍵基礎設施的驗證，係基於在超高速且萬物聯網時代，所有資通訊設備及可連網的裝置皆存在潛藏的資安問題。驗證本身不在於創造安全環境，只是揭露對驗證對象的信任程度，因此信任是一切的基礎。

依據安全設計開發及預設安全的產品無須驗證，因為安全設計與安全驗證即是呈現信任的一種措施。原則 7 描述的是企業提供關鍵基礎設施使用之產品需經獨立第三方驗證，係為落實信任規則（Rule of Trust）。並非所有資通產品都需要獨立第三方評鑑，但應用在極端要求安全的環境中的產品，獨立第三方評鑑是必要的。

(二) 歐盟網路安全法及標準化（Standardization and the EU CSA）

1. ETSI 論點

歐洲電信標準組織（ETSI）代表 SONIA COMPANS 女士表示，ETSI 有權提供與支持歐盟網路和整個系統政策所需標準。ETSI 從一開始就將網路安全納入考量，如定義不同網路功能元件間使用之加密機制，身份驗證等，但在安全與風險評估方面，ETSI 經驗尚待充實。

目前 IoT 市場對於安全議題仍處於混亂狀態，許多公司沒有為其產品提供安全功能與流程。為因應萬物聯網的時代，ETSI 在德國 BSI 等單位協助下，已發布一定義消費者端連網設備所採技術和流程之安全性要求的 IoT 安全標準。ETSI 雖然只邁出非常小的一步，但如果所有供應商都跟進，那麼將大大提高整體的安全程度。

2. 法國 ANSSI 論點

法國資訊安全機構代表 ANSSI 的 PHILIPPE MAGNABOSCO 先生表示，制定網路安全的標準是一件有意義和重要的事情。CSA 理想是希望在公共政策方面採取一些重大且一致的步驟來取得成功。

ANSSI 作為國家網路安全機構，在制定網路安全標準的角色上，要使其他部門標準之間保持一致。多年來使用的 Common Criteria 不會因 CSA 施行而消失，因為它們在 CSA 中絕對起著作用，因此 ANSSI 正在努力並花費大量資源試圖使它們變得更好。ANSSI 認為標準要被市場所接受，明確準則不可少，包括級別、內容等，而且標準也需要保持一致性。

Common Criteria 存在一個反饋循環機制，在此過程中評估人員會通知申請者改善初步發現的缺陷，改進後才進行評估。如要加速驗證的過程，可中斷反饋迴路，縮小驗證流程規模並集中精力測試產品。

3. **德國 BIS 論點**

德國 BSI 代表 HELGE KREUTZMANN 先生表示，標準經過國家層級的良好實踐後，才納入歐洲或國際標準或前期標準是至關重要的。

BSI 參加多個標準化組織，並實際參與工作小組運作，貢獻 BSI 經驗，以便將這種經驗進行標準化，最終將標準應用於認證產品。舉幾個例子，計量公路車輛的運行情況，BSI 參與制定歐洲標準，另一個例子是智慧卡，現在也已在歐洲使用。

4. **英國 NCSC 論點**

英國資安機構代表 DAVID MARTIN 先生表示，英國在幾年前就發展了自己的商用產品保證計畫（Commercial Product Assurance，CPA)，CPA 詳細說明標準的要求，並希望與行業公認的測試方法保持一致，因此需要發展與行業協作的保護配置文件，但這將需要很長時間。

在英國，大家都迫切需要一種能夠解決多種產品保證問題的工具。CPA 是一項全國性計畫，其優點是若遇到任何困難，可以與國內的 NCSC

聯絡，這一點是國際標準沒有能力做到的。而 CPA 計畫確實有一半要求，是所謂的“Bill Standards”，也就是在很大程度上是作業與流程安全，因此它所執行的不僅僅是 Common Criteria。Common Criteria 在流程保證的部分並不那麼強力有效，故採用 CPA 標準可以更有利益。目前，CPA 已實際應用於英國的智慧電錶。

英國的電力輸送配電方式與許多歐洲國家不同，因此要有自己的評估標準。英國一直在評估更廣泛的保證計畫的實施方式，包括電信，人員在內，公司在內，所有這些問題都經過了很長時間的評估討論，但該討論尚未完成。

5. 西班牙 Epoche & Espri 論點

西班牙驗證公司代表 MIGUEL BAÑON 表示，標準需要時間和資源來開發，而且驗證實驗室不可能擁有無限資源，驗證服務所需資源最小化應納入考量。自我評估可以減少驗證過程所需成本，但自我評估需要擁有足夠的透明度和足夠的細節，評估才有意義。若沒有足夠的透明度來建立信任關係，就必須藉由獨立的第三方驗證。

驗證的一切都與資源有關，實驗室在擇定測試項目時，應審慎評估所需成本及執行時間。有時驗證公司可能自認花費不少時間執行檢測，但申請者可能要花更多時間去解釋疑點與解決問題，因此在擇定測試項目時，應審慎為之。

(三) 展望下一代行業保障（Looking Ahead to the Next Generation of Industry Assurance）

1. 面對產業快速變遷，如何保障水平和垂直應用產品的安全

IBM 代表 Jonathan Sage 表示，現行的 IoT 裝置多與雲端服務連結，但如果雲端服務的安全性無法得到保障，即使 IoT 的裝置是安全的，但也無法保障整體的 IoT 系統為安全可用的。因此，在認證產品安全性時，應進一步思考產品的開發流程。確保開發過程中，相關流程符合資通安

全的規範。產品上市得到認證後，如果有相關資通安全議題或漏洞，在進行更新並發布新的韌體後，認證是否為有效乙節，應回歸到產品開發與後續更新發佈的流程是否通過資通安全相關認證，且開發商或製造商是否已盡最大努力，對風險作出適當的控制措施，藉此取得顧客對產品的信任。

NIST 代表 Michael Cooper 指出，在加速產品認證上，美國亦有類似的情況，更甚者，製造商會對政府施加壓力，以加速加密措施的驗證流程。針對類似要求，當局則是透過工作流程的自動化，以回應製造商之要求。

ENISA 代表 Slawomir Górniak 亦提到在依據歐盟的網路安全法案推動相關產業保障的認證時，須了解市場上的需求與造成之衝擊，例如物聯網相關產品認證的時過長，亦會對競爭力造成影響，進而變成製造商推辭認證的藉口，相關單位應將其納入考量，以免曲高和寡。

2. 認證相互承認

今年歐盟通過的網路安全法授權訂定資通安全認證框架，讓歐盟對 IT 產品有一至性的安全驗證體系與機制，但這也造成 Common Criteria 和網路安全框架融合之議題。各國相互承認他國資通訊技術與相關產品之資通安全認證結果，涉及各國國家利益，一直以來都是一個複雜待解的問題。但 Common Criteria 與網路安全法下的資通安全認證框架逐漸融合是勢在必行的趨勢。融合的過程中，應盡可能以較平穩的方式逐漸靠攏網路安全法下的資通安全認證框架認驗證體系，以逐步達到在此框架下的各種驗證邊準可以相互認可。

三、專題報告

(一) 公共政策（Public policy）

1. Update on ENISA Operations and CSA Implementation

ENISA 資通安全專家 Slawomir Górniak 以「歐盟資通安全框架-

ENISA 的角色」（The EU Cybersecurity Certification Framework- ENISA role）為題，說明網路安全法通過後，ENISA 的定位與職能，以及未來執行該法的規劃方向及首要處理的工作項目。

(1) 網路安全法通過後 ENISA 的定位

ENISA 的法定職掌依性質可區分為【提供專業建議】、【支援政策執行】及【專業社群協力】三部分。【提供專業建議】係針對歐盟境內資通安全議題提出建言或諮詢；【支援政策執行】為協助歐盟會員國與執委會落實政策之執行與進行政策協調；【專業社群協力】指與歐洲境內非政府組織及企業等團體，就資通安全防護事項積極合作。

ENISA 的施政策略則可大致劃分為網路與資訊安全以及數位單一市場兩方面。其政策依據則來自於歐盟之前通過的諸多法律，如網路與資訊安全指令（NIS Directive）、電子身分認證與信賴服務規章（eIDAS Regulation）、支付服務指令（Payment Service Directive 2）、一般資料保護規則（GDPR）、網路安全法及隱私與電子通訊規章草案等。整體施政則以強化歐洲網路系統韌性與培育具競爭力且創新的資通安全產業為目標。

圖 3 ENISA 施政作為之性質

資料來源：講者簡報

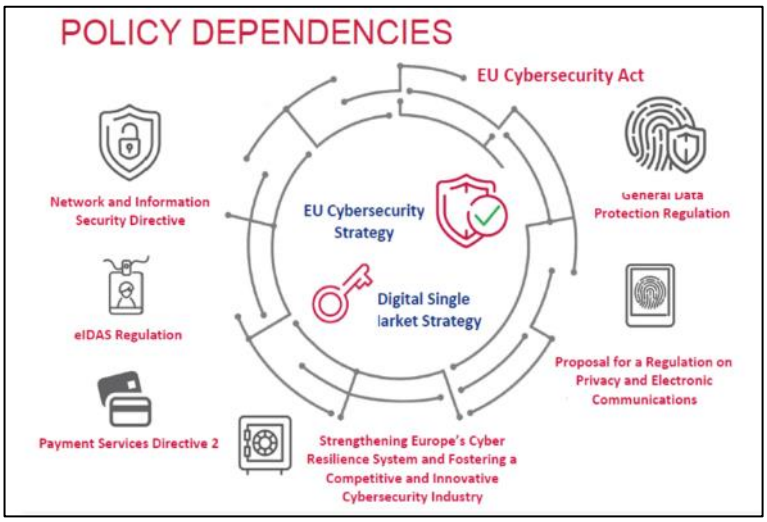

圖 4 ENISA 施政策略及政策依據

資料來源：講者簡報

(2) 資通安全驗證框架：背景、內容、產生程序

在網路安全法通過之前，歐盟境內存在數個互不相容的國家型或區域型安全驗證方案，為促進這些安全驗證方案相互承認或調和，歐盟執委會於 1992 年成立資訊系統安全資深官員小組（Senior Officials Group Information Systems Security, SOG-IS），並於 1997 年簽訂 SOG-IS 相互承認協議（SOG-IS Mutual Recognition Agreement），做為各會員國與各安全驗證方案進行協調與產生資訊技術安全評估共同準則（Common Criteria for Information Technology Security Evaluation，簡稱 Common Criteria 或 CC，即共同準則）的合作架構。

在歐盟建構數位單一市場，一直是歐盟執委會及相關利害關係人所努力的目標。為達成此一政策目標，歐盟執委會係以網路安全法，授權建立資通安全驗證框架。透過法定程序產出適用於歐盟某一領域的資通安全驗證方案[2]，其包括資訊安全要求項目以及檢視這些要求項目達成情

[2] 依據網路安全法第 2 條第 8 款定義，歐盟資通安全驗證方案（European cybersecurity certification scheme）為「在歐盟層級建立的一組包含法規、技術要求、標準及程序的規定，此組規定用於特定資通訊產品、資通訊服務或是資通訊流程之認證或是一致性評估」，同條第 9 款則定義「國家型資通安全驗證方案」（national cybersecurity certification scheme），規定在前款產出的特定認證方案之範圍內，成員國之主管機關發展與採用的資通安全驗證方

形的方法。

資通安全驗證框架整併既有的各類產品資通安全要求，改以三種安全保證級別做為統一的比較基準，並以一個橫跨全歐盟會員國的協調性框架做為往後認證之依據。

程序制定上，依據網路安全法規定，制定一歐盟層級的資通安全驗證方案需經四道程序，包括執委會確認優先發展領域， ENISA 制定與提出候選驗證方案，執委會完成候選方案立法程序，及各會員國符合性評鑑機構（conformity Assessment Bodies）執行驗證。

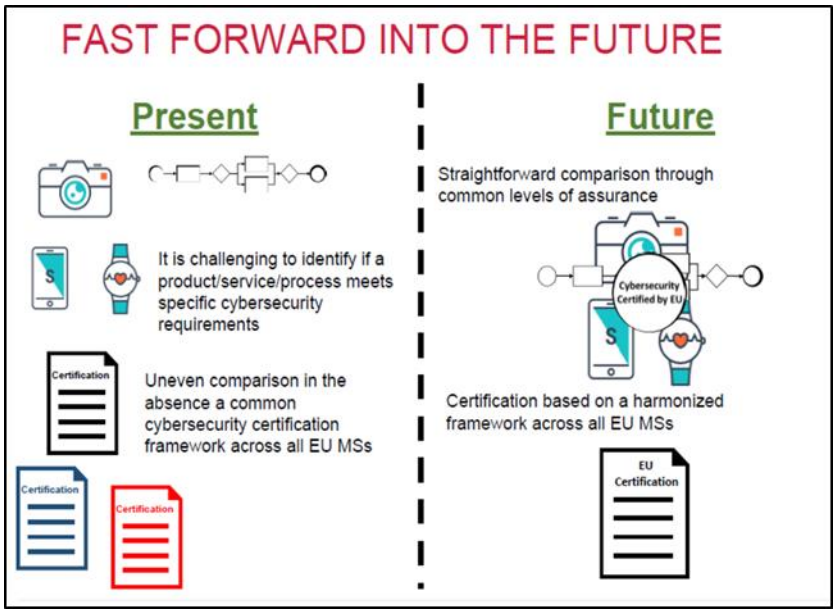

圖 5 資通安全驗證框架示意圖

資料來源：講者簡報

(3) ENISA 法定職掌及首件任務

網路安全法通過後，ENISA 不但成為歐盟永久性組織，年度預算也

案。

由 1,100 萬歐元增加至 1,600 萬歐元，人員編制亦從 80 人上調至 125 人。依網路安全法規定，ENISA 未來在推動資通安全驗證方案的具體工作包括：

- 起草及定稿最終候選驗證方案。
- 擔任利害關係人資通安全認證工作團（Stakeholder Cybersecurity Certification Group，SCCG）秘書單位並與執委會共同主持 SCCG。
- 協助執委會主持歐洲資通安全認證工作團（European Cybersecurity Certification Group，ECCG）。
- 協助檢視已採用的驗證方案。
- 經營及維運資通安全驗證框架網站。
- 協助各國資通安全認證主管機關彼此之間的同儕檢視。
- 提供關於資通安全認證市場方面的諮詢。

歐盟執委會已在徵詢 ECCG 與 SCCG 意見後，擬定首個聯盟滾動式工作項目（URWP），即將 SOG-IS 轉換為首個資通安全驗證方案，並交辦 ENISA 執行。ENISA 已定於今年 11 月 27 日召開專家質詢工作小組（ad-hoc Working Group）會議，就此進行討論。

