DEKRA

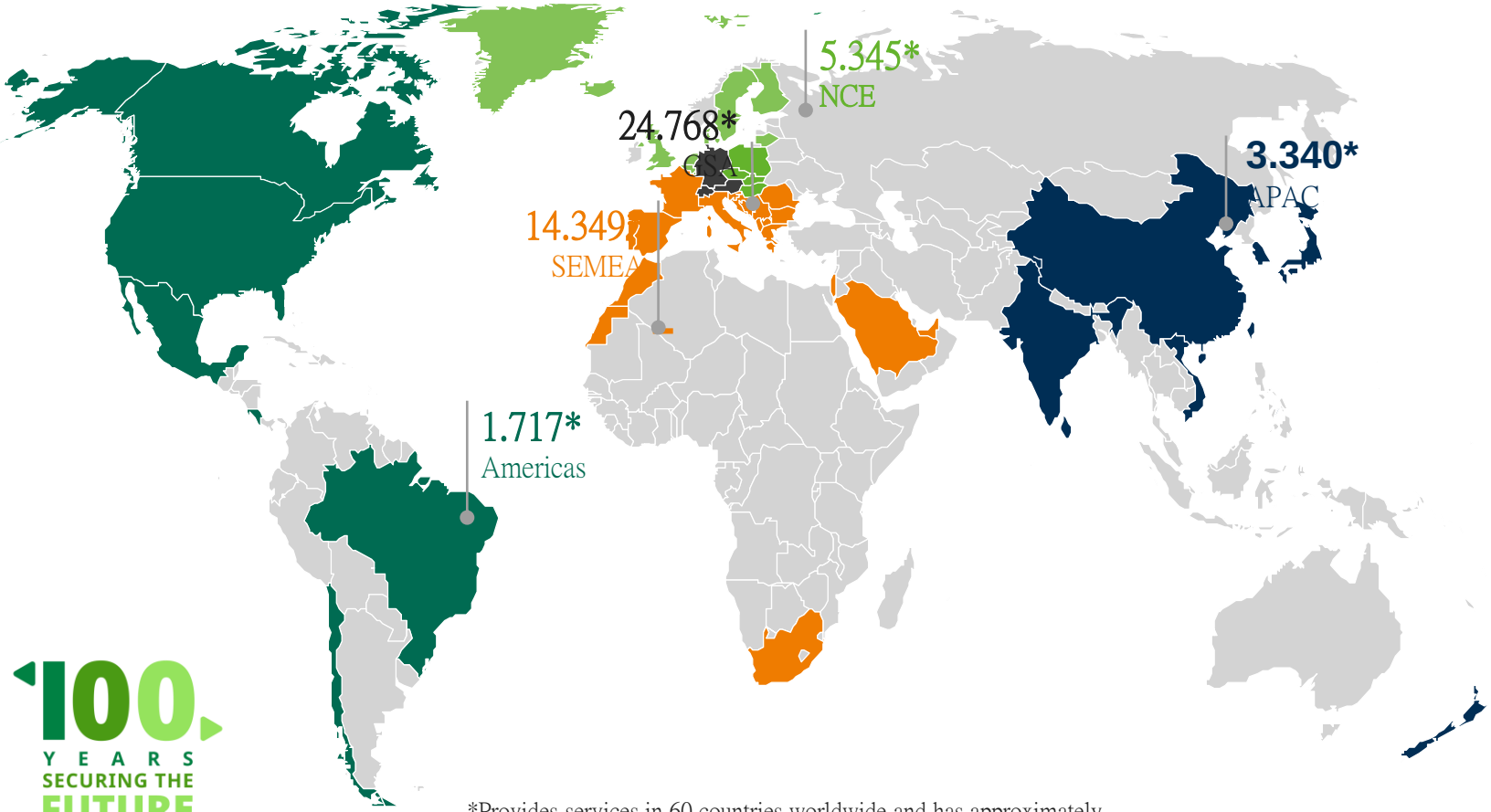
innovating safety & security

檢測機構

網路安全/軟體更新管理系統評估及車型檢測作業說明

CSMS/SUMS Evaluation and Testing

About DEKRA (since 1925)



100 YEARS SECURING THE FUTURE 1925 – 2025

*Provides services in 60 countries worldwide and has approximately 50,000 employees.

DEKRA in Taiwan

- Safety Testing
- EMC Wireless Testing
- Certification Service
- Global Market Access

- Reliability Testing
- Failure Analysis
- Material & Chemical Testing

- Enterprise Cybersecurity
- Security Compliance
- Testing and Certification
- Cybersecurity Assessment Tools

VSCC授權檢測

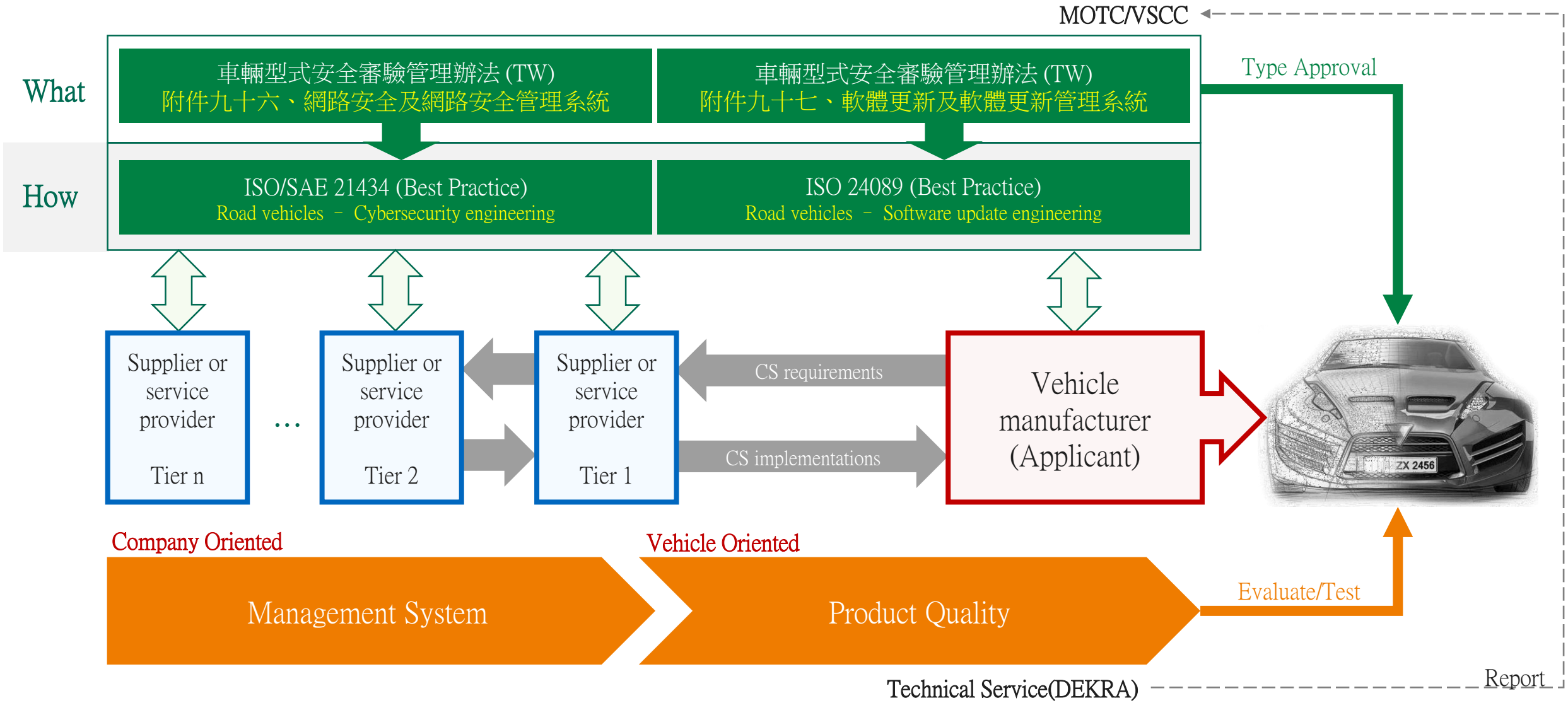
- 電磁相容性測試（560、561、562、563、564）
- 自願性車聯網產品型式認證
- 網路安全及網路安全管理系統（960）
- 軟體更新及軟體更新管理系統（970）