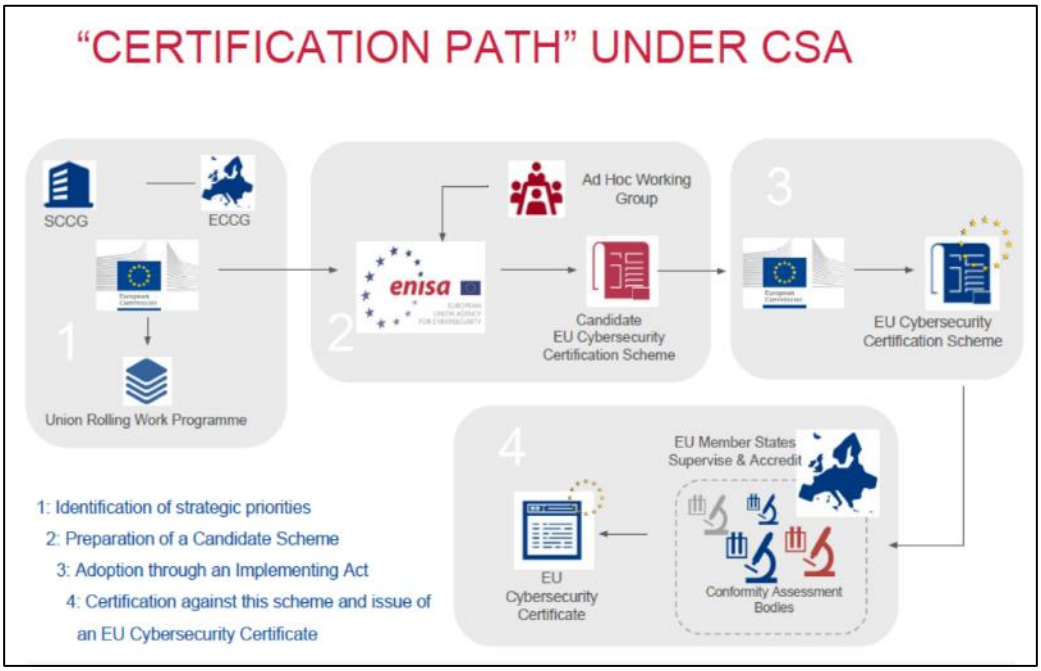

圖 6 歐盟資通安全驗證方案產出程序示意圖

資料來源：講者簡報

2. European Cybersecurity Certification Framework, State of Play

歐盟執委會資深政策官員 Aristotelis Tzafalias，他以執委會的角度向來賓說明「歐盟資通安全驗證框架之現狀」（European Cybersecurity Certification Framework, State of Play）。

(1) 歐盟資通安全驗證框架：一種框架，多種方案

資通安全驗證框架立意係為綜整市場需求端及供給端，除增加消費者或終端使用者對於數位產品與服務的信任，並允許業者向消費者顯示其產品及服務業經公正第三方的安全檢驗。建立共同的資通安全驗證方案對於數位單一市場之建立極為重要，但執委會也清楚，沒有適用各類產品的單一資通安全驗證方案。因此，資通安全驗證框架係採「一個框架，多種方案」（One Framework, many schemes）架構，廣納各類 ICT 產品服務或流程的特定資通安全要求及評估方式，輔以開放、包容與公開的治理過程，使各會員國彼此信任。此外，資通安全驗證框架也考量軟、硬體開發的動態過程，即產品生命週期納入考量，因此諸如資通安全管

理建立、漏洞處理與揭漏、軟韌體更新等，驗證方案將有相應要求。此外，一般使用者亦可透過驗證框架，取得資通安全驗證資訊、框架使用指引、網路威脅減輕措施、資通安全研究人員的聯絡資訊等。

(2) 安全保證級別與符合性評鑑之概述

歐盟資通安全驗證框架的安全保證級別分為【基本】、【實質】及【高級】三級，但實際驗證流程，可區分為【基本與實質】及【高級】兩個部分。當一項特定產品／服務／流程的歐盟驗證方案制定後，國家資通安全驗證主管機關、國家認證機構（National Accreditation Body，如我國財團法人全國認證基金會）及符合性評鑑機構（如我國台灣資通產業標準協會）三種角色即應相應而生。

申請產品／服務／流程資通安全驗證之安全保證級別為【基本】或【實質】者，由符合性評鑑機構（經國家認證機構驗證合格，並取得國家資通安全驗證主管機關授權者）依據歐盟驗證方案之內容，對待測物進行評估及驗證合規（國際、歐盟或國家標準/技術規範）情形。經評鑑合格者，核發適用歐盟之驗證合格證書。反之，申請產品／服務／流程資通安全驗證之安全保證級別為【高級】者，則交由國家資通安全驗證主管機關對待測物進行評估及驗證合規情形，經評鑑合格者，核發適用歐盟之驗證合格證書。

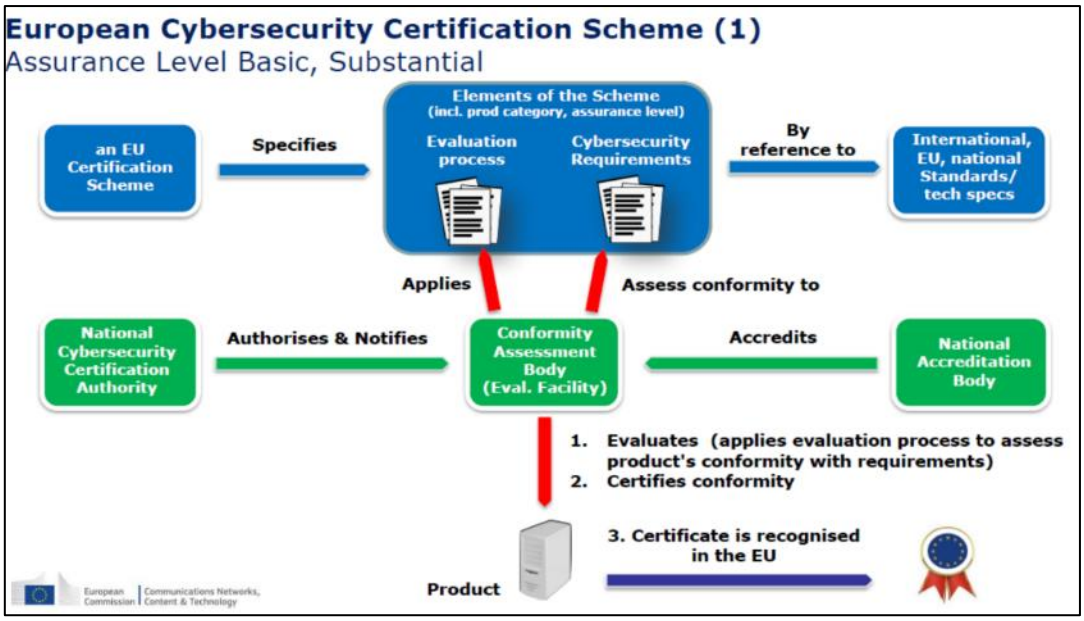

圖 7 基本與實質安全保證之運作機制

資料來源：講者簡報

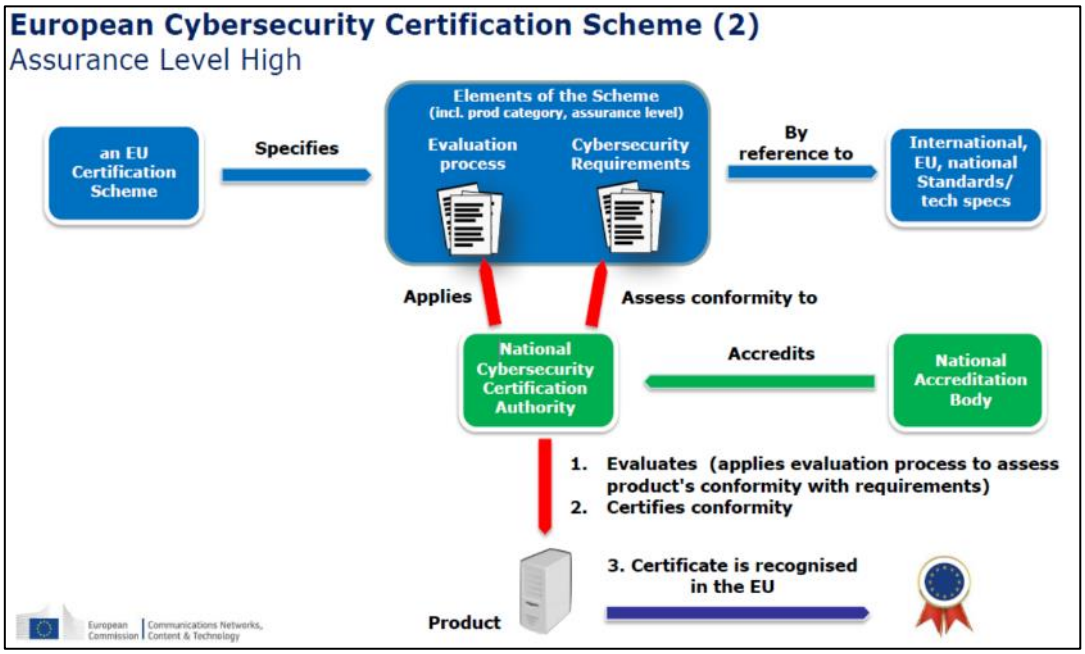

圖 8 高級安全保證之運作機制

資料來源：講者簡報

(3) 資通安全驗證框架的現狀及後續討論事項

截至今年 11 月 18 日止，歐盟執委會除建立 ECCG，並召開了兩次會議外，也責成 ENISA 預先準備建立共同準則基本方案所需資料，並於

9 月 17 日完成 SCCG 諮詢作業。未來，執委會將持續準備歐盟資通安全驗證的滾動式工作項目。

後續制定歐盟資通安全驗證方案時，各界可能關注之議題，包括哪些產品／服務／流程應優先推動資通安全驗證方案之對象，如何評量自願性驗證之有效性，或業者提供 ICT 產品／服務／流程的補充性資通安全資訊應包括哪些內容等。執委會在制定資通安全驗證方案，將綜合考量政策、法規、市場需求、新興威脅等因素，以完備整體規畫。

3. ECSO’s Outlook on the EU Cybersecurity Act

歐洲網路資通安全組織（European Cyber Security Organisation, ECSO）執行秘書 Roberto Cascella 以 ECSO 在歐盟網路安全法扮演的角色為題，摘要說明 ECSO 組織架構、重點工作等。

(1) ECSO：歐盟執委會在資通安全領域的公私協力夥伴

歐洲網路資通安全組織（ECSO）2016 年 6 月在比利時註冊成立，為一非營利組織，同時也是歐盟 Horizon 2020 計畫中，負責資通安全領域的契約型公私協力夥伴（contractual Public-Private Partnership, cPPPs）[3]。ECSO 目前擁有 260 家以上，涵蓋歐洲 29 個國家的產業組織會員，以及 2000 名以上的技術專家。ECSO 旗下設有驗證、標準化小組（WG1）、市場、投資及國際合作小組（WG2）、垂直產業小組（WG3）、支援中小企業及區域小組（WG4）、教育訓練及資通安全意識培育小組（WG5）、研究與創新小組（WG6），以執行資通安全各項工作。

[3] 此 10 項 cPPPs 領域分別是：未來工廠（Factories of the Future）、節能建築（Energy-efficient Buildings）、歐洲綠能車輛計畫（European Green Vehicles Initiative）、可持續性製造產業（Sustainable Process Industry）、光子學（Photonics）、機器人學（Robotics）、高效能運算（High Performance Computing）、未來網際網路的先進 5G 通訊網路（Advanced 5G networks for the Future Internet）、資通安全（Cybersecurity）、巨量資料價值（Big Data Value）。

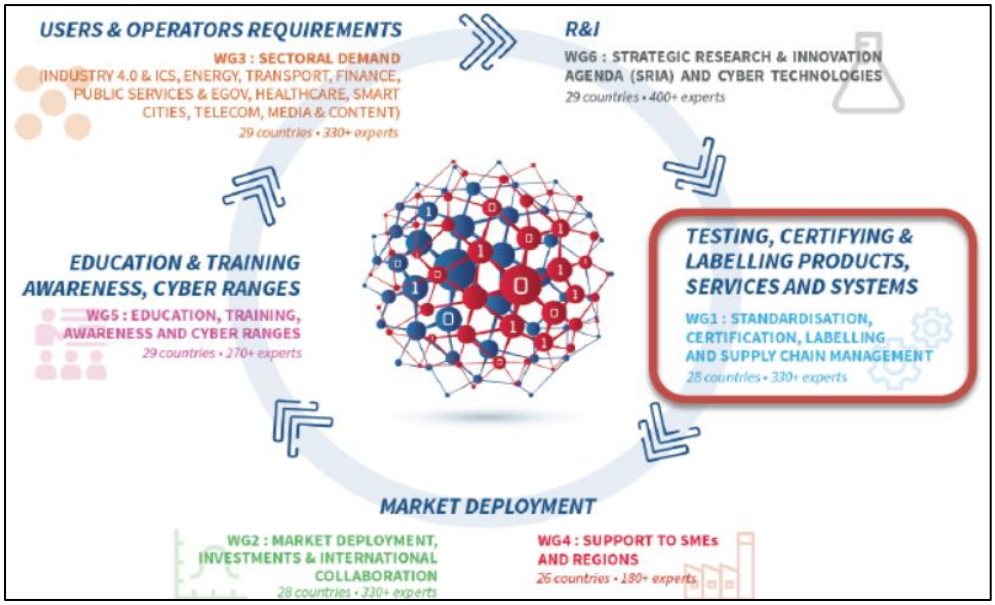

圖 9 ECSO 的 6 個工作小組及其職掌

資料來源：講者簡報

(2) 第一工作小組（WG1）活動概述

WG1 負責資通安全驗證及標準化工作，其任務包括提供歐盟資通安全驗證框架及優先推動標的建議；協助制定資通安全驗證方案相關標準；提供產品內容、系統、服務資通安全評估；提供歐洲境內的供應鏈/價值鏈測試及驗證服務；與歐盟各標準組織、機構合作（標準化事宜與 ETSI、CEN/CENELEC 合作；驗證事宜與 ENISA 協力）等。工作內容包括提供歐盟執委會關於資通安全政策及法制建議（網路安全法之立法制定及建構歐盟資通安全驗證框架的後設方法論上 ECSO 皆有著力）、編撰及出版資通安全教學大綱（State of the Art Syllabus，內容包括當前與資通安全相關的所有技術標準、規範，及這些標準規範的作者、發布日期等。

WG1 為完成所賦予之任務，業擬定兩項執行策略，包括依據歐盟網路安全法制定與資通安全驗證方案相關的可合成性/可組合性的方法、標準、驗證方式；及研究當前風險管理與專業驗證的需求及途徑。

目前 WG1 正在進行中的工作重點包括三項：

- 撰寫可組合性/可合成性文件：作為後續討論網路安全法資通安全驗證方案制定時之參考文件；
- 更新教學大綱：將網路安全法之法規內容及涉及資通訊標準納入
- 盤點挑戰及優先事項：盤點未來工作及投資方向可能面臨的挑戰及應優先挹注資源之項目。

(3) 資通安全驗證方案的可合成性/可組合性

此項工作的目標是建議未來的資通訊驗證方案之內容應具備可組合性/可合成性。組合／合成可分為同一驗證方案內（標準模式）與跨驗證方案兩種類型。

- 同驗證方案的組合／合成（標準模式）：產品係由不同供應商（different suppliers）提供的不同區塊（different building blocks）所構成。不同區塊先採相同方法進行驗證，最終產品再採用同樣方法進行驗證。但區塊經驗證者，無須再次驗證，新的評估得直接引用之前驗證結果。此模式重點在於專注整合及正確使用驗證功能。
- 跨驗證方案的組合／合成：產品不同區塊係經不同方法論驗證，最終產品採某方法論進行驗證。但區塊經驗證者，新的評估得直接引用之前驗證結果的部分內容。此模式需注意的重點是，要仔細定義實現可組合性的規則（rules for achieving composability）。

資通安全驗證方案如具合成性／組合性，驗證與評估證據即可重複使用、各應用領域可以客製化水平組件，降低驗證成本與改善整體文件處理速度，有效縮短產品進入市場的時間，有助資通安全驗證方案之推動

未來要推行資通安全驗證方案的組合／合成，需要考慮三點：

- 驗證方案需要仔細定義哪一類與驗證相關的評估證據（以及評估層級）能夠用於組合性評估；
- 組合後的驗證方案需定義額外的評估準則（additional assessment

criteria），以涵蓋引入組合後可能產生的驗證盲點；

- 最終產品仍需正確執行驗證功能。

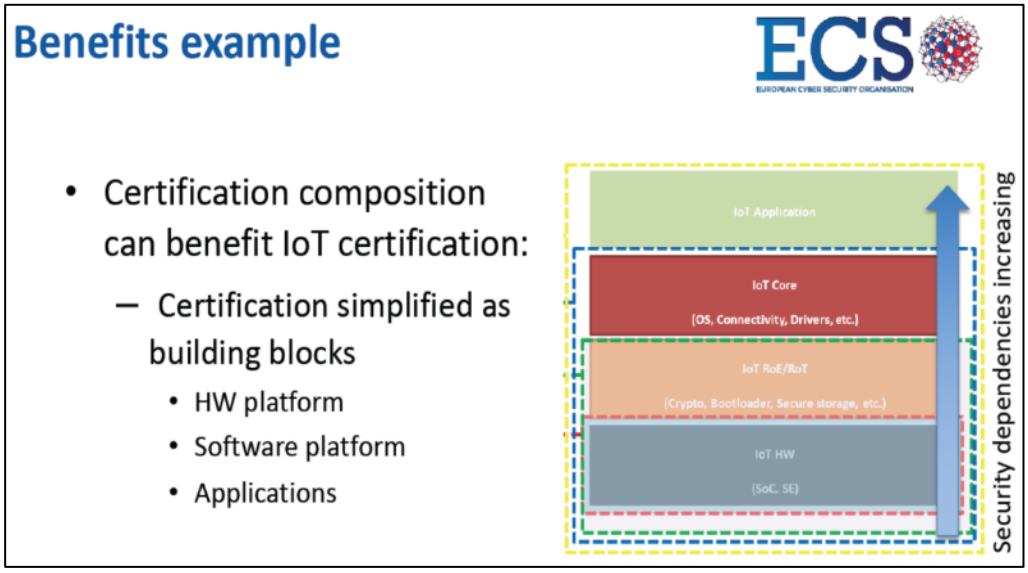

圖 10 ECSO 建議驗證方案採組合式架構所生效益

資料來源：講者簡報

4. Security Needs to be Consistent—The Role of Process in the Cybersecurity Act

英國國家資通安全中心（National Cyber Security Centre, NCSG）國際安全處的主管 David Martin，他針對網路安全法裡面的一些關鍵概念如資通安全（cybersecurity）、安全保證（assurance）、流程（process）、級別（levels）進行分析，並指出這些概念內涵的不一致以及對後續實務的影響。

- 資通安全（cybersecurity）：資通安全不僅是一個防護盒（boxes）或防護平臺（platforms）。從事資通安全工作，將整體性／系統性／生命週期納入考量是極端重要的。因此，在制定資通安全標準及驗證方法時，軟硬體的開發、支援、作業流程都是應考量之因素。歐盟網路安全法將產品／流程／服務納入資通安全驗證框架實允情允理。
- 安全保證（assurance）：以前英國很多資通安全專家都建議設置的網路防火牆，應至少取得共同準則（Common Criteria）第 4 級安全保證（EAL

4）。不過這類建議卻輕忽許多方面，例如許多第 4 級安全評估缺乏內在的安全保證，或是攻擊者不一定會從正面攻擊等。此外，NCSG 幾年前也有相關統計指出，取得產品驗證證書對於產品安全本身只有很小的益處。因此目前 NCSG 的觀點是，當一個產品要能合理的運作，產品如何設計、開發與維運才是最重要的安全考量。

- 流程（process）：歐盟網路安全法將資通安全概念擴展至過程，這並非首創之舉，至少歐盟其他國家在此前已有類似概念，比如英國數位文化媒體運動部（DCMS）於 2019 年 2 月時發布「給製造業的消費者物聯網實踐準則」（Code of Practice for Consumer Internet of Things （IoT） Security for manufacturers）就強調安全設計（Secure by Design）或是德國聯邦資訊安全辦公室（BSI）2018 年 11 月發布「關於連網醫療裝置的資通安全要求」（Cyber Security Requirements for Network-Connected Medical Devices）。因此隨著網路安全法的施行，接下來一個重要問題即是該如何「評估過程」（assess processes）？要做到這件事在實務上會是相當困難的一件事，而且還可能牽涉到智財權的議題。
- 級別（levels）：網路安全法設定安全保證級別，分為基本、實質、高級，不過在該法 51 條 i 款規定「ICT 產品、資通訊服務、資通訊流程皆應屬安全預設及安全設計」，所有級別均須符合此規定，也因此難以辨別三種級別之間的差異性。即使此三種級別之區分指涉過程驗證的形式，也會遭遇一些問題，比如現存的某些流程如能力成熟度模型（Capability Maturity Model, CMM）即是基於級別概念運作，因此安全保證級別可能無必要；或實務上難以運作，因為級別概念對於開發共同準則驗證沒有助益。

(二) 行業調整（Industry Alignment）

1. ETSI Security Evaluation Standardization Initiatives

ETSI 的技術長 Sonia Compans 講述有關 ETSI 在信託服務、5G 網路、

消費者 IoT 安全等領域之資通安全倡議參與成果。

信託服務主要講述對於電子識別與信託服務的認證與相互授權，例如歐盟會員國的學生可以線上註冊歐盟會員國的大學、公民可跨境在國外填寫報稅或是企業可以參與會員國的公開招標。既稱為數位市場，即應該有一大家共同信任的電子識別。ETSI 業訂有相關標準來強化電子識別之信託服務的整合，俾推動歐盟的信託服務的相互認證。

在 5G 網路安全的部分，ETSI 提出 Network Equipment Security Assurance Scheme （NESAS），即網路設備安全保證方案，該方案起源於 GSMA 與 3GPP 共同定義行動網路設備安全保證方案，該方案主要精神在於透過評估檢測網路設備以了解網路設備是否有達到安全基準，此外亦會評估設備製造商的設計、生產等過程是否符合安全要求以及是否依照相關標準指引開發，也就是會從設備本身以及製造商等兩方面進行評估，以確保資通安全。

IoT 安全部分，根據 Gartner 的預測，在 2020 年全世界將有 129 億臺以上的消費型連網裝置，然而大多數的連網裝置並沒有完善的資通安全防護，也因此 ETSI 在消費者 IoT 安全認證領域推動 TS 103 645 的標準。此標準為全球第一個物聯網產品相關的通用標準，此標準亦向 GDPR 對齊。此標準並非一次解決或消除消費者在 IoT 產品中的所有風險與一路，而是以結果導向的方式透過各種安全控制的手段來降低資通安全風險，其主要要求包括：無通用預設密碼、資通安全漏洞通報管理方法、軟體持續更新、資料保存安全、安全傳輸、減少可被攻擊的面向、軟體完整性的確保、個資確實保護、系統強韌性、遠端感測數值監控、消費者個資刪除、簡化設備安裝與維護、驗證輸入數據等。

綜觀上述 5G 網路與 IoT 資通安全評估方法，可知資通安全除了設備本身，包括上下游供應鏈之生態系管理、系統強韌性規劃等都是重要課題。

2. Lessons Learnt in the Commercial Use of Security Certification—From Setting Standards to an Innovator’ s Perspective

Trusted Computing Group （TCG） 為一非營利組織，其設定宗旨為開發、定義與推動開放、中立、全球的產業規格及標準，並支援以硬體為基礎的信任根基（Root of Trust）及具互通性的信任運算平臺（Trusted Computing Platform）。

TCG 技術強項在於信任平臺模組（Trusted Platform Module）、信任網路通訊（Trusted Network Communications）及網路安全與自我加密儲存裝置。在信任運算架構中，TCG 發明信任根基的儲存、回報與量測，並設計一具信任根基的更新方式以強化韌體安全；同時，TCG 也發明具信任根基的偵測與復原技術，以設計具強韌性之硬體。在相關技術之驗證日益重要下，TCG 亦已提供相應之驗證。但在網網相連的 IoT 時代，

產品製造商或供應商可藉由資通安全評估或驗證，增加其資安防護的透明度，並提升終端使用者對該產品的信任。然而現行資通安全驗證方案價格昂貴，且時間冗長，實無法跟上資通安全威脅進化的腳步。IoT 時代，更多的運算裝置融入日常生活、也有更多的資料被蒐集並在網路邊緣進行運算，資通安全風險及威脅更不容忽視。資通安全驗證方案除應接軌國際標準外，更應針對資通安全風險及威脅快速變遷的時代而改進

為了降低資通安全風險及避免威脅帶來的衝擊，應該鼓勵廠商在設計開發階段採用自願性的資通安全驗證方法，並針對驗證進行分級，例如自我宣告、基本的第三方驗證到更進階的第三方驗證，透過驗證讓資通安全融入開發流程，從源頭即開始注重資通安全。

3. Vendor Self-Assessment—The Good, The Bad, and the Ugly

在歐盟網路安全法案中，允許製造商或供應商針對 ICT 產品／服務／流程進行自我評估，但自我評估是否真的可行？

講者認為有些時候是可行的，而在產品／服務／流程三者當中，又以服務與流程會有較佳的效果，主要是因為其在資通安全的保證要求較低，而產品的資通安全要求通常較高。但即使對於資通安全保證要求較低，仍有使用上的限制。從風險承擔者的角度視之，產品／服務／流程的風險承擔者不同，服務與流程的承擔者為服務供應者，供應者有動機將事情做對、做好，但產品的風險承擔者為使用者而不是開發者。

對於服務、流程之供應商，把事情做對、做好可以避免潛在的資通安全問題，調適服務或流程變更，以強化資通安全也相對容易。自我評估的結果可立刻回饋到資通安全管控措施，所以服務、流程之供應商會有強烈動機來執行自我評估。

自我評估對於產品開發者來說，亦有相當好處。開發者是最了解其產品的人，相較於第三方，有更深入的知識，也沒有學習曲線的困難，且評估時可取得所有資訊。因此，倘若能由開發者進行自我評估，應該是最好的選擇。然而在大多數的狀況下，資通安全並非產品開發的第一要務，尤其自我評估的時間和成本通常不在產品開發的預算之內，故自我評估發現的事項通常會被忽略。除了上述議題外，倘若自我評估的結果為負面或不如預期時，常會陷入天人交戰的情況。

上述內容亦反映出國內相關 ICT 產品的開發現況，除非是有法令法規或是合約要求，通常資通安全並不會是產品開發的第一優先順位，主管機關宜考量在對產品開發者衝擊最小的情況下，適度的要求產品的資通安全自我評估與相關監理或稽核工作。

4. ISCI WG （International Smartcard Initiative） Who Are We? What Do We Do? How Do We Do It? And How Do We Contribute to The EU Cyber Act?

本場次係介紹 ISCI WG1 及其工作職掌。ISCI 全名為 International Security Certification Initiative，其工作項目如下：

- 協助詮釋 Common Criteria 在資通訊領域-軟硬體安全之認證事宜，並使

Common Criteria 容易為外界所理解、應用，以確保認證最佳化、簡明及清楚。

- 推動 SOG-IS 中 17 個會員國對於認證產品評估結果間的相互信任與承認，並定義、支援及推動一適用於 Common Criteria 的資通安全評估與認證方法（即通用框架），並納入所有評估及驗證流程中的角色，以強化與調和各國間之評估流程並採一致做法。

5. Update on The EU Cybersecurity Act: Is The Feared Balkanization of Common Criteria Being Reversed?

此場次主要在探討 Common Criteria 的巴爾幹化，及 EU Cybersecurity Act 能否反轉巴爾幹化，並讓歐盟會員國對於資通安全評估有一致的參考框架，促使會員國間能相互信任其評估及驗證結果。

EU Cybersecurity Act 授權 ENISA 成為歐盟永久機構，並強化 ENISA 之地位與授權，同時建立一個歐洲 ICT 產品資通安全驗證框架（即 Cyber Security Framework），其目的係為強化歐盟內網路的撓性（Flexibility）及應變能力，並調和相關標準，以達成符合歐盟數位單一市場之目標。

ENISA 將協助發展歐盟會員國所承認之自願性歐盟驗證框架（包括相關技術性要求、標準及程序等內容），以確保 ICT 產品／服務／流程在資通安全方面是安全無虞的。但安全設計原則係要求資通安全防護應落實於產品設計及開發階段，然而 ICT 產品／服務／流程的初始設定，在衡酌多數消費者不具相關知識或技術原理，設定須簡單、明瞭且易用。如何衡平，仍待多方努力。

6. The Certification Landscape and What Industry Needs

各種裝置或系統，佈建後我們仍需維持其資通安全，尤其是當他連上網路後，更要假設他是脆弱的，並增加相關資通安全防護措施，如定期更新韌體與軟體、檢查裝置是否有實體入侵的可能性、開啟資料加密、

當裝置不用時關閉、考量利用區塊鏈來強化資通安全等。

針對產品資通安全驗證部分，應考量裝置測試與流程驗證兩個面向。裝置測試可以找出產品的脆弱性，釐清其是否符合資通安全相關標準或技術規範，但相關測試僅限於該裝置而不是整個應用系統或情境。流程驗證則可以瞭解到公司的整體資通安全政策與規劃，該驗證亦可適用於所有產品的流程，但僅限流程而不是產品測試，而且如果廠商惡意欺瞞，其脆弱性將不容易發現。

(三) 成功標準（Standards for Success）

1. CEN-CENELEC JTC13 WG3 Security Evaluation Standardization Initiatives

JTC13 WG3 於此次 EU Cybersecurity Act 會議中，提出一 ICT 產品資通安全評估方法的概念性框架。其概念源於 2019 年歐盟之網路安全法案強調需對所有 ICT 產品進行資通安全評估，衍生出不同資通安全驗證標準間相互調合之需求。

多數歐盟會員國需要一簡單、易用、有效，且經歐盟認可的資通安全評估標準框架，以輕易調和並齊一不同資通安全評估方法，俾達互通性。此外，透過推廣與部屬該評估框架，可讓設備製造商取得資通安全驗證與競爭優勢，也能以此贏得使用者與顧客的信任。

驗證單位可依申請者需求選擇適當的評估方法，並依照擇定方法之資安要求進產品行驗證。該框架也提供足夠的彈性，並針對不同需求、技術、市場、使用情境等建立評估與驗證方法。框架相關利害關係人包括：

- 產業界：主要受惠於單一資通安全評估/驗證框架，包括產品資通安全評估僅須花費適當的驗證成本。
- 政府單位：可推動採購經資通安全驗證合格之產品。
- 消費者：對於 ICT 產品有更高的信心
- 非政府組織：瞭解產品資通安全透明度

2. Comparing National Lightweight Methodologies around Europe

目前歐洲評估 ICT 產品的資通安全，多依 Common Criteria 規定辦理。採用 Common Criteria，係該準則之評估面向包括產品測試、生命週期、產品文件，且有保證級別之分，並盛行於國際間。但執行 Common Criteria 規定之評估時間過長、應交付之文件繁雜，且驗證費用高昂，除中小企業實難以負荷外，對於生命週期有限或搶上市商機之 ICT 產品，亦造成驗證阻礙。

為求產品資通安全驗證時間與測試要求之平衡，爰市場發展出一套輕量級資安驗證方法。輕量級資安驗證係指僅驗證部分或特定功能，然而驗證項目之擇定，須由具相關經驗及相當技術背景的評估人員始得為之，故輕量級資安驗證是否妥切，端視評估人員之專業能力而定。而且歐美作法亦有所差異。