《車輛安全檢測基準》附件九十六

網路安全及網路安全管理系統 - 管理系統要求

車輛產業合規運作機制

Vehicle Supplier Chain Compliance Working Model



VSTD 96 服務項目

01 系統評估 - 初步評估

02 系統評估 - 年度評估

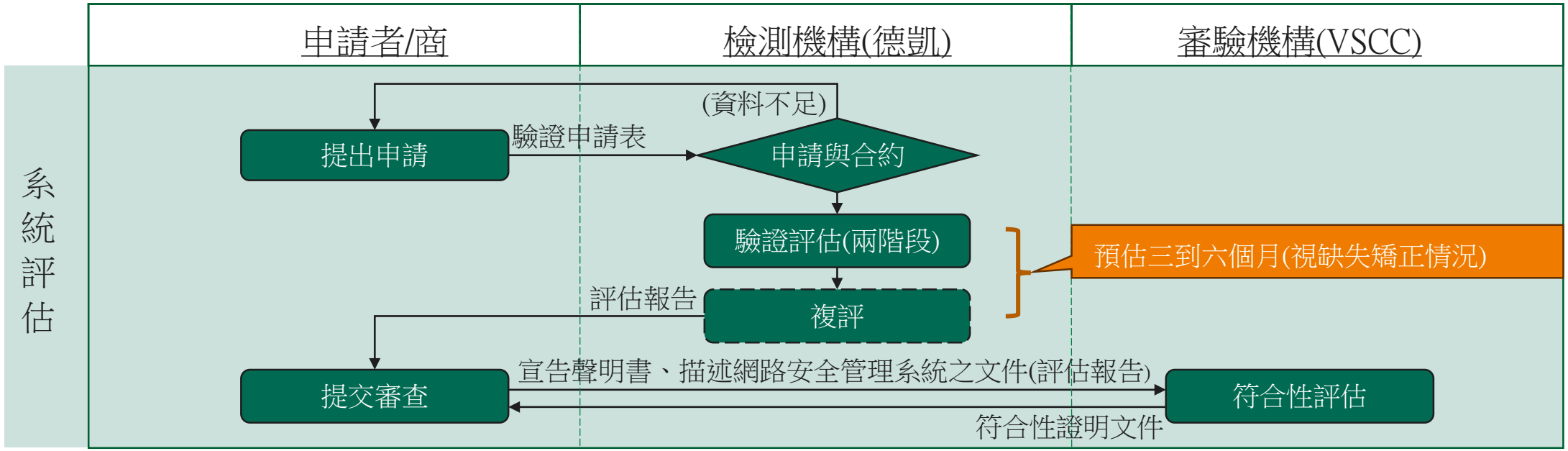
03 系統評估 - 重新評估

04 系統評估 - 變更評估

05 車型檢測

申請流程圖 – 初步評估

ISO 17021-1Conformity assessment — Requirements for bodies providing audit and certification of management systems



- 驗證評估範圍認定
  - 一個法律實體內參與CSMS活動的所有部門。
  - 使用此CSMS的所有車輛廠牌。
- 評估依據
  - 「5.2 網路安全管理系統要求」(VSTD 96 / 5.2共16項)。
- 驗證評估所需資料
  - 自我評估表、管理系統、執行紀錄。

VSTD 96 / 5.2 網路安全管理系統要求

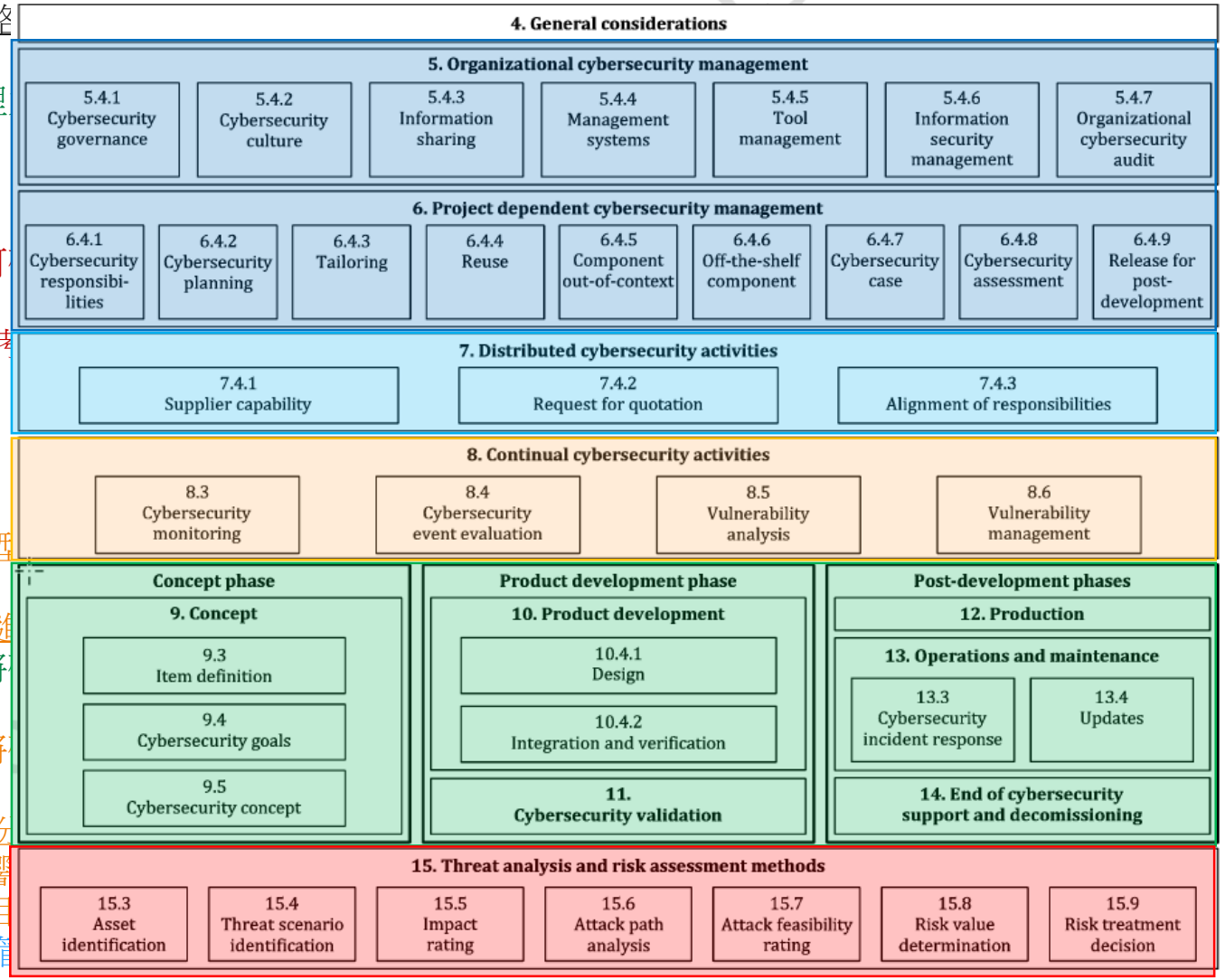
- 5.2.1 **審驗機構或檢測機構應驗證並評估申請者是否具有網路安全管理系統（CSMS），並應驗證其符合本項法規。**
- 5.2.2 網路安全管理系統應包括：
  - 5.2.2.1 申請者應向審驗機構或檢測機構證明網路安全管理系統適用於以下階段：
    - (a) 開發階段；
    - (b) 生產階段；
    - (c) 生產後階段。

網路安全管理系統 (Cyber Security Management System，CSMS)：係指一種以風險為基礎的系統方法，並定義組織化的流程、職責和治理，以處理與車輛網路威脅相關的風險及保護免受網路攻擊。

  - 5.2.2.2 申請者應證明其網路安全管理系統中使用的流程可確保充分考慮安全性，包括附件中所列的風險和緩解措施。應包括：
    - (a) 申請者組織內用於管理網路安全的流程；
    - (b) 用於識別車輛型式風險的過程。在相關過程中，應考慮條文6規定所列出之相關威脅；
    - (c) 用於評估、分類和處理已識別風險的程序；
    - (d) 驗證所識別的風險是否得到適當管理的流程；
    - (e) 用於測試車輛型式網路安全的程序；
    - (f) 用於確保風險評估**與時俱進**的程序；
    - (g) 用於監控、檢測和反應網路攻擊、網路威脅和車輛型式漏洞的過程，以及用於評估所實施的網路安全措施是否仍然有效的過程，以確保新的網路威脅和漏洞可被識別。
    - (h) 用於提供相關資料以支持對未遂或成功的網路攻擊進行分析的流程。
  - 5.2.2.3 申請者應證明其網路安全管理系統中使用的流程將確保，依條文5.2.2.2(c)、 5.2.2.2(g)規定中提到的分類，需要申請者反應之網路威脅和漏洞，應於合理之時間範圍內獲得緩解。
  - 5.2.2.4 申請者應證明其網路安全管理系統中使用的流程將確保依條文5.2.2.2(g) 規定所述的監控應持續進行。
    - (a) 將首次登記領牌後之車輛納入監測；
    - (b) 包括從車輛資料和車輛紀錄（如保養維修紀錄）中分析和檢測網路威脅、漏洞和網路攻擊的能力。此功能應遵守條文1.3規定及車主或駕駛的隱私權，尤其須經其同意。（本法規不影響其他法規、區域或國家立法關於授權存取車輛、其資料、功能和資源以及相關存取條件，其亦不排除國家或地區有關個人資料保護相關法令之適用。）
  - 5.2.2.5 申請者應依條文5.2.2.2規定的要求證明其網路安全管理系統將如何管理與簽約供應商、服務提供商或製造商的子組織可能存在的依賴關係。

VSTD 96 / 5.2 網路安全管理系統要求

- 5.2.1 審驗機構或檢測機構應驗證並評估申請者是否具有網路
- 5.2.2 網路安全管理系統應包括：
  - 5.2.2.1 申請者應向審驗機構或檢測機構證明網路安全管理
    - (a) 開發階段；
    - (b) 生產階段；
    - (c) 生產後階段。
  - 5.2.2.2 申請者應證明其網路安全管理系統中使用的流程可
    - (a) 申請者組織內用於管理網路安全的流程；
    - (b) 用於識別車輛型式風險的過程。在相關過程中，應考
    - (c) 用於評估、分類和處理已識別風險的程序；
    - (d) 驗證所識別的風險是否得到適當管理的流程；
    - (e) 用於測試車輛型式網路安全的程序；
    - (f) 用於確保風險評估**與時俱進**的程序；
    - (g) 用於監控、檢測和反應網路攻擊、網路威脅和車輛型
      以確保新的網路威脅和漏洞可被識別。
    - (h) 用於提供相關資料以支持對未遂或成功的網路攻擊進
  - 5.2.2.3 申請者應證明其網路安全管理系統中使用的流程將
    威脅和漏洞，應於合理之時間範圍內獲得緩解。
  - 5.2.2.4 申請者應證明其網路安全管理系統中使用的流程將
    - (a) 將首次登記領牌後之車輛納入監測；
    - (b) 包括從車輛資料和車輛紀錄（如保養維修紀錄）中分
      主或駕駛的隱私權，尤其須經其同意。（本法規不影響
      存取條件，其亦不排除國家或地區有關個人資料保護相
  - 5.2.2.5 申請者應依條文5.2.2.2規定的要求證明其網路安全管
    依賴關係。



Best Practice – ISO/SAE 21434 （以風險評估資產識別為例）

Objectives

- a) identify assets, their cybersecurity properties and their damage scenarios;
- b) identify threat scenarios;
- c) determine the impact rating of damage scenarios;
- d) identify the attack paths that realize threat scenarios;
- e) determine the ease with which attack paths can be exploited;
- f) determine the risk values of threat scenarios; and
- g) select appropriate risk treatment options for threat scenarios.

Inputs	Requirement(RQ/RC/PM)	Work Products
Prerequisites The following information shall be available: — item definition [WP-09-01]. **Further supporting information** The following information can be considered: — cybersecurity specifications [WP-10-01].	**[RQ-15-01]** Damage scenarios shall be identified. **[RQ-15-02]** Assets with cybersecurity properties whose compromise leads to a damage scenario shall be identified.	**[WP-15-01]** Damage scenarios, resulting from [RQ-15-01] **[WP-15-02]** Assets with cybersecurity properties, resulting from [RQ-15-02]

系統評估標準（持續優化）

Evaluation of the findings according to table 1 in ISO/PAS 5112:2022, section 6.4.8

Objective evidence regarding full achievement of all objectives	Conformity
Minor deviations were observed	Minor nonconformity
Major deviations were observed, one or more objectives are not achieved	Major nonconformity

Deriving the audit result according to table 2 in ISO/PAS 5112:2022, section 6.4.9

There are no major nonconformities and no minor nonconformities.	Pass
There is one or more minor nonconformities, but no major nonconformities. Identified minor nonconformities do not call into question the overall effectiveness of the CSMS.	Conditional pass
One or more major nonconformities or several minor nonconformities that, due to their number or in their dependencies, call into question the overall effectiveness of the CSMS.	Fail

網路安全管理系統 (Cyber Security Management System ，CSMS)：係指一種以風險為基礎的系統方法，並定義組織化的流程、職責和治理，以處理與車輛網路威脅相關的風險及保護免受網路攻擊。

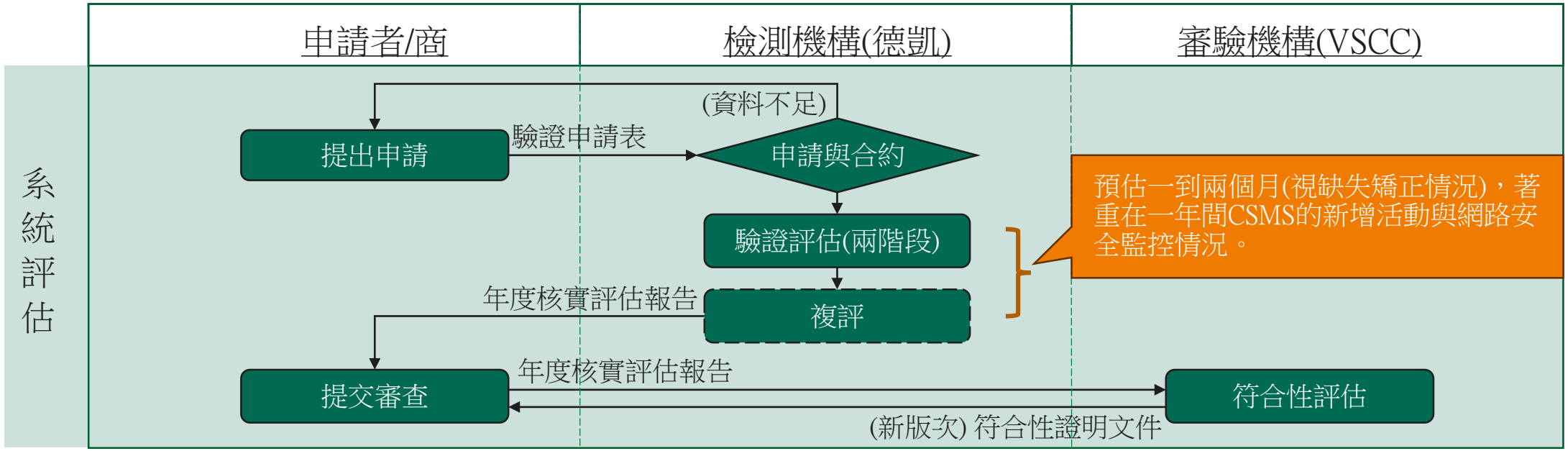
"Cyber Security Management System (CSMS)" means a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.

稽核重點（Verification）

- **管理系統已存在（Exist）**：對應所有要求的四階文件已建立並實施。
- **管理系統已落實（Execution）**：管理系統相關活動均有正式紀錄，如內部稽核、管理審查、持續監控、風險評估、安全開發等。
- **管理系統確認有效（Effectiveness）**：確認規劃的做法有效，同時團隊有能力執行。

申請流程圖 – 年度評估

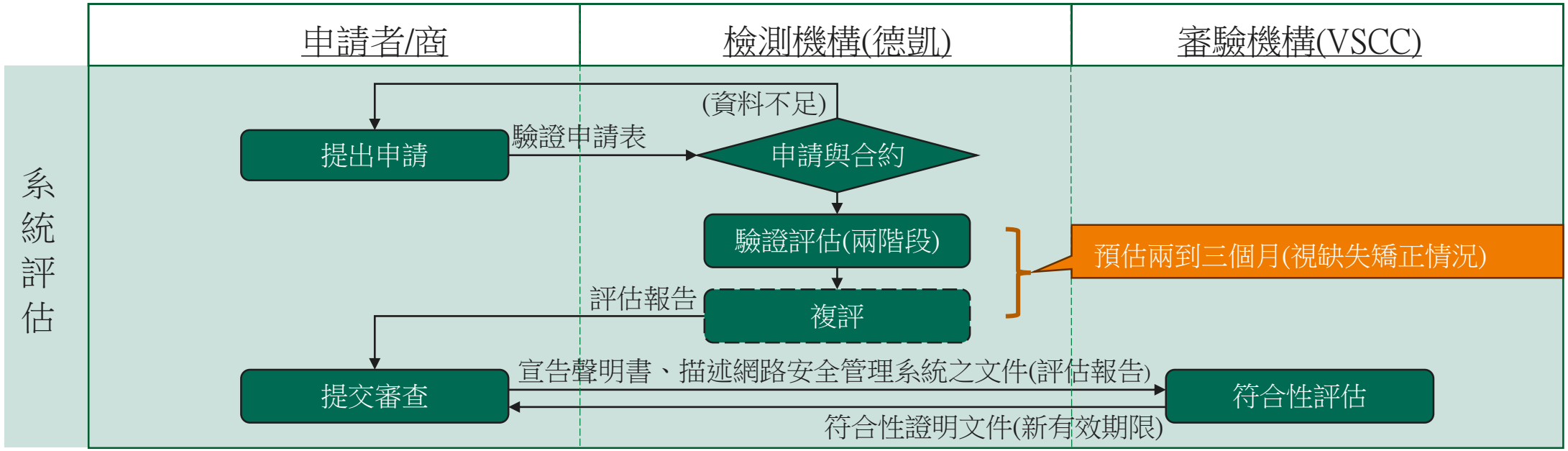
ISO 17021-1Conformity assessment — Requirements for bodies providing audit and certification of management systems