美國試圖將 Common Criteria 視為一合規工具，並盡可能將其自動化及重複使用，同時省略滲透測試與弱點分析等評估；此舉，雖降低資通安全保證的深度，但仍可應用在沒有已知弱點的大型供應商產品上。歐洲則是採用情境分析，並區分為需高度保證與與低度保證的情境；在高度保證的情境中，採用傳統的 Common Criteria 規定，並盡可能地重複使用與維持軟體變更後的相關驗證；低度保證的情境會建立敏捷的產品評估與驗證標準，並在限制條件下執行弱點分析與滲透測試。

目前，歐洲輕量級資安驗證之執行案例，大多應用在行政部門，但未來將可逐漸推廣至消費者市場，且各國間的驗證也可相互調和。為調和歐盟會員國間不同之輕量級資安驗證，JVC WG3 正在研擬一通用驗證框架。

3. Implementing and Maintaining a Cybersecurity Program—The Role of Standards

美國於 2002 年發布「聯邦資訊安全管理法（Federal Information Security Management Act，簡稱 FISMA）」，以法的形式規範美國聯邦政府

應盡之資訊安全管理責任，並據以實施，以奠定及強化美國資訊安全管理措施。

FISMA 主要內容涵蓋：

- 資訊安全與國家安全之定義
- 聯邦政府各機關之責任
- 資訊安全之年度評估
- NIST 於國家之定位與法律位階，並授權 NIST 開發資通安全標準。

此外，FISMA 也定義一風險管理框架以預防來自天然與人為的威脅，確保聯邦政府之資訊安全。其框架內容包括：資訊系統分類、控制措施之挑選、控制措施之實作、控制措施之評鑑、資訊系統之授權、安全狀態之監控等，聯邦政府各部門須依照上述框架建立資通安全計畫並據以實施。

NIST 亦依 FISMA 授權，分別建立相關指引。與 FISMA 風險管理框架相關之指引，包括 NIST SP 800-60 的資訊資產或系統分類、SP800-53 的控制措施挑選、SP 800-70 的控制措施實作、SP 800-53a 的控制措施評鑑、SP800-37 資訊系統授權、SP 800-37 與 SP 800-53a 對於安全狀態監控等一系列指引。此外，NIST 亦針對非聯邦機構之民間關鍵基礎設施提出 Cybersecurity Reference Framework，作為民間單位訂定資通安全防護計畫之參考。

此外，FISMA 亦授權掌管聯邦政府預算的「預算管理局 （OMB）」，督導聯邦政府建置及施行資訊安全保證措施，並向國會報告聯邦政府資訊安全工作執行情形等。

另美國在歐巴馬政府時代，因應雲端運算世代的來臨，為提供雲端產品與服務一安全評估、授權方式、持續監控之標準與方法，亦發布聯邦雲端運算安全標準（Federal Risk and Authorization Management Program，簡稱：FedRamp）。透過 FedRamp，聯邦政府即可了解雲端服務供應商資

通安全防護能力，亦為聯邦政府選擇供應商的標準。

(四) 雲端與 GDPR 框架（Cloud and GDPR Frameworks）

1. Toward the European Cloud Security Certification Scheme: The CSPCERT Final Public-Private Recommendation

本場專題演講係由 Cisco 代表 William Ochs 主持，講述未來歐盟資通安全驗證框架下之雲端資通安全驗證方案（European Cloud Security Certification Scheme）之設計構想以及最終建議，並由德國經濟及能源部代表 Thomas Niessen、法國資訊安全署（ANSSI）代表 Aurelien Leteinturier、Google 代表 Saurabh Ghelani、ENISA 代表 Slawomir Gorniak 等四位依序報告。

(1) CSPCERT 是什麼？

CSPCERT 為歐洲雲端服務供應者驗證（European Cloud Service Provider Certification）工作小組，其成立係為提供歐盟官方組織如歐盟執委會、ENISA 及各會員國，有關歐洲雲端服務資通安全驗證建議。CSPCERT 由 32 名成員創立，成員組成涵蓋政府、企業、非政府及非營利團體等。除 32 名創始成員外，另有 29 名觀察成員。以地理區域角度視之，涵蓋 52 名歐盟成員與 16 名非歐盟成員。

CSPCERT 最終目標係提出一驗證工具包（certification toolkit）供各界參用，工具包將內含三個階段目標（Milestone）及相關文件。階段目標包括產出【驗證對象】、【評估與稽核的方法】及【執行 CSP 驗證方案的人員及方式】。另 CSPCERT 並已於今年 6 月發布「雲端服務供應者驗證方案執行建議報告」（Recommendations for the implementation of the CSP Certification scheme）[4]。

- 驗證對象（what to certify）：將 ISO、SecNumCloud 等種標準所設定的資通安全目標，統合為具廣泛性且和諧一致的驗證對象；

[4] 報告下載網址 https://drive.google.com/file/d/1J2NJt-mk2iF_ewhPNnhTywpo0zOVcY8J/view

- 評估與稽核的方法（how to evaluate and audit）：綜合 ISO、ISAE 等國際標準組織之評估、稽核方法，並將其方法論協調一致，以作為雲端服務供應者驗證（CSP certification）的方法論；
- 執行 CSP 驗證方案的人員及方式（who and how to implement a CSP certification scheme）：定義 CSP 驗證方案的治理方案與指導原則，以協助日後歐盟 CSP 驗證方案之執行。

(2) CSPCERT 與 CSA 相關部分

CSPCERT 於今年 6 月發布「雲端服務供應者驗證方案執行建議報告」，所提的三點一般性建議，分別是：

- CSPCERT 未向歐盟執委會與 ENISA 建議全新的驗證方案，所提出建議主要基於當前產業界及國際採用之實踐準則、方案或標準，其相關內容亦直接扣合歐盟網路安全法之要求。
- CSPCERT 建議歐盟執委會應將適用全歐盟範圍的雲端安全驗證方案之發展，納入歐盟滾動式工作項目（URWP）
- CSPCERT 請求 ENISA 基於 CSPCERT 所提出之內容，提出候選驗證方案。

(3) CSPCERT 解決方案所生影響

CSPCERT 所提雲端安全驗證方案，如被納入歐盟資通安全驗證架構的候選計畫，將促成一致性的雲端安全驗證要求出現，驅動泛歐盟體系承認此一實際上已使用的雲端安全驗證。對於雲端服務提供者（CSPs）、中小企業及客戶、主管機關三方所生影響分別為：

- 雲端服務提供者

  由於 CSPCERT 建議的雲端安全驗證方案精簡及強化現存的資通安全要求，因此預期將致使歐盟境內更多地區採用雲端服務；同時雲端安全驗證方案也為新興的未來法規及特定產業部門的資通安全要求提供制定基準，並且降低與多國驗證框架相關的第三方稽核的組織成本。

- 中小企業及客戶

  雲端安全驗證方案提供標準化框架，有利中小企業及客戶瞭解雲端服務供應商所提方案之安全性。另驗證方案中所提協助組織簡化法遵優先事項，大幅降低雲端服務提供者法遵成本，可促使更多企業於不同區域進行商業活動，並帶動中小企業進行數位轉型。

- 各國主管機關：

  各國主管機關可利用 CSPCERT 的法遵事項，滿足產業對於資通安全的特定要求。且整個歐盟地區存在統一的做法，採用雲端安全驗證方案除可降低國家管理成本，也增強與其他國家主管機關的合作程度。主管機關也能藉由採用雲端安全驗證方案達成資通安全知識與最佳實踐方式之共享，並以此簡化相關資訊以擴散至其他行業；採用雲端安全驗證可以視作促進企業進行數位轉型的方式。

2. The EU-SEC Framework

本場次係由雲端安全聯盟（Cloud Security Alliance）代表 Eleftherios Skoutaris 分享歐洲資通安全驗證框架計畫(European Security Certification Framework，The EU-SEC Framework Project）的執行情形。

(1) EU-SEC Framework 概述

歐洲資通安全驗證框架計畫為歐盟資助的專案型計畫，其運作資金來自地平線（Horizon）2020 計畫，執行期程為 2 年（2017 年 1 月 1 日起至 2019 年 12 月 31 日止），計畫參與者共 9 名企業及非營利組織。此計畫成立背景源於當前歐盟資通安全市場存在過多的資通安全驗證方案、其驗證方式也缺乏明確性、各國接受之驗證亦不均等，致使 ICT 產品驗證成本過高且缺乏效率。因此本計畫旨在創建可整合現有各類資通安全驗證方案的資通安全驗證框架，使當前的驗證及安全保證方法可以共存，進而提供雲端服務提供者（Cloud Service Providers, CSPs）有效率的雲端安全驗證，提供雲端服務客戶（Cloud Service Customers, CSCs）透明可

控且具保證的服務，以及提供涉及各國稽核機構與競爭主管機關多方稽核服務。本計畫的具體產出包括多方互相承認框架（Multiparty Recognition Framework, MPRF）、持續性稽核的驗證（Continuous Auditing-based Certification, CABC）及符合 GDPR 規定的隱私行為準則（Privacy Code of Conduct for GDPR compliance, PLA CoC）。隱私行為準則因非屬本次研討會討論議題，故未做介紹。

(2) 多方互相承認框架

多方互相承認框架（MPRF）的執行目標有三點：

- 驗證成本極小化，此係指當雲端服務提供者已經取得 X 型驗證時，再行取得相關的 Y 型驗證，其取得成本、程序之花費應降至最低；
- 協助雲端服務提供者及雲端服務客戶正確理解各類方案中關於資通安全、隱私、稽核要求的文義；
- 簡化雲端驗證過程以提昇效率、增加安全保證並降低重新評估的花費。

在多方互相承認框架的運作中，利害關係人包括驗證方案擁有者或主管機關、治理機構、獲得授權的稽查人及雲端服務提供者。驗證方案擁有者或主管機關應參與框架運作並提供指導、治理機構則負責運行此框架、獲得授權稽查人則負責支援申請者相關要求，雲端服務提供者則於申請後得到相關資訊。

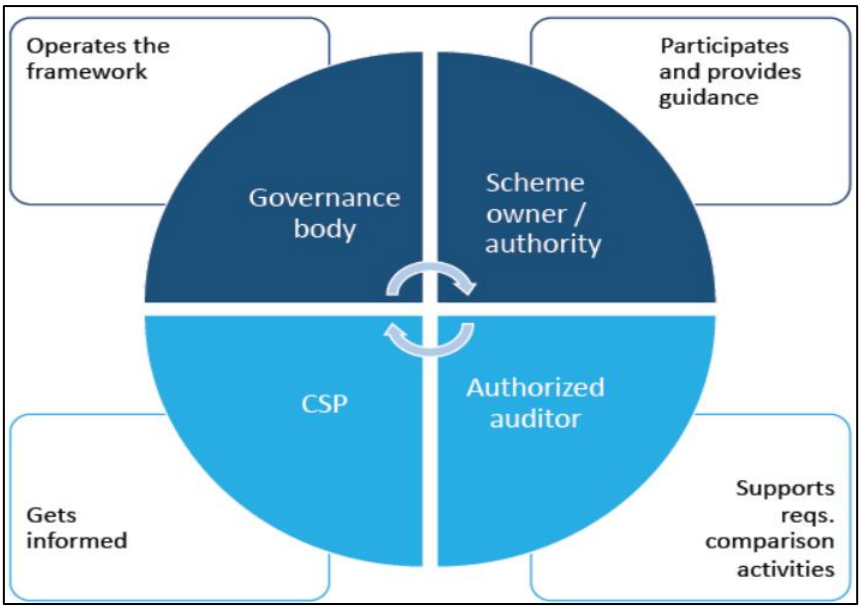

圖 11 多方互相承認框架中各利害關係人之職責

資料來源：講者簡報

多方互相承認框架整個運作可分為評估(Evaluate)、執行(Execute)、治理(Govern)三個部分。【評估】係指依據現存的指導原則(principles)、評量標準（criteria)、資通安全要求（requirements）進行評估；【執行】係檢視安全控制／要求、隱私要求、稽核要求是否符合 MPRF 建置之綜合資料庫內容。【治理】指變更管理流程以及申訴管理流程二類，用以監督評估及執行部分。

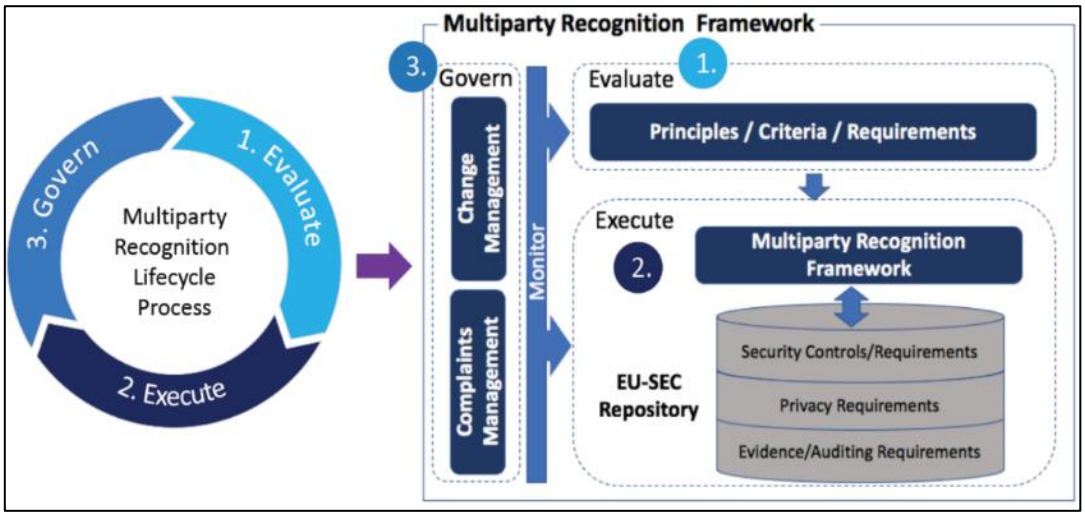

圖 12 多方互相承認框架運作週期示意圖

資料來源：講者簡報

(3) 持續性稽核的驗證

EU-SEC 框架另一重點，以「持續性稽核驗證」取代傳統型驗證。傳統型驗證係金融業或醫療業等高度管制產業所採用的驗證方式，且通常以定點（point-in-time）、定期（period- of-time）方式執行資通安全驗證。但對於高度變動、高風險環境的雲端產業而言，這種驗證方式不足以提供其所需的高等安全保證與透明性。以稽核週期為例，傳統型驗證通常為 6 至 12 個月，其空窗期即產生安全上的不確定性。因此 EU-SEC 框架呼籲應以「持續性稽核驗證」補足傳統型驗證無法涵蓋的領域。Eleftherios Skoutaris 也強調持續性稽核驗證並非試圖取代傳統型驗證，而是互為補充，使雲端服務提供者在取得相關驗證更具彈性，且更能確保其安全與透明性。

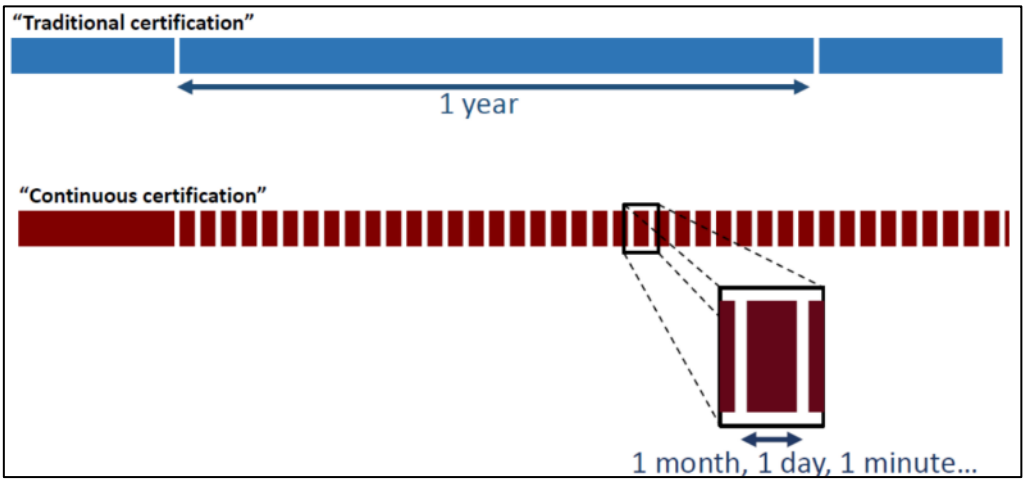

圖 13 傳統型驗證 v.s 持續性驗證 稽核週期示意圖

資料來源：講者簡報

傳統型驗證之驗證對象僅為控制目標（control objectives），但持續性稽核驗證之驗證對象，更進一步細分為安全屬性（security attributes）、度量（metrics）、服務等級目標及服務質性目標（service level objective & service qualitative objective）三類，並採用自動化評估方式進行驗證。