- 驗證評估所需資料
  - 自我評估表、管理系統、執行紀錄、監測活動報告。
- 執行依據
  - 申請者應至少每年一次或更頻繁地(若有相關狀況)向審驗機構或檢測機構報告其監測活動的結果，如5.2.2.2.(g)所定義，這應包括關於新的網路攻擊資訊。申請者還應向審驗機構或檢測機構報告並確認為其車輛型式實施的網路安全緩解措施仍然有效，並且已採取任何其他措施。(VSTD 96 / 5.4.1)
  - 用於監控、檢測和反應網路攻擊、網路威脅和車輛型式漏洞的過程，以及用於評估所實施的網路安全措施是否仍然有效的過程，以確保新的網路威脅和漏洞可被識別。(VSTD 96 / 5.2.2.2(g))
  - 申請者應證明其網路安全管理系統中使用的流程將確保依條文5.2.2.2(g) 規定所述的監控應持續進行。(VSTD 96 / 5.2.2.4)
    - (a) 將首次登記領牌後之車輛納入監測；
    - (b) 包括從車輛資料和車輛紀錄（如保養維修紀錄）中分析和檢測網路威脅、漏洞和網路攻擊的能力。此功能應遵守條文1.3規定及車主或駕駛的隱私權，尤其須經其同意。（本法規不影響其他法規、區域或國家立法關於授權存取車輛、其資料、功能和資源以及相關存取條件，其亦不排除國家或地區有關個人資料保護相關法令之適用。）

申請流程圖 – 重新評估

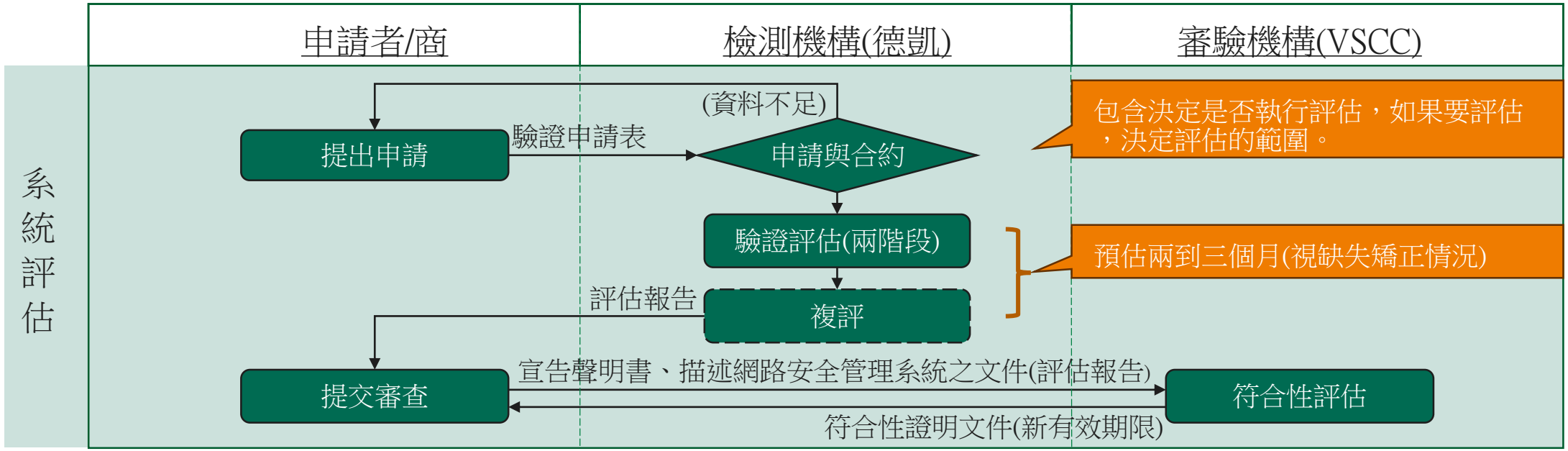
ISO 17021-1Conformity assessment — Requirements for bodies providing audit and certification of management systems



- 執行依據
  - 在CSMS符合性證明文件有效期屆滿前，申請者應向審驗機構（檢測機構）申請新證或延伸現有CSMS符合性證明文件，經審驗機構正向評估(positive assessment)同意後，核發新的CSMS符合性證明文件或延長其證明有效期三年。審驗機構應驗證CSMS是否持續符合本法規的要求。(VSTD 96 / 4.8)
- 驗證評估所需資料
  - 自我評估表、管理系統、執行紀錄、監測活動報告。

申請流程圖 – 變更評估

ISO 17021-1Conformity assessment — Requirements for bodies providing audit and certification of management systems



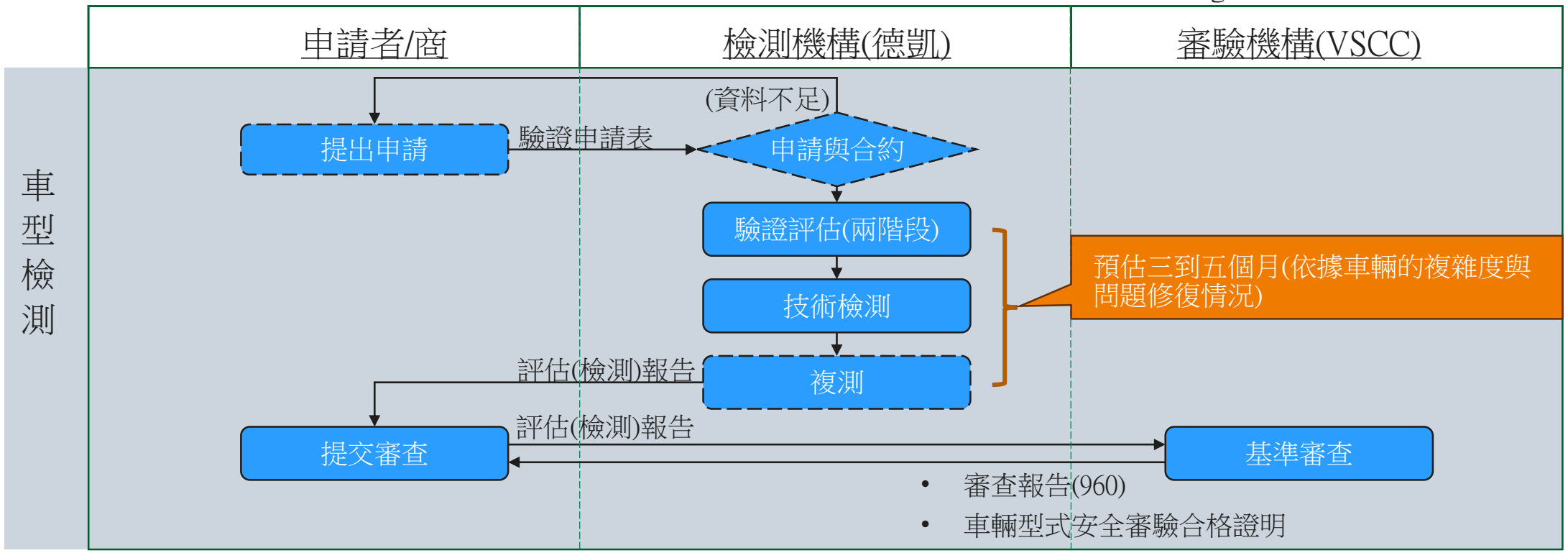
- 執行依據
  - 申請者應向審驗機構或檢測機構通知有關任何影響CSMS符合性證明文件之變化情形，並經與申請者協商確認後，應由審驗機構或檢測機構決定是否有重新進行檢查之必要性。(VSTD 96 / 4.7)
  - 若已向審驗機構或檢測機構申請變更時，則應正向重新評估後，核發新的符合性證明文件(VSTD 96 / 4.8)
  - 對於CSMS相關之車型，若製造商符合CSMS之符合性證明文件期滿或撤銷則應辦理變更認證，其包含無法符合審驗者得撤銷其符合性證明文件。(VSTD 96 / 4.9)
- 驗證評估所需資料
  - 自我評估表、管理系統、執行紀錄、監測活動報告。

《車輛安全檢測基準》附件九十六

網路安全及網路安全管理系統 - 車輛型式要求

申請流程圖 – 車型檢測

ISO 17021-1Conformity assessment — Requirements for bodies providing audit and certification of management systems、
ISO 17025 Testing and calibration laboratories



- 申請商已取得CSMS「符合性證明文件」
  - CSMS應涵蓋申請車輛之開發階段、生產階段、生產後階段。
- 範圍認定標準(VSTD 96 / 3)
  - 車輛廠牌相同。
  - 與網路安全相關的電子電氣架構和外部介面的基本要素相同。
- 檢測依據：
  - 「5.3 對車輛型式的要求」(VSTD 96 / 5.3共10項)。

VSTD 96 / 5.3 對車輛型式的要求

主要透過技術檢測手段以評估有效性

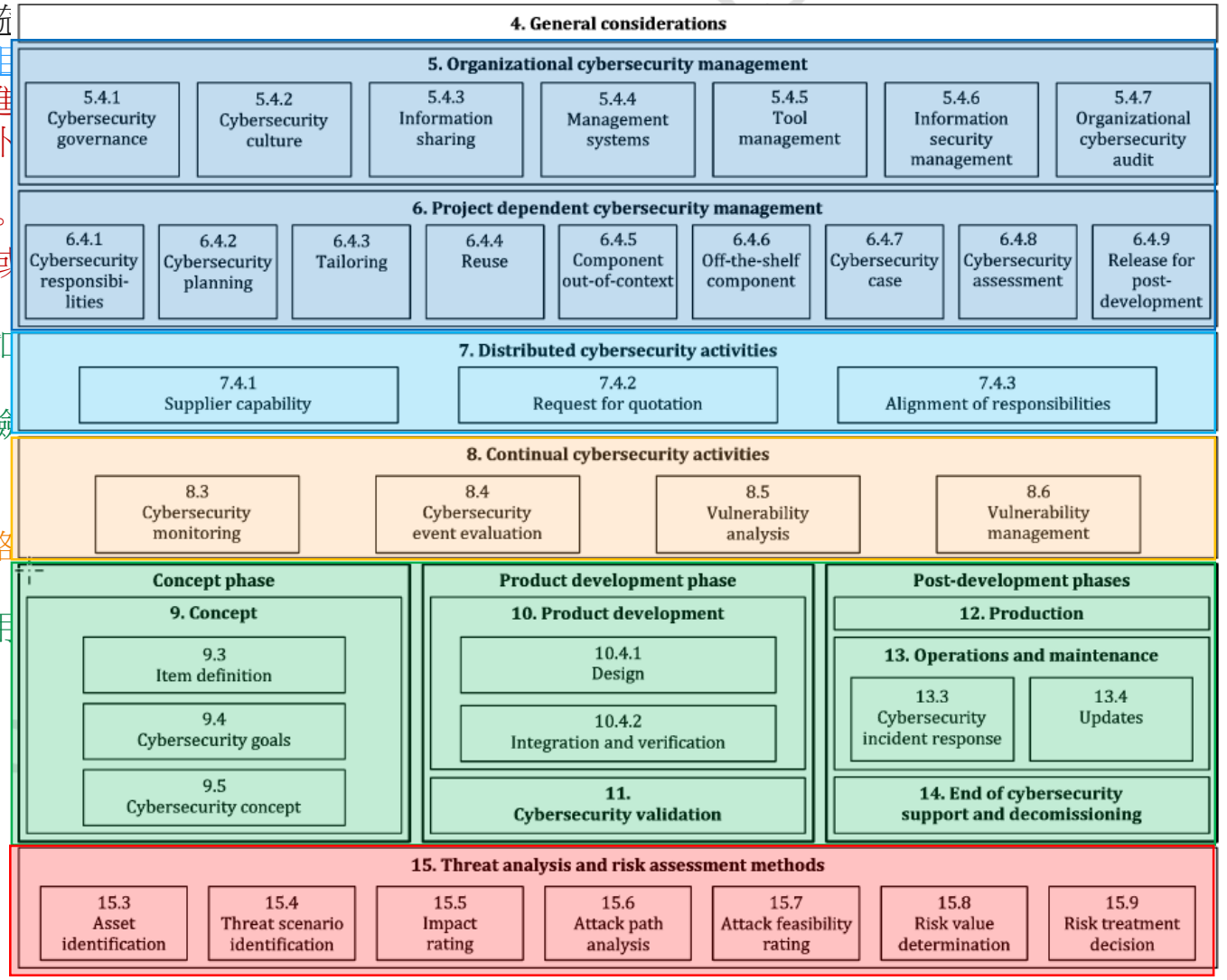
- 5.3.1 申請者應持有與審驗相關車輛型式之網路安全管理系統有效符合性證明文件。
- 5.3.2 申請者應對所認可的車輛型式，識別和管理與供應商相關的風險。
- 5.3.3 申請者應識別車輛型式的關鍵要素，並對該車輛型式進行詳盡的風險評估，並應適當處理/管理已識別的風險。風險評估應考慮車輛型式的各個要素及其互動。風險評估應進一步考慮與任何外部系統的互動。在評估風險時，申請者應考慮依條文6.5規定之所有威脅相關的風險以及任何其他相關風險。
- 5.3.4 申請者應保護車輛型式免申請者風險評估中確定風險。應實施適當的緩解措施以保護車輛型式。實施的緩解措施應包括依條文6.6、6.7規定與識別的風險相關的所有緩解措施。惟若依條文6.6或條文6.7部分規定提到的緩解措施與識別的風險不相關或不充分，則申請者應確保實施另一種適當的緩解措施。
- 5.3.5 申請者應採取適當且相稱的措施，以確保車輛型式（如提供）的專用環境用於售後市場軟體、服務、應用程式或資料儲存和執行（的安全）。
- 5.3.6 申請者應在型式審驗之前進行適當和充分的測試，以驗證所實施的安全措施的有效性。
- 5.3.7 申請者應實施以下措施：
  - (a)檢測並防止針對該型式車輛的網路攻擊；
  - (b)支援申請者在檢測與車輛型式相關的威脅、漏洞和網路攻擊方面的監控能力；
  - (c)提供資料取證能力，以分析未遂或成功的網路攻擊。
- 5.3.8 用於本法規目的的密碼模組應符合共識標準。如果使用的密碼模組不符合共識標準，則申請者應證明其使用的合理性。

VSTD 96 / 5.3 對車輛型式的要求

- 5.3.1 申請者應持有與審驗相關車輛型式之網路安全管理系統
- 5.3.2 申請者應對所認可的車輛型式，識別和管理與供應商相
- 5.3.3 申請者應識別車輛型式的關鍵要素，並對該車輛型式進型式的各個要素及其互動。風險評估應進一步考慮與任何外風險以及任何其他相關風險。
- 5.3.4 申請者應保護車輛型式免申請者風險評估中確定風險。6.7規定與識別的風險相關的所有緩解措施。惟若依條文6.6或確保實施另一種適當的緩解措施。
- 5.3.5 申請者應採取適當且相稱的措施，以確保車輛型式（如安全）。
- 5.3.6 申請者應在型式審驗之前進行適當和充分的測試，以驗
- 5.3.7 申請者應實施以下措施：
  - (a)檢測並防止針對該型式車輛的網路攻擊；
  - (b)支援申請者在檢測與車輛型式相關的威脅、漏洞和網路
  - (c)提供資料取證能力，以分析未遂或成功的網路攻擊。
- 5.3.8 用於本法規目的的密碼模組應符合共識標準。如果使用

稽核重點（Verification）

- 依據條文（上述）查證相關佐證資料。
- 受檢測車輛已依據CSMS，執行到（至少）生產前的階段，並保留佐證資料。
- 依據法規要求查證風險評估已確實且完整執行。
- 以技術檢測方式執行實機檢測，以確認受測車輛的安全性。



車型檢測申請說明

- 驗證與檢測所需資料
  - 系統架構圖，包含功能元件(如IVI、TBOX)、連接界面(如USB、Ethernet)、連線技術(如CAN、ETH、Wireless)等。
  - 整車風險評估分析與控制說明。
  - 資安檢測基本規格調查表。
  - 更新流程說明、連線車輛終端機制、車內網路的設定值(如CAN之相關DBC檔)。
  - 韌體檔案、SBOM/HBOM、ECU清單(含軟韌體版號)。
  - (其他依車輛情況而定)
- 檢測執行說明
  - 需準備一台已完成開發的車輛供檢測用。
  - 廠商需提供車輛依據管理系統的相關作為(執行紀錄)與風險管控說明。
  - 以車輛本身的安全為準(不含主機端)。
  - 車輛測試在檢測機構認可的環境內檢測。
  - 必要時，需要廠商提供特規工具與派員協助檢測。
- 車型檢測重點
  - 已識別風險：驗證風險已被適當緩解。
  - 未識別風險：驗證是否存在潛在未發現的風險或問題。
- 技術檢測評估判定標準
  - 符合：測試結果符合安全性要求。
  - 不符合：測試結果不符合安全性要求。
  - 不適用：本測試項目不適用，如無此功能等。