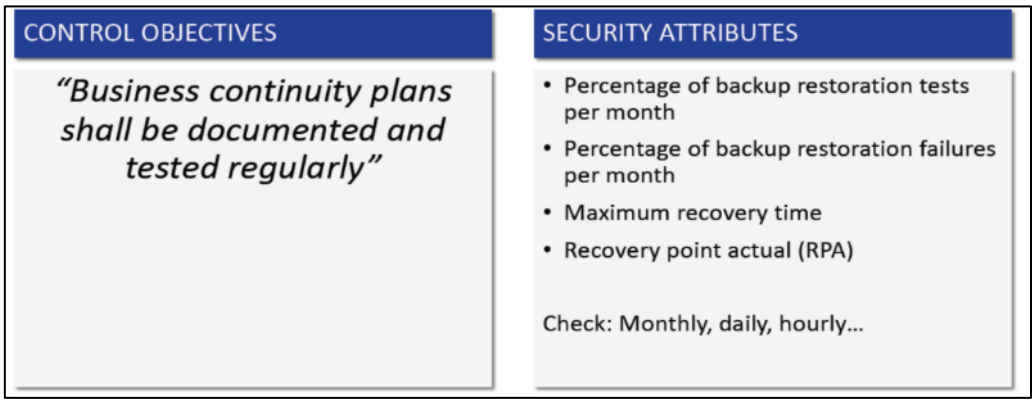

圖 14 傳統型驗證 v.s 持續性驗證 驗證內容

資料來源：講者簡報

持續性稽核驗證包括預備作業（preparation）、證據蒐集（collection）、測量證據（measurement）、評估目標（evaluation）、提供驗證（certificate）等 5 個步驟。其中預備作業包括定義服務等級目標及服務質性目標，以描述整個控制過程，並決定評估的頻率、範圍及服務等級目標及服務質性目標。經評估、驗證所蒐集的驗證證據後，驗證不合規定，則重新蒐集證據，並繼續次輪之驗證程序。

此種基於持續性稽核的驗證亦可扣合歐盟網路安全法提出的三種安全保證等級，比如在基本等級只需雲端服務提供者採取持續性自我評估（continuous self-assessment）；實質等級層面則採用持續性自我評估佐以擴充型驗證（extended certification）；高安全保證層面才需採用持續性稽核驗證。

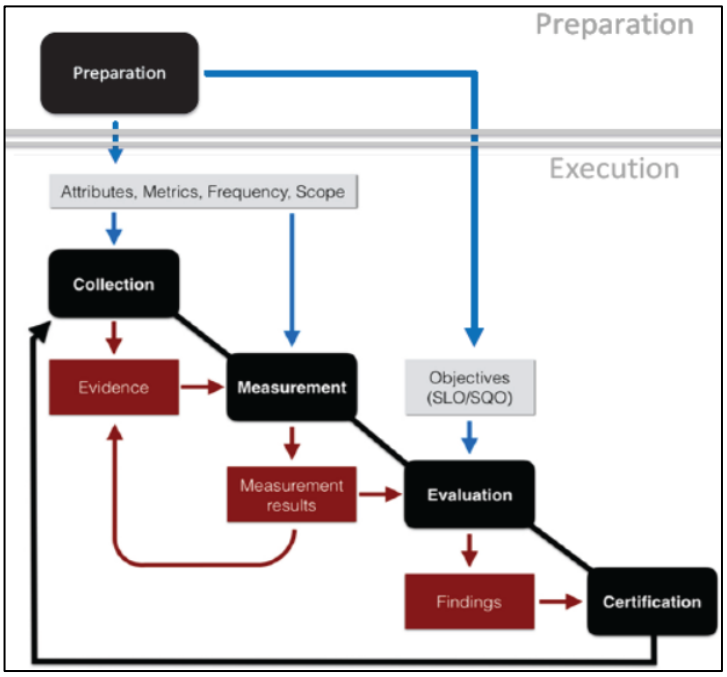

圖 15 持續性稽核驗證方法論

資料來源：講者簡報

3. Addressing GDPR Requirements Using the ISO/IEC 27701 Standard. Is the CSA Looking At It?

第三場專題報告由英國標準學會（British Standard Institute, BSI）代表 Willy Fabritius 介紹 ISO 27701 標準，並由微軟代表 Alex Li 補充說明。

(1) ISO/IEC 27701 制定緣由、條文結構

ISO/IEC 27701 隱私資訊管理(ISO/IEC 27701:2019Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines) 為國際標準組織（ISO）於 2019 年 8 月發布之隱私資訊管理系統(Privacy Information Management System, PIMS ）最新國際標準。ISO/IEC27701（發展時期標準編號為 ISO/IEC 27552）係延伸 ISO/IEC 27001 資訊安全管理系統和 ISO/IEC 27002 資訊安全控制措施，除明定個人識別資訊（Personally Identifiable Information，PII）的控制者（controllers）與處理者（processors）之實務指引（guidance）與要求（requirements）外，並增進個人識別資訊控制者彼此間之透明度、

提供管理個人識別資訊流程的方法，及協助個人識別資訊處理者向客戶提供獲得有效管理之保證。ISO/IEC 27701 條文內容亦對應至包括 ISO/IEC 29100 隱私框架、歐盟一般資料保護規則（GDPR）、ISO/IEC 27018 保護個人識別資訊、ISO/IEC 29151 個人識別資訊保護實務等法規及標準，目的在於提供隱私保護之指引及要求，以協助組織管理個人資訊以利害關係人提供明確處理流程，以及協助組織遵守各國隱私法律規定。

ISO/IEC 27701 計有 8 條文及 6 個附錄（Annex A~F）。條文 1 至 3 分別為適用範圍、參考規範、術語定義與縮寫；條文 4 為一般性要求，條文 5 及條文 6 分別對應 ISO/IEC 27001 與 ISO/IEC 27002 之特定要求。條文 7 和條文 8 則參照 ISO/IEC 27002，分別以個人識別資訊控制者及處理者的角度，提供額外指引。附錄 A 及附錄 B 為規範性附錄（Normative Annex），羅列個人識別資訊控制者與處理者可參照之控制目標及控制措施，以補充條文 7 及條文 8 不足之處；附錄 C 至 F 為資訊附錄（Informative Annex）。其中附錄 C 至 E 分別對應 ISO/ IEC 29100、GDPR、ISO/IEC 27018 與 ISO/IEC 29151 之條文編號以及應用標準之說明，附錄 F 則為說明如何將 ISO/IEC 27701 適用於 ISO/IEC 27001 與 ISO/IEC 27002。

(2) 為法規課責設計

以微軟為例，為業務或服務得以順利推展，逐一檢驗供應商或其提供之服務是否符合各國隱私法遵為必要之務。但囿於其規模及供應鏈之複雜度，執行相關檢驗著實耗費人力及時間，也降低微軟的市場競爭力。故微軟希望有一套萬用標準可以使用，並要求所屬供應商遵循，ISO/IEC 27701 就符合微軟的期待。

ISO/IEC 27701 將歐盟一般資料保護規則（GDPR）、巴西一般資料保護法（Lei Geral de Proteção de Dados, LGPD）、美國加州消費者隱私法（California Consumer Privacy Act, CCPA）等目前主要市場的隱私法規之條文，對應至 ISO 標準，並建立相應的法遵控制措施。

產品開發者為取得 ISO 27701 驗證，應先依相關法遵擬定控制措施，並據以開發產品及服務；經組織內部及授權得執行 ISO27701 稽核之第三方確認控制措施及執行情形符合相關法遵，始得取得期驗證。

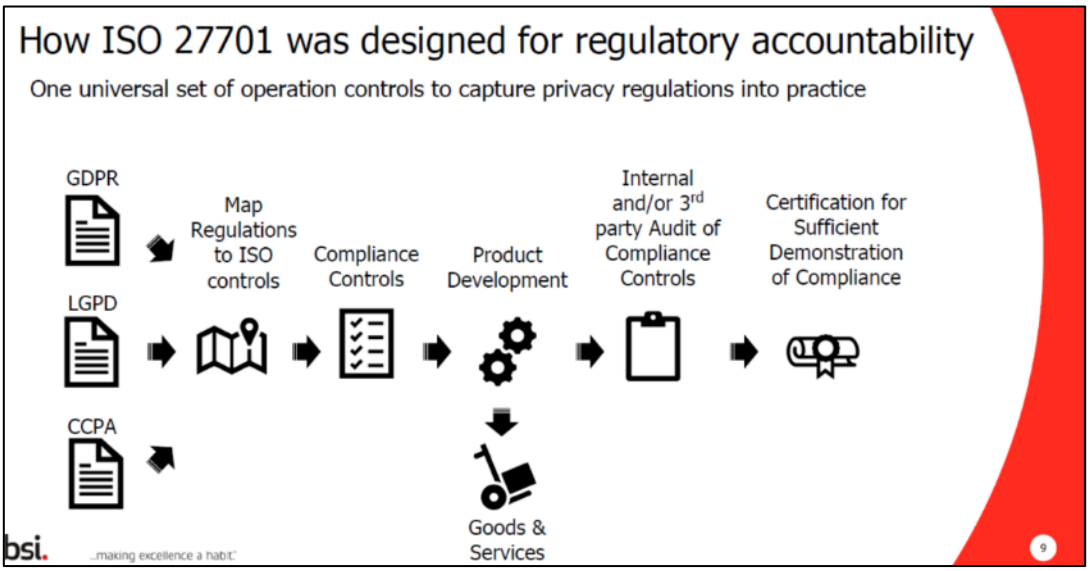

圖 16 ISO27701 架構設計示意

資料來源：講者簡報

(3) ISO/IEC 27701 亦可協助 ENISA 處理個人資料及成為驗證要求

ISO/IEC 27701 同時對個資的處理者及控制者提出指引及要求，無論組織大小規模形式皆可取得相關驗證或要求其供應商取得驗證。此外，歐盟網路安全法第 41 條規定，ENISA 在處理個人資料時應遵守 Regulation （EU） 2018/1725，該規則係規範歐盟所屬機關及機構處理個資時應遵守之規範，因此又被稱為「歐盟官方適用的 GDPR」（GDPR for European Union Institutions）[5]。歐盟網路安全法施行後，ENISA 執法時需遵照 Regulation （EU） 2018/1725 之規定，建立處理個資的操作規則，為此需要一套合適的標準及驗證做為依據，而 ISO/27701 或許可成為制定規則之基準。

[5] https://www2.deloitte.com/be/en/pages/risk/articles/gdpr-for-eu-institutions.html

(五) 物聯網挑戰（IoT Challenges）

1. Embedded Systems for IoT Products: What is the Current Certification Offer?

目前流行於歐洲的 18 種 IoT 認驗證體系，可分為三類：

- 政府機關所發布：如英國的 Commercial Product Assurance （CPA）認驗證體系、西班牙的 National Essential Safety Certification（LINCE）認驗證體系、法國的 Certification de Sécurité de Premier Niveau（CSPN）認驗證體系以及歐盟的 Senior Officials Group Information Systems Security（SOG-IS）所協調的共同準則（Common Criteria，CC）認驗證體系等。
- 行業組織所發布的體系：如 ETSI TS 103 655、GSMA IoT Security、Eurosmart IoT Scheme，以及 GlobalPlatform TEE。
- 私人公司所發布的體系：如 ARM Platform Security Architecture （PSA）L1&L2、UL 2900、UL IEC 62443，以及 Security Evaluation Standard for IoT Platforms （SESIP）。

講者所屬單位在 EUROSMART 經費挹注下，對上述 18 種 IoT 認驗證體系做一詳細的問卷調查，相關結果如下：

- 認驗證體系概觀（Scheme overview）：80%的體系是這幾年才開始發展。
- 目標市場與用戶（Targeted market and users）：前三大市場依序為工業控制、IoT 電路板，以及醫療設備。而各認驗證體系的目標用戶種類則是大同小異，皆含括如晶片與設備製造商、應用程式與作業系統開發人員、政府機構、服務供應者、設備供應商與終端用戶。
- 運作與治理現況（Operational description and governance of the scheme）：
  - ❖ 頒發證書的工作通常是驗證體系的擁有者所負責頒發。
  - ❖ 頒發證書的數量每年從 0 件到 50 件不等。
  - ❖ 整個驗證費用則是每個 IoT 設備從 0 元到 1 萬 5 千歐元不等。
  - ❖ 認驗證體系由專家成工作小組來進行維護管理。
  - ❖ 證書的效期有數種，如無期限，或者限制為 1、3 或 5 年

- ❖ 超過半數的體系需要評估產品生命週期中的風險管理流程

- 實績（Products evaluated by the scheme）：前三大產品類型為應用程式、網通設備以及 IC 晶片。
- 評估方法（Evaluation methodologies）：評估方法多採用第三方評估（Independent evaluation by an approved lab）方式，也有 10%的體系採用自我評量（Self assessment）的方式。
  - ❖ 實驗室（Evaluation labs）：近 80%的認驗證體系已經提供實驗室清單
  - ❖ 步驟過程（Evaluation process）：近 60%的體系支持更新與持續保證（patching and assurance continuity）
  - ❖ 測試步驟（Testing process）：測試方法（The attack catalog）多由專家小組所設計，且所有體系皆要求提供文檔。另外額外要求提供原始碼（source code）、功能測試（Functional Testing）、滲透測試（Penetration Testing），以及開發、製造場域（Development and Production sites）等資訊也是在所多見。
- 與歐盟資通安全法案合規（Compliance with Art. 54 of the Cyber Security Act）：超過 60%的體系將契合目前已獲通過的歐盟資通安全法案。

講者最後總結目前歐洲的 IoT 認驗證體系還是在萌芽發展階段，但可以看出將朝著市場需求與風險管理的兩個趨勢前進。且雖然這些認驗證體系都基於 Common Criteria 所開發，但都宣稱可以比 Common Criteria 來的更有效率且更貼近特定產品所需。

2. SESIP: A Practical, Operational, Lightweight CC Methodology

本場次的講者具 20 年業界經驗，設置過 5 個認驗證體系，也協助驗證超過 60 項產品，更是目前 SESIP 認驗證體系主要貢獻者。他認為 Common Criteria 的問題在於條文艱澀難懂，許多條文若未經專家解釋，跟天書一般無法理解，無法理解就使人無法使用與操作。因此，他現在

的工作目標是設立一個可操作（Operate）且可持續優化（Optimize）的認驗證體系。

一個良好的認驗證體系有幾個特色

- 驗證到發證的時間應可預期且申請者可接受，目前 Common Criteria 時間太長。
- 已驗證的部分可重複利用（re-use）。
- 使用產業界已公認且熟知的測試方法與工具。
- 支持大規模化（scale）的驗證。