系統架構圖範例

連線技術（外部）
說明對外連線所使用的傳輸技術。

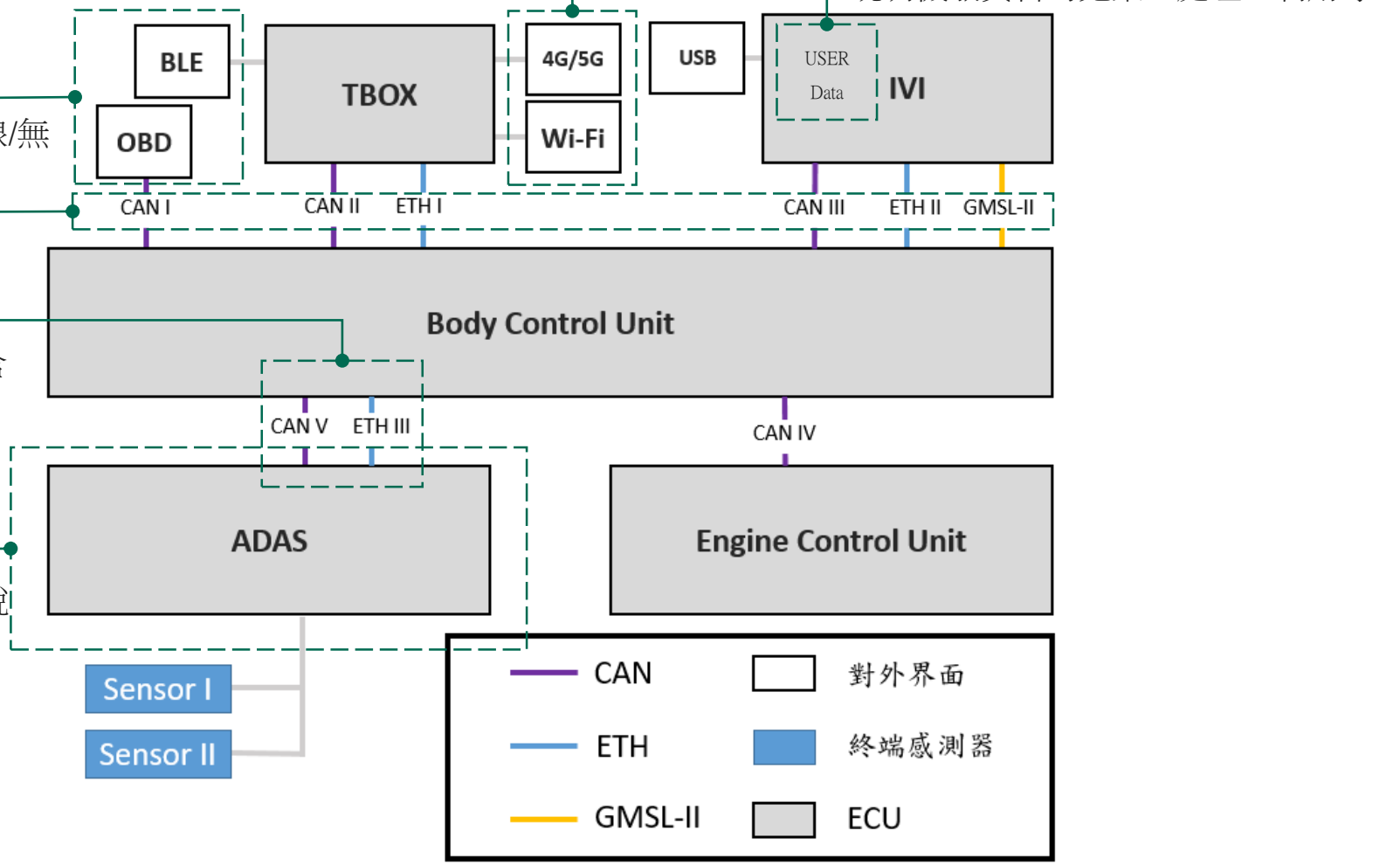
連接界面（外部）
說明對外界面，包含對外開放的有線/無線連接介面與使用者介面等。

連線技術（內部）
說明元件之間的資料傳輸技術。

連接界面（內部）
說明元件之間的資料傳輸通道，包含有線/無線等方式。

功能元件
標示內部的軟硬體元件與模組，並說明主要功能。

機敏資料
說明機敏資料的蒐集、處理、利用等。

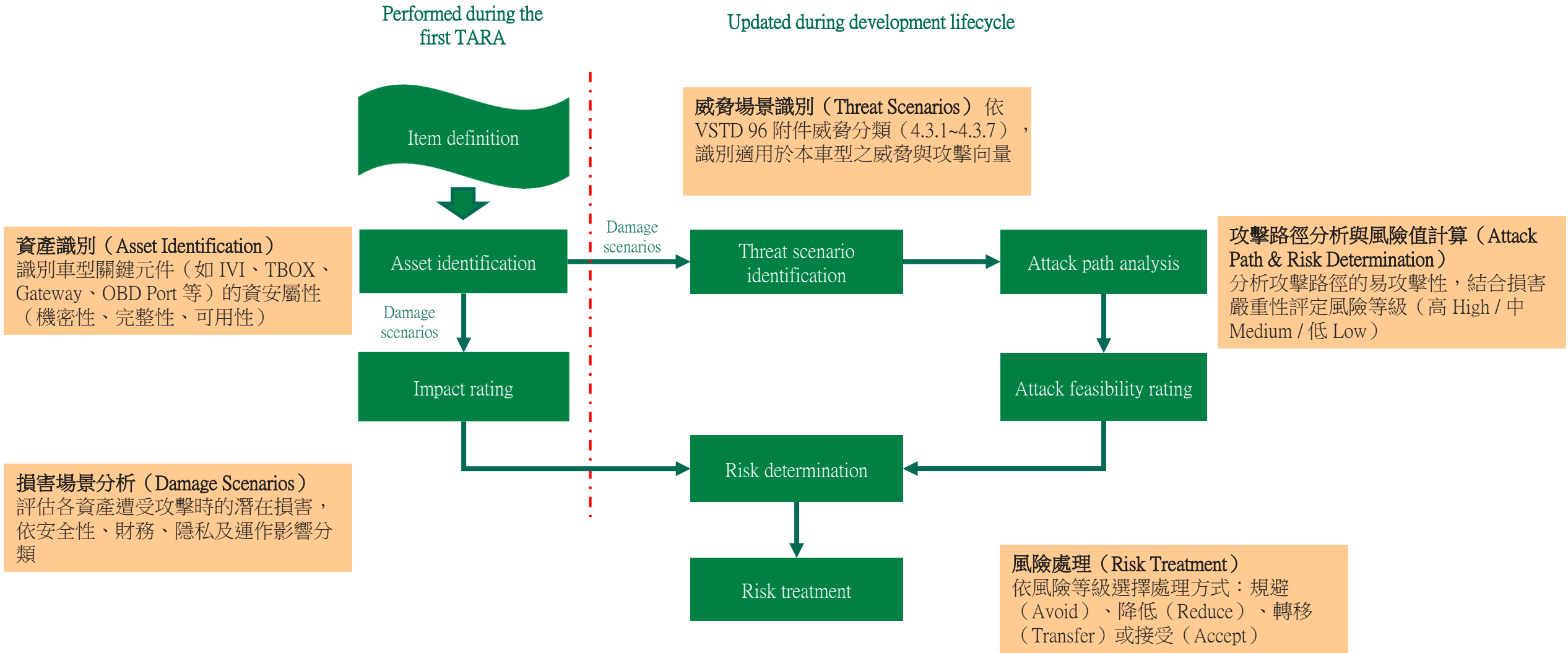


威脅之高等級描述和相關漏洞或攻擊方法（表一）

共7大類、共67項攻擊範例

漏洞/威脅的高等級和次等級描述		攻擊範例
4.3.1 現場車輛相關後端伺服器的威脅	1. 用作攻擊車輛或擷取資料的手段的後端伺服器	3
	2. 後端伺服器服務中斷，影響車輛運作	1
	3. 後端伺服器上保存的車輛相關資料遺失或受損（“資料洩露”）	5
4.3.2 對車輛通訊頻道的威脅	4. 車輛接收到的資訊或資料的欺騙	2
	5. 用於對車輛持有的代碼/資料進行未經授權的操作、刪除或其他修改的通訊頻道	5
	6. 通訊頻道允許接受不可信/不可靠的資訊或容易受到會話劫持/重播攻擊	3
	7. 資訊很容易被揭露，例如，通過竊聽通訊或允許未經授權存取敏感文件或文件夾	2
	8. 通過通訊頻道進行拒絕服務攻擊以破壞車輛功能	2
	9. 非特權使用者能夠獲得對車輛系統的特權存取	1
	10. 嵌入通訊媒體的病毒能夠感染車輛系統	1
	11. 車輛接收的資訊（例如 X2V 或診斷資訊）或在車輛內部傳輸的資訊包含惡意內容	4
4.3.3. 對車輛更新程序的威脅	12. 濫用或破壞更新程序	4
	13. 可以拒絕合法更新	1
4.3.4 因人為意外行為促成網路攻擊而對車輛造成的威脅	15. 合法行為者能夠採取行動，在不知不覺中促進網路攻擊	2
4.3.5 對車輛外部連接和連接的威脅	16. 操縱車輛功能的連接性使網路攻擊變為可行，可能包括遠程資訊服務；允許遠程操作的系統；和使用短距離無線通訊的系統	3
	17. 託管的第三方軟體，例如娛樂應用程式，用作攻擊車輛系統的手段	1
	18. 連接到外部連接埠的設備，例如 USB 端口、OBD 端口，用作攻擊車輛系統的手段	3
4.3.6 對車輛資料/代碼的威脅	19. 擷取車輛資料/代碼	3
	20. 操縱車輛資料/代碼	5
	21. 刪除資料/代碼	1
	22. 惡意軟體介紹	1
	23. 引入新軟體或覆蓋現有軟體	1
	24. 系統或操作中斷	1
	25. 操縱車輛參數	2
4.3.7 如果沒有得到充分保護或加固，可能會被利用的潛在漏洞	26. 加密技術可能受到損害或應用不足	3
	27. 零件或供應品可能會受到破壞，從而使車輛受到攻擊	1
	28. 軟體或硬體開發允許存在漏洞	2
	29. 網路設計引入漏洞	2
	31. 可能會發生意外的資料傳輸	1
	32. 系統的物理操作可以實現攻擊	1