SESIP 的特色是使用一般用戶與開發者可理解的語句所撰寫，使得不具備認驗證背景的讀者也能理解。另一個特色是將各類形形色色的安全要求，採用一致化的切分，構成整齊有序的要求項目（Fixed requirements），這類的整理功夫也只有像講者這樣資深的專家有辦法綜整。SESIP 的驗證等第分為 5 級，各級的分界是用從攻擊者的攻擊強度來區分，級別越高，防禦力越強。

- 第五級：即 EAL4 + ALC_DVS.2 + AVA_VAN.5，等同於智慧卡 CC 驗證。
- 第四級：白箱漏洞分析與不受限時數的滲透測試。
- 第三級：白箱漏洞分析與有限制時數的滲透測試。
- 第二級：有限制時數的黑箱滲透測試。
- 第一級：自我評量與功能驗證測試。

上述等級係對應攻擊者的能力，如攻擊者在偵查期間與漏洞利用時具有物理訪問權限（第四級）或者攻擊者在漏洞利用後具有加載惡意程式軟件的能力（第四級）。透過這樣自然語言式的描述，IoT 廠商可以更明確的得知應該選擇哪一個等級的驗證服務，而不是毫無根據地選擇第一級（有作就好）或是最高級（一定要很安全）。

SESIP 刻正對應各認驗證體系，俾通過 SESIP 驗證的產品，在取得

另一個體系的證書時，較為無痛，其策略包括【相互承認】及【提供差異分析】。客戶可清楚得知哪些元件必然通過驗證，哪些元件尚待處理。SESIP 對於處理方式也會提供如採用管理機制或是採用軟體設計之建議。目前 SESIP 已經對應的體系有 ENISA IoT guidelines、GSMA IoT guidelines、ICA Secure （Alibaba Cloud），以及 IEC 62443 4-2。最後講者提出很有野心的目標，要使得 SESIP 成為大一統的驗證體系，未來要可對應 500 個以上的驗證體系，成為國際性的事實標準。

3. EUROSMART IoT Security Certification Scheme（eIoT SCS）

Eurosmart 是一資通安全技術專家們所組成的社群，他們相信未來 IoT 的安全，需要 IoT 生態圈的各方參與者在透明協作、相互信任關係下，建立一統一且一致的框架來解決。在歐盟通過網路安全法案後，該社群認為是時候提出新的認驗證體系，即 Eurosmart IoT Certification Scheme（E-IoT SCS）。其目標是建立一個以 IoT 系統威脅模型與風險管理為基礎的整體、共通的資通安全要求，且要契合新通過的歐盟網路安全法案的合規要求。該社群所提的體系等級分為高中低三種，低級要求需能最小化已知安全風險與應付已知的攻擊手法。中級要求除包括低級要求外，尚需抵擋具有一般技能與資源的攻擊者，即一般因金錢理由驅動的駭客。高級要求則是要求能抵擋國家資助型駭客的攻擊。該認驗證體系擷取了許多其他驗證體系所具備的優秀觀念，例如依照攻擊者角度進行風險管理、以更新為優先的品質保證（Adapted Assurance Continuity）、主動式的漏洞監控（Active Monitoring/Vulnerability Surveillance），當然也含括符合性分析（Conformity analysis）與弱點分析（vulnerability Analysis）。此驗證體系除符合歐盟網路安全法案的合規要求外，也提供可預期的人天數，廠商可明確知道整個驗證所需的時程，中級驗證僅需 1 個人月，低級可短到 3 個人天。講者同時歡迎大家能夠參與該驗證體系的前期測試（pilot certification phase），並且這些文檔都是以開放原始碼的方式分

享至其官網，歡迎大家下載 https://www.eurosmart.digital/eurosmart-iot-certification-scheme/。

4. X-Gateway as a Modular Part of IoT

X-Gateway 係源自歐洲的開放數據基礎架構 GAIA-X 專案。一般談到 IoT 都專注於裝置與服務供應商本身，但本場次垂注重點係從上游的設備商、中游的服務供應者，到下游的服務與數據使用者與政府監管機構，整個 IoT 生態圈。未來的 IoT 系統必然發生多個利害關係人因法令或合約之故，被授權存取 IoT 所蒐集之數據並自動進行交換。被授權使用者多必然導致管理碎片化及授權不一，導致授權管理變的異常複雜，難以維護，最終導致服務供應者將妥善隔離所蒐集之數據的假設不復存在。

層層堆疊的模組設計可提供安全服務，但至少需要四個層次，從最外層到裏層分別為【使用者角色授權與權限控管】、【安全的通訊機制】、【安全演算法】及【金鑰安全存放】。層層模組化的安全服務恰好可以透過 Common Criteria 這樣的工具來達成重複利用（re-usability）及大量套用。舉個例子，若在底層的金鑰晶片與加密算法，已經獲得驗證，透過層次模組化與重複利用的概念，IoT 開發者只需要再取得安全通訊與權限控制的驗證，而不需要再去驗證底層的晶片與算法，有助於降低驗證成本。採用 Common Criteria 的好處在於 Common Criteria 已經出版了不少保護剖繪（PP）這類的要求，且已經實現在不同的層次，例如 IoT 的安全算法層有 SCA IoT SE PP，而在通訊安全層上，則有 SCA IoT SCA PP，未來各種類似 Common Criteria 驗證體系的安全要求都會陸續提出，運用這樣層次模組的概念，很容易有組織地建構 IoT 系統的安全體系。

5. Common Criteria as Backbone of IoT Security Certification

IoT 裝置的應用軟體層、作業系統層開發商，及硬體晶片製造商數量

相當稀少，所以將信任根（Trust Root）交由硬體晶片商負責是相當具有經濟效益的決策。為因應 IoT 裝置【數量龐大】、【軟體更新】及【持續處於安全】等挑戰，組合經 Common Criteria 驗證合格的模組，透過多層次的方法保證其安全是較為可行的方法。擇定 Common Criteria，係 Common Criteria 提供了一個一致性描述的通用語言，可以對 IoT 整體及每個層次的安全問題進行建模。

目前歐洲有大量的資通安全法規、驗證方案與標準，要如何選擇合適的驗證體系，取得合格證書，這對 IoT 的設備商及服務商帶來的不小的困擾。SESIP 這個驗證體系所提供的對應服務，即提供不同驗證體系間的轉換證書服務，使得已經取得某一驗證的產品可以快速的轉換成其他驗證體系所需的安全要求，以增加產品的的驗證廣度。

6. OWASP IoT Project: A Great Ally for the IoT Candidate Schemes

OWASP 社群並不會如一般的驗證體系，提供實驗室認可，或者證書發放等驗證服務。OWASP 只提供來自社群專家們免費的資訊安全建議與錯誤態樣排序，而這些安全建議常被驗證體系引用作為補充材料，以更好的應對威脅態勢（Threat Landscape）的變化。

OWSAP IoT Project，已分別於 2014 及 2018 發布 IoT 十大錯誤態樣報告，提醒外界 10 個 IoT 系統在設置與營運時常需要避免的錯誤態樣，並予以排名。該專案也衍伸出韌體分析（Firmware Analysis Project）、IoT 攻擊面（IoT Attack Surface Project）、IoT 框架評估（IoT Framework Assessment）、韌體分析工具（Byte Sweep Firmware analysis tool）等等專案工作。

2020 年，OWASP 預計將啟動 IoT Security Verification Standard（ISVS）專案，ISVS 標準對 IoT 安全控制羅列了許多要求，同時提供開發人員一安全開發要求列表。ISVS 名稱雖有標準二字，但其作用更像產品型錄，而非一般觀念中的務必要遵守的標準。

未來，OWASP 對 IoT 專案的三個工作方向：

- Seek & Understand：包括每兩年更新錯誤態樣報告與對齊其他資通安全組織之安全指引，如 ENISA。
- Validate & Test：即前述 ISVS 專案與韌體分析工具開發等。
- Governance：如盤點其他組織的 IoT 的監理政策與認驗證制度，或者開發 IoT Security Framework 等。

(六) 觀點與機會（Outlook/Opportunities）

1. SOGIS View on the Cybersecurity Act

網路安全法通過的首件候選資通安全驗證方案，即將現行的資訊系統安全資深官員小組相互承認協議（Senior Officials Group Information Systems Security Mutual Recognition Agreement, SOG-IS MRA）轉換為歐洲共同準則方案（European CC Scheme）。

(1) SOG-IS MRA 概述

在網路安全法通過之前，歐盟境內存在數個彼此互不相容的國家型及區域型安全驗證方案。SOG-IS MRA 係以 Common Criteria 為基礎，所建立的歐洲驗證框架，參與者為各國公共安全主管機關。透過驗證的相互承認，建立各會員國間之信任。

SOG-IS MRA 目前有 17 名會員國，會員國在參與權限上依據其國內有無自身驗證方案/國家驗證機構區分三個層次，無國家型驗證機構的為一般等級（consuming participants），國家型驗證機構如可執行各類產品驗證至 EAL4 則為授權類參與者（authorising participants）成員，最高級別成員則是能夠評估智慧卡（如晶片金融卡）或硬體安全驗證至 EAL7 的驗證機構。

由於網路安全法要建立歐盟資通安全驗證框架，因此質疑 SOG-IS MRA 已無存在必要也甚囂塵上。講者特別於報告中釐清外界所指 SOG-IS MRA 並非屬框架體系，不接受非歐盟成員，不適用於 IoT 裝置，實驗

室及驗證方案的同儕評估非屬必要，以及需為歐洲驗證市場的零碎化（Market fragmentation）負責任等不實指控。市場零碎化乙節，更指出其原因係各類垂直產業的法規缺乏協調，而非 SOG-IS MRA 未能達成各驗證方案間的協調一致。

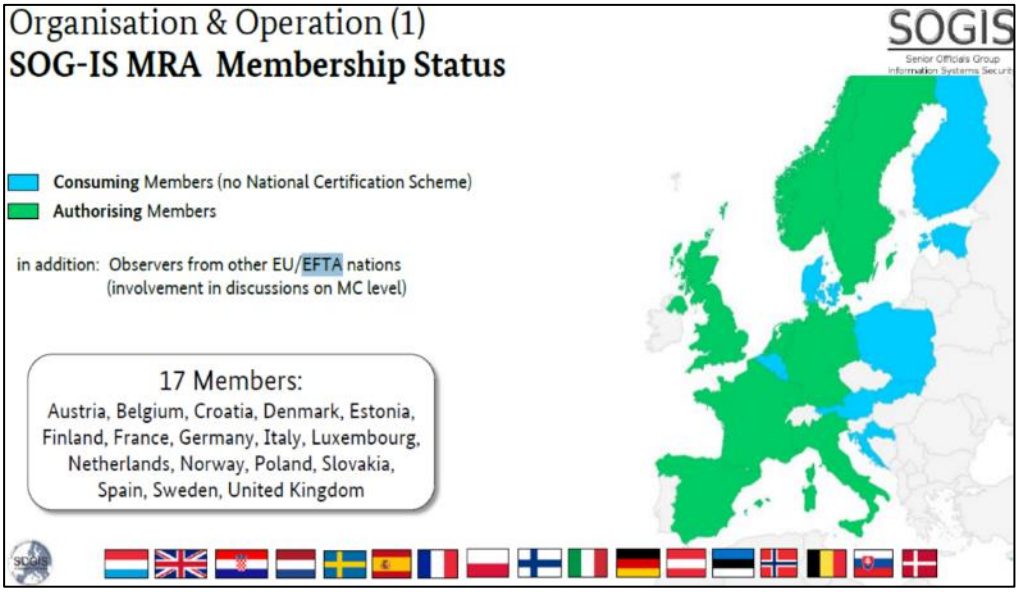

圖 17 SOG-IS MRA 會員國

資料來源：講者簡報

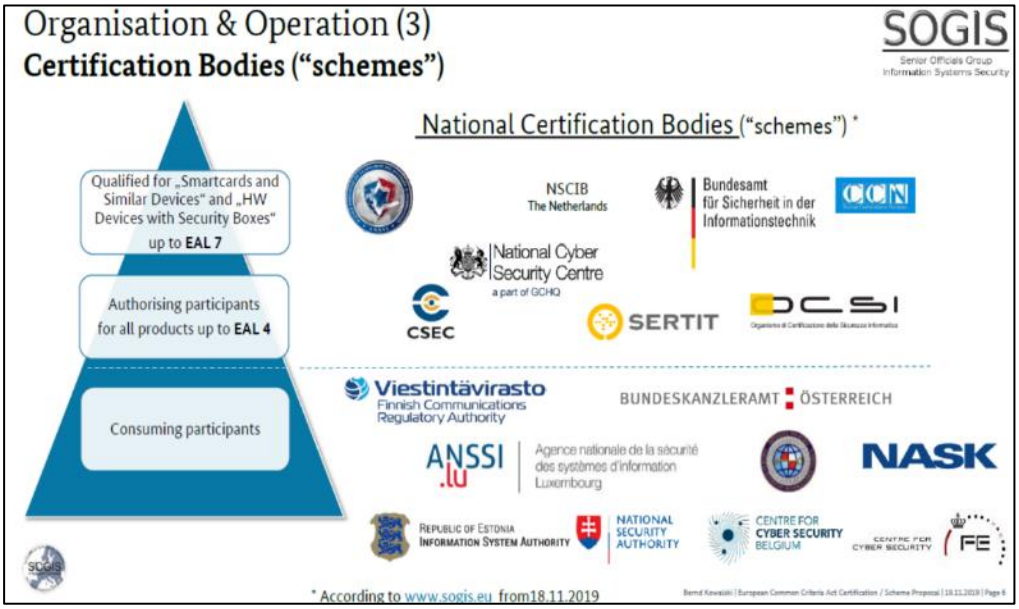

圖 18 SOG-IS MRA 會員國參與等級

資料來源：講者簡報

(2) 歐洲共同準則計畫草案

歐盟執委會在彙集歐洲資通安全驗證工作團（ECCG）及利害關係人資通安全驗證工作團（SCCG）意見後，已提出首件歐盟滾動式工作項目（URWP），即要求 ENISA 將目前 SOG-IS MRA 機制轉換為歐盟資通安全驗證方案（CSA scheme）。SOG-IS MRA 管理委員會已著手準備相關轉換工作，並提出相應的歐洲共同準則方案草案（Draft Proposal for a European CC Scheme）。

此驗證方案（草案）係以 Common Criteria 為標準，用保護剖繪（protection profiles）描述產品類型。提供涵蓋資訊產品與保護剖繪的驗證，且不涉及特定產業部門，三種安全保證等級皆可適用，但不允許自我驗證（self-attestation），亦不適用於資訊服務本身及產品服務的工作流程。此外，草案建議將 SOG-IS MRA 管理委員會整合至 ECCG，並分散至國家資通安全驗證主管機關（national cybersecurity certification authorities, NCCA）、歐洲共同準則和諧工作團（European Common Criteria Harmonization Group, ECCHG）、歐盟網路與資訊安全局（ENISA）、符合性評鑑機構（Conformity Assessment Body, CAB）、資訊安全評估設施（IT Security Evaluation Facility, ITSEF）等組織。

草案已提交 ENISA，2020 年上半年應可被確定為資通安全驗證方案候選項目。

2. Overview of Current and Future NIAP and US Government Certification Initiatives

本場次係由美國國家資訊安全保證夥伴關係（National Information Assurance Partnership, NIAP）闡述當前美國資通安全驗證運作現況，及歐盟資通安全驗證方案與國際資通安全共同準則相互承認協議（common criteria recognition arrangement, CCRA）相容之可能。

(1) 美國資通安全驗證及授權概觀

美國資通安全驗證政策框架包括聯邦資訊安全管理法（FISMA）、聯邦資訊處理標準第 140 號（Federal Information Processing Standards, FIPS 140）、國家安全命令第 42 條（National Security Directive 42）、國安體系委員會政策第 11 號（Committee on National Security Systems, CNSS Policies＃11）及國防部指示 8500.01 號（DoD instruction 8500.01）等。執行上，涉及之美國行政機關/機構及權責範圍如下：

- ❖ 國家標準與技術研究院（National Institute of Standards and Technology，NIST）：FIPS 140
- ❖ NIAP：共同準則
- ❖ 國防部：資訊網路核可產品清單（DoDIN APL）
- ❖ 總務署6（GSA）：雲端服務的風險評估及授權管理提供標準作業規範
- ❖ 國土安全部[7]（DHS）：提供聯邦機構改善資通安全的工具及服務。

資安驗證流程，需由產品供應商送交合格之檢試實驗室測試其符合性（tests for conformance），經相關主管機關確認（validates）方可交至使用者手上。

NIAP 為 NIST 監督之國家型專案，負責管理美國境內共同準則適用的相關事宜。美國目前關於驗證方案的關注焦點包括提昇安全評估的速度、創新評估技術、建立涵蓋產品生命週期的評定（Assessment）、協調各驗證方案等。

6 聯邦政府風險與授權管理計畫（Federal Risk and Authorization Management Program, FedRAMP）

7 持續診斷及緩解專案（Continuous Diagnostic and Mitigation, CDM）

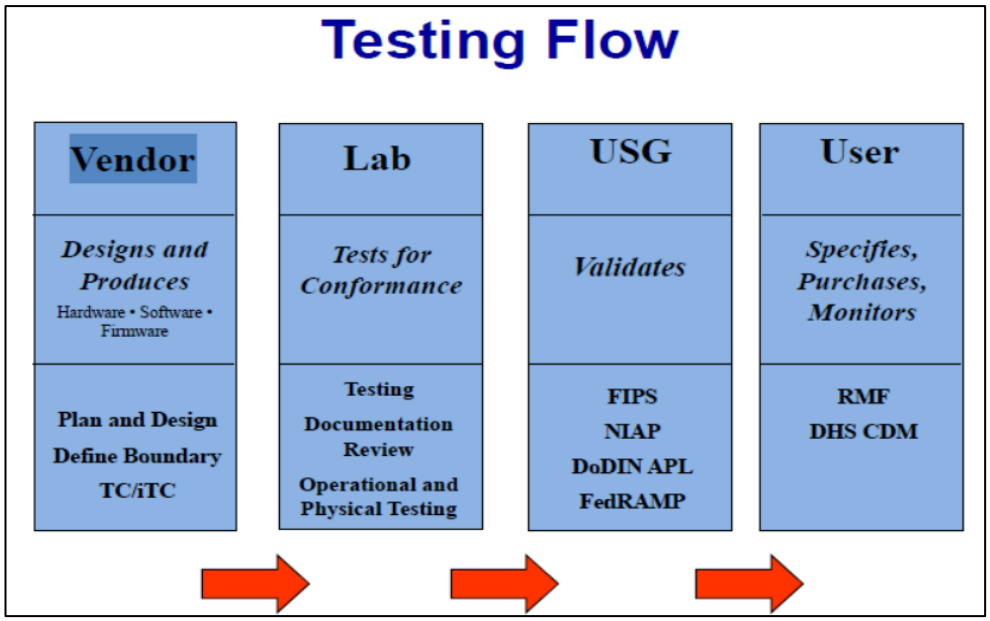

圖 19 美國產品資通安全審驗流程

資料來源：講者簡報

(2) 歐盟網路安全法與共同準則相互承認協議之競合

共同準則相互承認協議（CCRA）係 1997 年，由美國、加拿大、法國、德國、荷蘭經多年談判後的成果，後經 2009 啟動改革並於 2014 年更新相關協議內容。美國境內對共同準則的需求自 2018 年 9 月以來上升百分之三十，顯示共同準則仍是資通安全驗證的核心基礎。由於歐盟網路安全法似乎將建立一套新的驗證框架及標準，然而其內容似乎與共同準則多有重疊、相互衝突之處，除可能導致歐盟會員國與其他簽訂 CCRA 之會員產生分裂外，各國產業亦恐被迫選邊站或二者全押。此將不利 CCRA 會員之間的合作，亦可能引發貿易問題。因此就美國立場而言，目前除致力降低 CCRA 因歐盟網路安全法施行引發之影響外，也希望網路安全法未來建立的共同準則驗證方案，能改善歐盟內部協調作業，亦能強化與 CCRA 會員國之間的協調合作。

3. BSI View on the EU Cybersecurity Act

(1) 水平式立法 V.S.垂直式立法

歐盟制定的各類規章、指令，依其立法架構性質可區分為水平及垂直兩大類。水平式立法為發展各領域適用的框架，如以烹飪為例即類似

於將「香料」(各類產品之安全要求)經由「篩子」(如歐盟資通安全驗證工作團《ECCG》、ENSIA 專家工作小組《AhWG》訂定之框架制度)附加在各類食材(如雲端、5G、IoT 等資通領域)上;垂直式立法則是以產業為主體而發展的規則、指令,如 GDPR、eIDAS 等。歐盟網路安全法採水平式立法架構,然而其設計允許各國在共同基礎下推動市場需求,以促成各類資通領域的安全驗證一致。

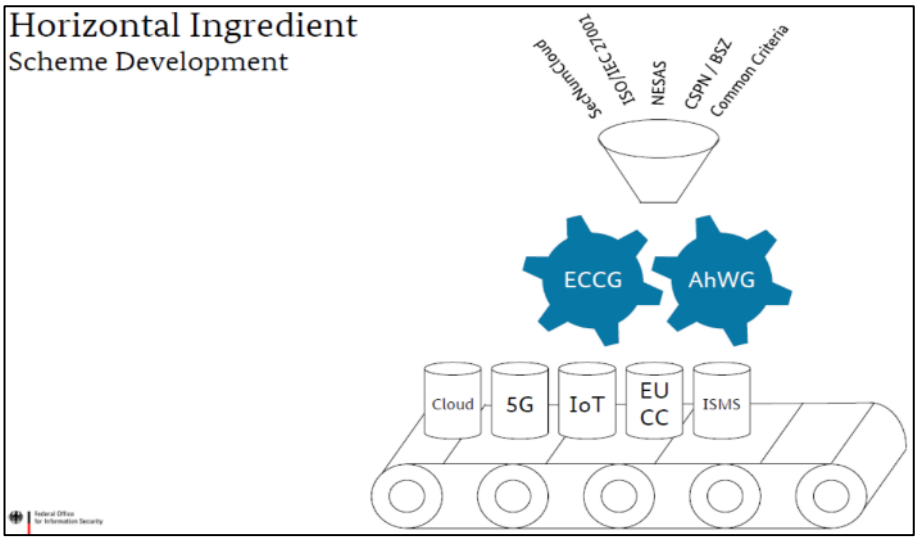

圖 20 水平式立法架構示意圖

資料來源:講者簡報

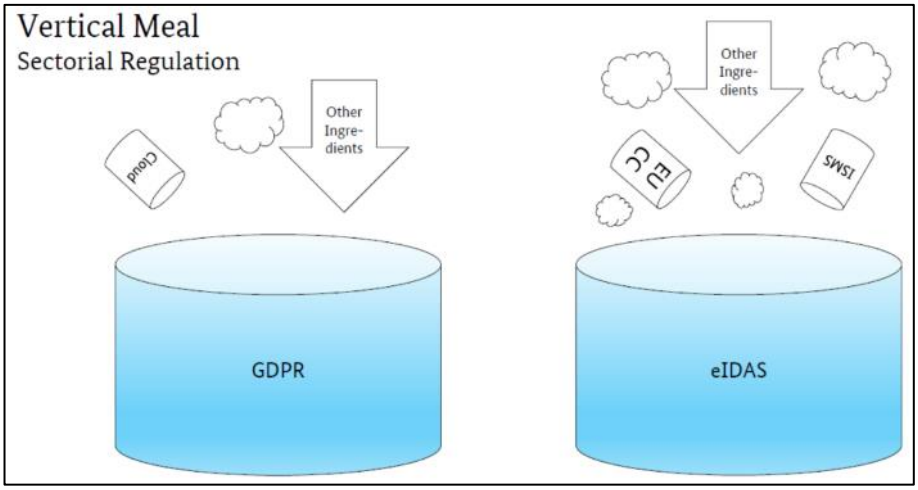

圖 21 垂直式立法架構示意圖

資料來源:講者簡報

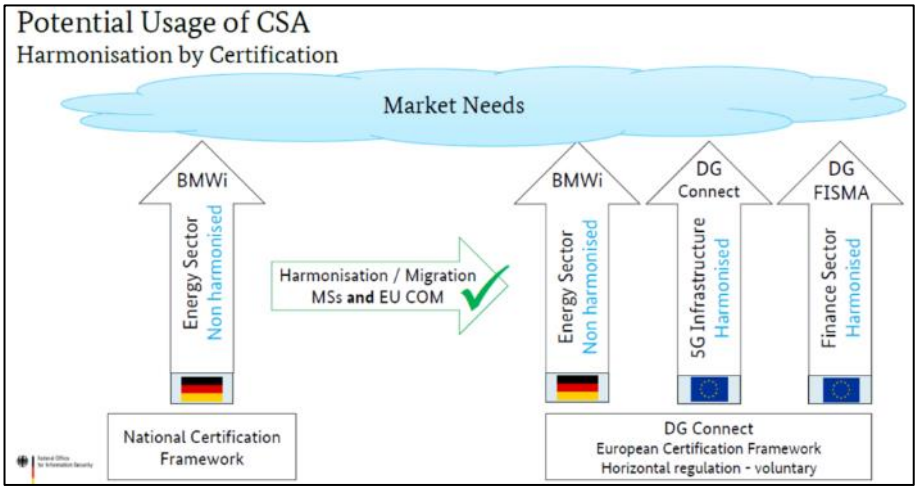

圖 22 歐盟網路安全法的使用方式

資料來源：講者簡報

(2) BSI 對於資通安全驗證方案候選的期望清單

歐盟資通安全驗證框架提供制定單一領域資通安全驗證方案的立法架構，其應優先制定的安全驗證方案領域包括一般性資通產品、工業自動化及控制系統、雲端產品服務、5G 通訊網路、物聯網等。以 5G 通訊網路為例，應在網路安全法資通安全驗證架構下，制定一歐盟層級的 5G 工具箱，並調和 Common Criteria 或 Basissicherheitszertifizierung（BSZ）部分版本規定；5G 設備之驗證可能採 3GPP 與 GSMA 所推出的 NESAS，至於系統驗證則可基於 ISO 27000 系列。

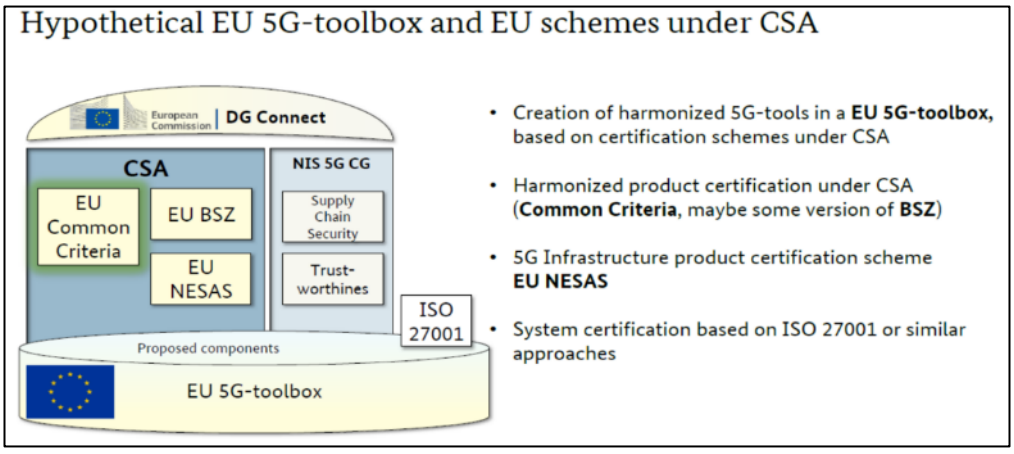

圖 23 BSI 假定的 5G 資通安全驗證方案架構示意

資料來源：講者簡報

(3) 網路安全法的利弊分析

網路安全法施行後，可預期之優缺點如下：

- 優點：
  - ❖ 彌平法規與驗證之間的落差；
  - ❖ 引入驗證的可擴充性（scalability）；
  - ❖ 為所有驗證方案列出核心需求；
  - ❖ 框架設計允許各領域之專家處理各垂直產業法規，驗證方案之運作毋須負擔相關法規調適；
  - ❖ 促使各會員國調和自身驗證方案，方可相容於歐盟範圍的驗證方案；
  - ❖ 經由協調各類驗證有效性與監控產品生命週期，有效處理跨會員國安全漏洞。
- 缺點：
  - ❖ 歐盟會員國需提供大量資源以運作該法所設制度；
  - ❖ 該法雖以試圖彌補各類資通安全標準之間的落差，然而各產業部門本身的法規及驗證仍需逐一解決；
  - ❖ 各會員國需確認每個驗證方案具備可比較性，因此驗證體系成為各國的基本設置（Accreditation system is the default）。

4. The ROI of Security Evaluations

(1) 安全驗證的投資報酬率

製造商對於歐盟資通安全驗證框架，除被動配合政府要求外，自主推動的最大的誘因應屬投資報酬率（return on investment, ROI）。

從商業活動的本質觀之，企業執行一項業務必須同時判斷該業務的投資及回報，投資越低回報越高是企業的首要考量，企業的此種心理狀態可用最簡易的公式描述➔投資報酬率＝回報（收益）除以投資（花費）。如將此投資報酬率公式應用在安全驗證，則可簡易描述為：取得安全驗

證投資報酬率＝驗證證書所含的價值除以（付出的金錢及花費的時間）。

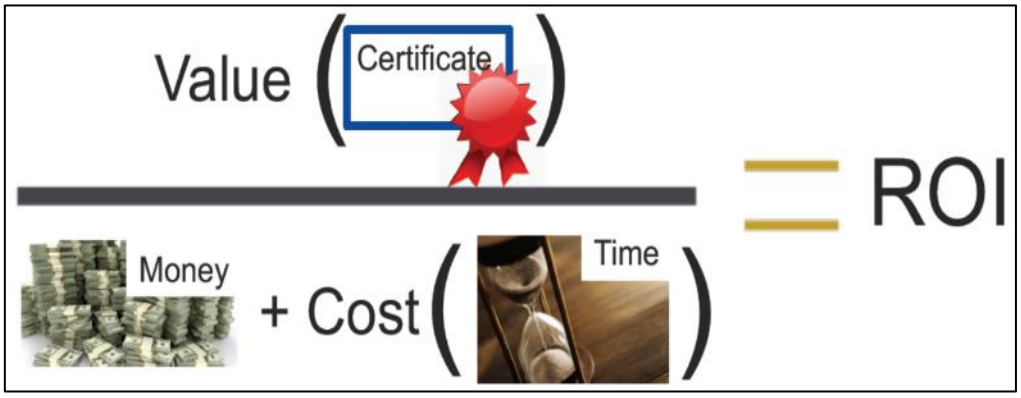

圖 24 取得安全驗證的投資報酬率公式

資料來源：講者簡報

(2) 安全驗證的價值考量：符合法令、展現善意、分散責任

金錢及時間的花費易於計算也易於評估及節省，然而安全驗證本身價值卻不易量化為具體數字也不易評估。因此其價值可由遵循政府法令（compliance）、顯示企業善意（goodness）、分散事故責任（liability）評判。