風險評估（以TARA為例）



車型檢測示意 – 4.2 女巫(Sybil)攻擊

女巫攻擊（Sybil Attack）

駭客透過偽造多個虛假身份，使單一惡意節點看起來像是一群車輛，藉此操縱網路判斷，可能造成的問題：

- 高級輔助駕駛系統 (ADAS)：若系統接收到數十個虛假車輛回報前方有障礙物，可能導致車輛無預警緊急煞車。
- 自動駕駛 (Self-Driving Cars)：自動駕駛車需要高度精確的環境建模，Sybil Attack 可透過大量偽造位置訊息誤導路徑規劃。
- 排隊行駛 (Platooning) 功能：多輛車以近距離串聯行駛時，若其中一個身分是被偽造的，會影響整個車隊的安全間距控制。

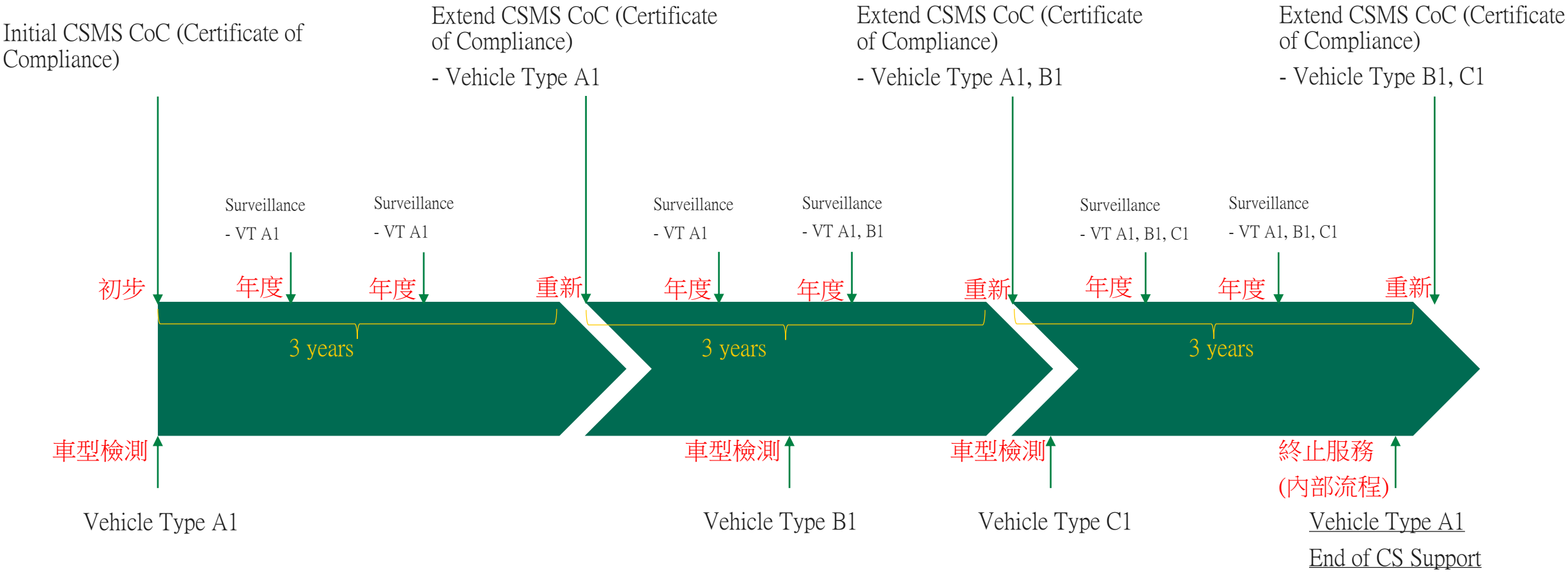
具備被 Sybil Attack 風險的汽車類型與技術特徵：

- 具備 V2X 通訊能力的聯網汽車 (Connected Vehicles)
- 依賴協作式感知與決策的車輛
- 使用去中心化或基於地理路由的系統

測試手法：

- 依照車輛設計及使用之通訊協定進行女巫攻擊實作，以IEEE 1609.2為例，則使用多個certificate bundle配合CAN工具進行模擬發送（可能透過無線方式或直接接取車輛內部之CAN Bus），造成受測車輛附近出現多個虛擬車輛之情境。

運作與維護情境(取得符合性證明文件後)



《車輛安全檢測基準》附件九十七

軟體更新及軟體更新管理系統 - 管理系統要求

VSTD 97 服務項目

01 系統評估 - 初步評估

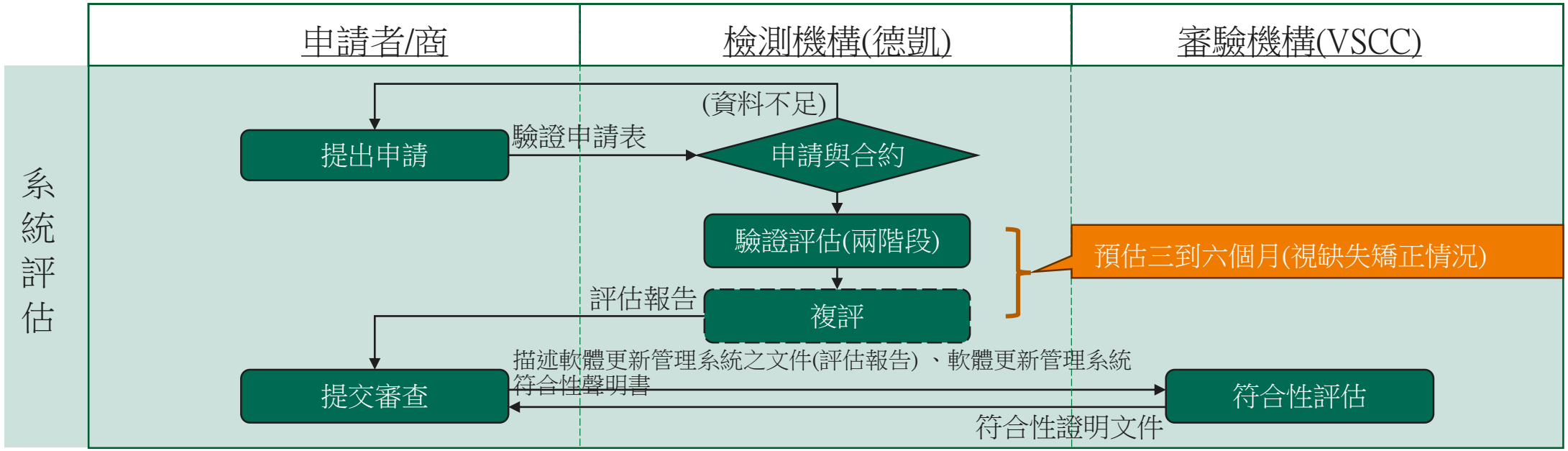
02 系統評估 - 重新評估

03 系統評估 - 變更評估

04 車型檢測

申請流程圖 – 初步評估

ISO 17021-1Conformity assessment — Requirements for bodies providing audit and certification of management systems



- 驗證評估範圍認定
  - 一個法律實體內參與SUMS活動的所有部門。
- 評估依據
  - 「5.1 對申請者之軟體更新管理系統要求」(VSTD 97 / 5.1共30項)。
- 驗證評估所需資料
  - 自我評估表、管理系統、執行紀錄。