- 遵循政府法令：為了進入當地市場販售產品，企業需完成各國政府制定的相關安全驗證要求並取得證明，此時對於企業而言安全驗證的價值高低即取決於證書內容（content）與嚴格性（strictness）兩項因素。安全驗證的內容在於告訴主管機關已有符合保護剖繪，所有各類驗證的價值皆屬一致（因為只要有安全驗證就會有相關的保護剖繪描述），然而如某類安全驗證的安全保證要求越嚴格，則使該驗證就越有價值（因為只會有少數廠商符合，而物以稀為貴）。
- 顯示企業善意：由於有些產品依 Common Criteria 規定，所提之保護剖繪、安全標的與驗證報告等文件非常難以理解，甚至可能造成外界誤解，因此企業取得驗證動機僅僅就是透過證明向顧客顯示自身的產品非常安全。然而，這類安全驗證的內容，如未具備保護剖繪或保護剖繪難以理解，則對於安全驗證的價值幾乎不產生影響。另安全驗證的嚴格性雖

然重要，但過於嚴格也可能造成產品難以使用，甚至無法使用。

- 分散事故責任：最後一種取得安全驗證的理由在於分散風險，此時取得安全驗證的目標在於稀釋產品開發過程各環節參與者的責任，包括開發者、評估實驗室、驗證機關、送驗客戶、終端使用者等。其最終目的是希望發生安全事故時，無人需擔負所有責任（因為各環節已盡其所能驗證產品的安全）。當發生前述情況，則需由司法部門介入以評判驗證的內容及嚴格性。

資安安全驗證方案制定時，應綜合此三項因素，極大化安全驗證的商業價值，並注意其制定目的，非為了展現技術或完全泯滅人性。

(七) 保險創新（Innovations in Assurance）

1. Addressing the Continuity of Software Security for Embedded Devices

頻繁的軟體更新對連網設備而言，已是不可抵擋的趨勢。對 IoT 製造商來說，對一個已經取得證書的 IoT 產品更新軟體，實在是令人兩難。更新軟體要花成本，而且會使得已取得之驗證證書失效，但不更新會引發客戶抱怨等。如何調和設備驗證與軟體更新的衝突，使得廠商願意不停地提供更安全的軟體，而不會被 Common Criteria 重新驗證所需的繁複流程與手續所綁架，已成重要課題。

如果一個驗證方案的品質保證，得以累積（Accumulative）方式完成，即允許【半自動化測試】、【安全的軟體開發，又或者可稱之為開發成熟度】、【差異修改的驗證評估（Delta evaluation）】及【既存之安全驗證】，並各自發揮其功效。這樣的驗證方案就會變得有彈性，可以支持頻繁的軟體更新，而不會破壞產品驗證的狀態。

2. Updating Certified Products

Common Criteria 對於產品更新之規定如下：

- 原核發之驗證證書自動失效，但更新屬微幅者，其評估技術報告

（Evaluation Technical Report）仍符 Common Criteria 規定者，不在此限。

- 更新屬重大者，如擬維持驗證之有效性，則應重新驗證（re-certificate）。經驗證合格者，核發新證。

假定某一產品取得驗證證書 1.0，某日產品更新後，證書 1.0 即失效，意味著更新後的產品是無任何驗證的。待驗證合格後，其證書改版為 1.a 版。

採取更新即破壞驗證（No changes prior to recertification）的驗證體系，除 Common Criteria 外，法國 CSPN 及西班牙 LINCE 亦採此作法。然而，此作法無疑曠日廢時。

一種稍微改進的替代方法是採取簡易審查機制（speeded-up process），在智慧卡的驗證機制 EMVCO 以及美國 FIPS 140-2 就是採用如此方式。即輕微的更新，只要廠商向原實驗室提出書面的資通安全衝擊分析（Security Impact Analysis），經實驗室審查一週無誤後，即更新驗證證書。

簡易審查機制，可稱之為更新前審查機制，但在產品軟韌體更新頻繁的時代已經無法適用，較為進步的做法是採用先更新後審查機制，也就是採取廠商先更新，再送件進行審查。更新後到審查完竣前之空窗期，驗證合格之效力仍持續，如此才能激勵廠商先解決眼前的安全問題。採用這個做法的認驗證體系有英國輕量級 Common Criteria 體系，CPA、Globaplatform 組織的 Common Criteria 體系以及 Eurosmart IoT 體系。但這種機制要得以落實，其前提係廠商須先取得實驗室的信任。即廠商須以產品開發流程的成熟度等，說明產品更新的過程中，不會引發新的安全漏洞，並取得實驗室的信任；通常，這需要廠商具有安全的開發流程與自動化工具的配合。

3. Agile Assurance: Modernizing IT Product Certification

Common Criteria 與 FIPS140 驗證都是上個世紀 80 年代的產物，雖然還是挺有效，但已經無法應付軟韌體更新頻繁的議題。隨著資通安全

威脅不斷增長，缺乏更新的產品即便是取得證書且時效尚未過期，也是過時的產品，因為該產品無法應付新的威脅。

提供那些定期更新的 IT 產品，一個方便且有效的驗證服務刻不容緩。然而，這需要更多的創新與最佳化，使得品質保證過程來的更快速及敏捷。最佳化創新趨勢包括

- 自動化的測試方法

  並非所有的測試都可自動化，但測試的作業流程是可以標準化與生產線化的，例如由平臺自動跳出提示、紀錄步驟、蒐集證據、整理與分類資料與產生報告。

- 安全的軟體開發流程及可擴展的自動化協作（Expand Automation）

  透過安全的軟體開發流程與可擴展的自動化協作可以使得實驗室與 IT 公司取得更多的開發證據與更好的資料同步，加速驗證過程。

相較傳統的方法，採用自動化測試平臺可以將驗證時程從年月之久，加速到以周計算。但是開發自動化平臺需要大量投資，這樣的挑戰需要透過集體的協作才有可能，而且需要在一致且在一定的範圍內定義良好的測試要求；同時，驗證機構也要同步擁有這些測試結果文件，以更快更持續的驗證產品。

4. Making Evaluation Schemes Scale Up: the Tensegrity of Process and Product

以食品安全為例，將產品零件與生產過程當作兩件事情分開看待是沒有道理的事情。英國的商業產品保證體系（Commercial Product Assurance，CPA）不光是要驗證產品零件（Produce part），也要驗證產品的生產過程（Process）。

產品驗證在現實中很難大規模的進行（Scale up），畢竟技術上有其難度，替代的方案是對過程（Process）進行評估。換言之，我們不需要評估所有產品，只需評估製造過程是否正確，並期待正確的過程就會產

生良好的產品，這也是英國 CPA 驗證步驟之一。

講者也不諱言，過程與產品零件是分不開的，缺乏正確的流程將產品零件組裝起來，再好的零件也只是零件；反之亦然。因此，同時評估產品與過程，遠比只評估兩者之一來的好。

評估產品可類比 X 光的快照，只是當下該筆產品的數據，這些 X 光數據都是單點的；惟有透過過程評估，始得確保各批次產品驗證結果的連續性。這樣的過程評估能力能更準確預測未來驗證通過與否，並提升自我評估準確度。

伍、 心得與建議事項

一、建構「安全可信賴」的 ICT 生態鏈，已為各先進國家強化其數位經濟領先地位之重要措施

由於資通訊科技的快速發展，促使人工智慧、大數據、物聯網等應用服務的推陳出新，不論是金融、能源、交通、教育、通訊傳播、醫療健康，乃至政府體系等領域，創新的數位服務已逐漸成熟，更因此帶動了數位經濟之發展。

雖然創新數位服務提供民眾前所未有的便利生活及商業契機，然而，新型態的資通安全威脅卻逐漸成為隱憂。2018 年世界經濟論壇（WEF）發布之全球風險報告指出，網路攻擊的發生機率由 2017 年排行第 6 名，竄升至 2018 年第 3 名；其風險影響程度也竄升至該年度第 6 名。隨著資通安全攻擊事件的不斷發生，不僅對民生與經濟造成衝擊，若被攻擊的對象為關鍵電信基礎設施，更將影響社會整體運作，甚至危及國家安全，其危害不可小覷。

面對數位生活日益嚴峻的資通安全威脅，美國 NIST、歐盟 ETSI，以及 OWASP 等資通安全機構，已紛紛發布非強制性的安全框架或指引，而歐盟也於今年 6 月公布「網路安全法（Cybersecurity Act）」，建立 ICT 產品／服務／流程之資通安全驗證方案，更矢言於 2021-27 年編列 20 億歐元的網路安全預算，以提升歐盟網路安全能力，促進歐盟數位經濟、社會和民主發展。雖然目前這些資通安全建議或驗證方案均非強制規定，但建構「安全可信賴」的 ICT 生態鏈，已為各先進國家為確保數位經濟永續發展的重要目標，更為其強化數位經濟領先地位之重要措施。

二、5G 設備第三方資通安全驗證指日可待

5G 三大應用場景，已被外界視為產業轉型、數位經濟升級之重要推手。mMTC 可提供大規模物聯網服務；eMBB 可提供 AR/VR 或超高畫質影像等大流量行動寬頻服務；uRLLC 可應用於包括無人駕駛、工業自動化等需要低時延、高可靠連接的服務等。5G 可以提供使用者高速、低延遲等優質服務，同時又具備彈性及擴充性，以廣納更多新興應用服務，係緣自於採用大量軟體化網路功能（Software Defined Network，SDN）、基地台基頻單元（Baseband Unit，BBU）邏輯分離、核心網路功能軟體化（Softwarization）及多接取邊緣運算（Multi-access Edge Computing，MEC）等設計，然

而 5G 開放彈性與整合性，也使得 5G 網路面臨之資通安全威脅較以往更嚴峻且多元。又未來 5G 將成為所有數位經濟的骨幹網路，承載包括應用於能源、交通、金融及衛生等關鍵基礎設施及工業控制系統等數十億個連網裝置及系統，因此 5G 資通安全之重要性更是數位經濟發展上的重中之重。

GSMA 與 3GPP 為提升行動通信網路資通安全，於 2016 年共同推出一涵蓋網路設備生命週期之安全保障方案-網路設備安全保障方案（Network Equipment Security Assurance Scheme，NESAS）。該方案包括由 GSMA 擇定的安全稽核員評估【供應商在產品開發過程及整個生命週期之安全性】及 GSMA 認可的安全測試實驗室評估【網路設備安全性】兩部分。在評估【網路設備安全性】所需之檢測基準則由 3GPP 制定。

目前與 GSMA 合作的稽核機構包括 ATSEC、NCC Group 等 2 家公司，但並無 GSMA 認可合格的安全測試實驗室可評估 5G 網路設備安全性。5G 設備亦屬 ICT 產品之一部，此次會議中，來自 ETSI 的講者更將 NESAS 列為報告重點之一。顯見，在歐盟大力推展 ICT 產品資通安全驗證下，5G 設備資通安全驗證應指日可待。

三、我國連網設備資通安全驗證標的及檢測標準應調和歐盟資通安全驗證方案，將驗證效果極大化

歐盟資通安全驗證方案是基於歐盟級別的協議，針對在歐盟範圍內之 ICT 產品／服務／流程，所議定的一套全面性規則、技術要求、標準及程序，用於評估其資通安全屬性。且鑑於 ICT 產品／服務／流程的多元性及多樣性，歐盟資通安全驗證方案將對不同的 ICT 產品／服務／流程量身訂做一基於風險的歐盟資通安全驗證方案，且具體描述其【涵蓋的產品和服務的類別】、【資通安全要求】、【評估類型】及【安全保證級別】。而【資通安全要求】將盡可能依賴國際標準，以避免產生貿易壁壘或技術互操作性問題。現行 ISO 27000 系列雖屬資通安全國際標準，但側重於資訊安全管理；而 ISO 15408 共同準則部分，側重於商業化產品，且驗證時間冗長，不符 ICT 產品／服務／流程快速上市的特性。

依國際貿易組織（WTO）技術性貿易障礙協定（TBT），會員之國內技術法規、標準及合格評定程序，應以國際標準為基礎。在既有資通安全國際標準不足以因應 ICT 產品、服務或流程資通安全驗證所需，且歐盟會員國國民隱私安全防護意識高漲下，相關資通安全檢測實驗室及驗證機構等利害關係

人將戮力催生更多資通安全國際標準，歐盟也將協力推動，形成一正向循環。

另根據歐盟網路安全法規定，歐盟委員會每 5 年將審視所採取的歐盟資通安全驗證方案執行情形，並評估是否透過歐盟其他法規，強制特定場域或全面實施歐盟資通安全驗證方案，以確保 ICT 產品／服務／流程維持一適當資通安全水準，並改善內部市場的運作。資通安全驗證方案所採【資通安全要求】為國際標準者，以歐盟法令或其會員國之法令強制要求 ICT 產品、服務或流程應經資通安全驗證始得輸入、上市，並無違反 WTO 規定。一旦成真，各國將群起效尤，屆時本會推動智慧型手機系統內建軟體、具射頻介面及通傳終端介面之連網設備資通安全驗證，相關標的及資通安全要求經調和（harmonized）國際標準，即可水到渠成，而且有助於我國 ICT 及資通安全產業之發展。

四、輸歐 ICT 產品或服務者應關心歐盟資通安全驗證方案發展，並積極送測，提升產品市場競爭力

歐盟資通安全驗證方案是基於歐盟級別的協議，ICT 產品／服務／流程經歐盟資通安全驗證方案驗證合格者，可通行全歐盟會員國，除助於供應商跨境營運外，更助於消費者識別擬選購之產品或服務的安全功能。輸歐 ICT 產品或服務者，尤其相關產品或服務係應用於歐盟關鍵基礎設施者，應關注歐盟資通安全驗證方案制定階段之發展，並積極送測，以提升產品市場競爭力，並於相關驗證方案成為強制規定時，取得最佳戰略地位。

另 ICT 產品、服務或流程資通安全驗證方案之制定須經【ECCG / SCCG 建議滾動工作計畫的驗證方案】、【歐盟委員會要求 ENISA 制定驗證方案草案】、【ENISA 準備驗證方案草案】、【ENISA 諮詢行業，標準組織和利益相關者】及【歐盟委員會採用驗證方案】等 5 大階段。而 SCCG 由相對利害關係人所組成，學術機構，消費者組織，符合性評鑑機構，標準制定組織，公司，行業協會和其他會員組織均可向歐盟委員會提出申請，輸歐 ICT 產品或服務者應申請加入歐盟 SCCG，以取得最新資訊。

五、我國資通安全檢測實驗室應積極爭取擔任歐盟資通安全驗證方

案之合格檢測實驗室，更甚者申請成為其符合性評鑑機構

基於 ICT 產品／服務／流程的多元性及多樣性，歐盟資通安全驗證方案將對不同的 ICT 產品／服務／流程量身訂做一基於風險的歐盟資通安全驗證方案，且具體描述其【涵蓋的產品和服務的類別】、【資通安全要求】、【評估類型】及【安全保證級別】。其中【評估類型】包括自我宣告或第三方評估；【安全保證級別】則分為基本，實質及高級三個級別；安全保證級別為【基本】者，得採自我宣告。即不論安全保證級別為何，均需合格資通安全檢測實驗室依【資通安全要求】出具之評估報告。考量歐盟為全球最大經濟體，且為我國第四大外銷市場，不論是為公司營運或協助我輸歐 ICT 產品或服務者提早取得相關資通安全驗證，我國資通安全檢測實驗室應積極爭取擔任歐盟資通安全驗證方案之合格檢測實驗室，提早卡位。更甚者，申請成為相關驗證方案之符合性評鑑機構。