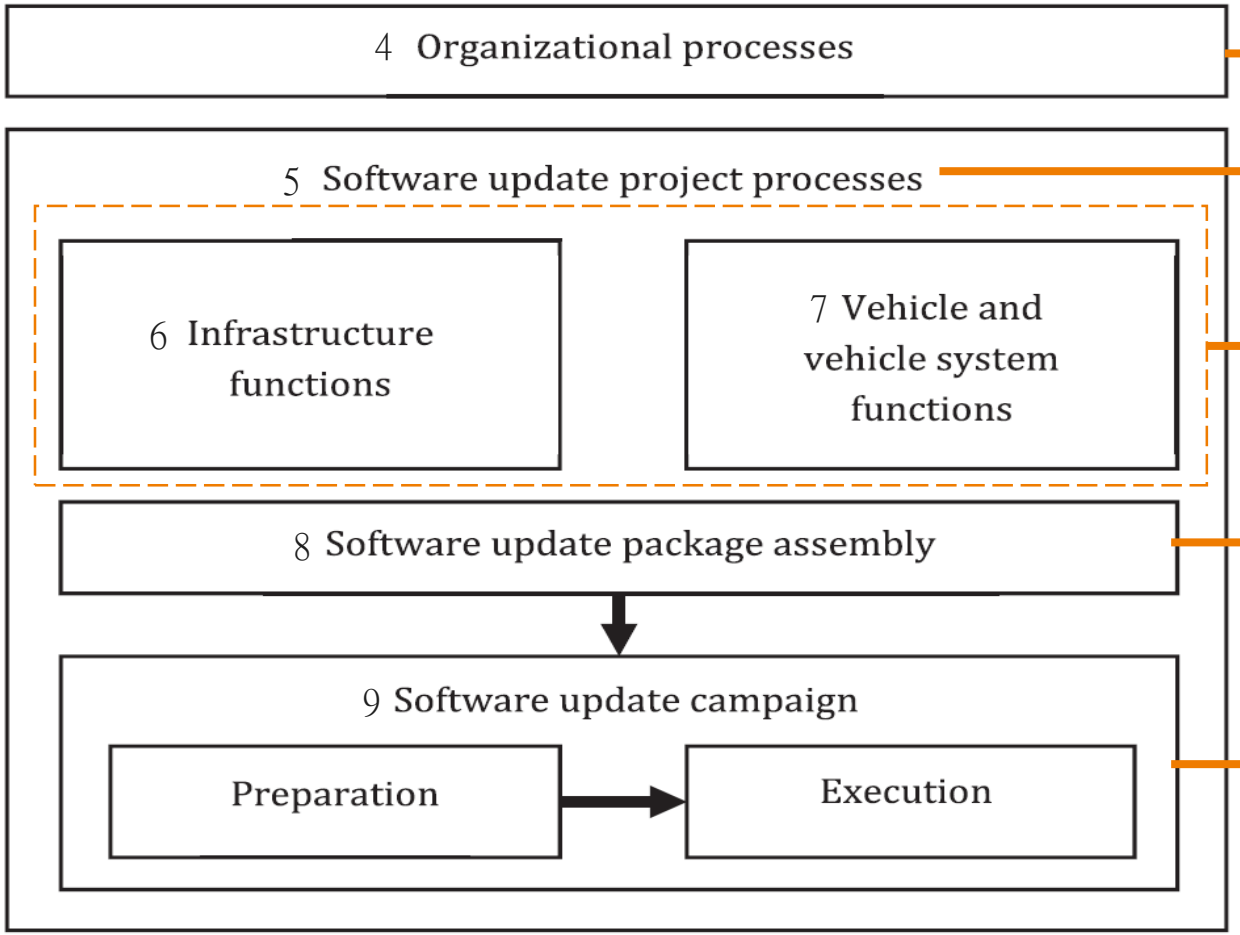
VSTD 97 / 5.1 對申請者之軟體更新管理系統要求

- 5.1.1 初步評估之驗證程序
  - 5.1.1.1 將與本項法規有關的資訊，於申請者處記錄及安全地保存，並可提供予審驗機構或其檢測機構之程序。
  - 5.1.1.2 可唯一識別所有初始和更新軟體版本資訊的程序，包括完整性驗證數據，以及型式認證系統相關之硬體零組件。
  - 5.1.1.3 對於具有RXSWIN的車輛型式，可藉以存取和更新有關該車輛型式於軟體更新前後 RXSWIN資訊的程序。這應包括更新每個RXSWIN的軟體版本及其所有相關軟體的完整性驗證數據能力。
  - 5.1.1.4 對於具有RXSWIN的車輛型式，申請者可藉以驗證型式認證系統零組件所存在之軟體版本與相關RXSWIN所定義版本一致的程序。
  - 5.1.1.5 可藉以確定更新的系統與其他系統任何相互依賴關係的程序。
  - 5.1.1.6 申請者能夠識別目標車輛進行軟體更新的程序；
  - 5.1.1.7 在軟體更新發布前確認其與目標車輛配置相容性的程序，應包括在發布前評估目標車輛最後已知的軟體/硬體配置與更新之相容性。
  - 5.1.1.8 評估、識別和記錄軟體更新是否會影響任何型式認證系統的程序，並應考慮更新是否會影響或改變用於定義更新可能影響的系統任何參數，或是否會改變用於對這些系統進行型式認證的任何參數（如相關法律所定義）。
  - 5.1.1.9 評估、識別和記錄軟體更新是否會增加、改變或啟用車輛型式認證時，不存在或未啟用的任何功能，或改變或禁用法律規定的任何其他參數或功能之程序。該評估應考慮包括如下：
    - (a) 將需要修改的條目資訊；
    - (b) 測試結果不再涵蓋改裝後的車輛；
    - (c) 車輛功能的任何修改將影響車輛型式認證。
  - 5.1.1.10 評估、識別和記錄軟體更新是否會影響車輛安全和持續運行所需的任何其他系統，或者更新是否會增加或改變車輛與註冊時相比的功能之程序；
  - 5.1.1.11 車輛使用者能夠被通知更新資訊的程序；
  - 5.1.1.12 申請者應能依據條文5.1.2.3和5.1.2.4規定之資訊提供予審驗機構或檢測機構的程序。

VSTD 97 / 5.1 對申請者之軟體更新管理系統要求(cont.)

- 5.1.2 申請者應記錄並儲存適用於提供車型每次更新的資訊如下：
  - 5.1.2.1 描述申請者用於軟體更新流程的文件，以及用於展演其符合的任何相關標準；
  - 5.1.2.2 描述更新前後任何相關型式認證系統配置的文件，包括型式認證系統的硬體和軟體（包括軟體版本），以及任何相關車輛或系統參數的唯一標識。
  - 5.1.2.3 對於每個RXSWIN，應當有一個可核對的記錄器(auditable register)，描述更新前後與該車型RXSWIN相關的所有軟體。這應包括每個RXSWIN所有相關軟體的軟體版本及其完整性驗證數據資訊。
  - 5.1.2.4 列出更新的目標車輛，並確認這些車輛最後已知配置與更新相容性的文件。
  - 5.1.2.5 描述該車型的所有軟體更新文件：
    - (a) 更新的目的
    - (b) 更新可能影響之車輛系統或功能
    - (c) 已通過型式認證之軟體更新（依實際狀況）
    - (d) 軟體更新是否影響到型式認證系統任何相關要求（依實際狀況）
    - (e) 軟體更新是否影響到任何系統型式認證參數
    - (f) 是否已取得審驗機構對更新之認可
    - (g) 執行更新方式及執行條件
    - (h) 確認可安全且可靠的執行軟體更新
    - (i) 確認軟體更新已完成並通過認證和確認程序
- 5.1.3 安全性—申請者應展演下列程序：
  - 5.1.3.1 確保軟體更新受到保護之程序，其可於更新過程開始之前合理的防止竄改；
  - 5.1.3.2 對所使用的更新程序進行保護，以合理地防止其被破壞，包括開發更新交付系統；
  - 5.1.3.3 用於驗證和確認車輛使用的軟體功能和代碼的程序是適當的。
- 5.1.4 對軟體無線（空中）更新的額外要求
  - 5.1.4.1 申請者應展演將使用之流程和程序，以評估若在駕駛過程中進行無線（空中）更新，不會影響安全。
  - 5.1.4.2 申請者應展演所使用的流程和程序，以確保當無線（空中）更新需要一個特定熟練或複雜的動作時（例如在編譯後重新校準一個傳感器，以完成更新過程），只有當一個熟練地做該動作的人在場或控制該流程時才能進行更新。

Best Practice – ISO 24089（以風險評估資產識別為例）



Top level design and dependencies

Project level management

What processes and functions are required to support SW update engineering

How to deploy a SW update package assembly

How to do a SW update campaign

Best Practice – ISO 24089（以專案層要求為例）

Objectives

- a) planning for a software update project, including assigning roles and responsibilities;
- b) managing and storing of information regarding a software update project;
- c) providing justifications for any tailoring of a software update project;
- d) confirming interoperability of the infrastructure and the vehicle functions for a software update project; and
- e) preserving integrity of software, and either metadata or software update packages, or both.

Requirement	Work Products
5.3.1.1 The organization shall develop, implement and maintain a plan for each software update project that covers all necessary activities. **5.3.1.2** The organization shall manage and store documentation for each software update project. **5.3.1.3** The organization shall establish, assign and maintain the roles and responsibilities for each software update project. **5.3.2.1** A software update project may be tailored. **5.3.2.2** If a software update project is tailored, then a rationale shall be provided as to how the tailored activities achieve the applicable objectives of this document. **5.3.3.1** The organization shall establish, implement and maintain a process to confirm the interoperability of the functions developed in accordance with the requirements from Clause 6 and Clause 7. **5.3.4.1** The organization shall establish, implement and maintain processes to preserve the integrity of software, and either metadata or software update packages, or both, during distribution in the context of interoperability:…	**5.4.1** Software update project plan resulting from the requirements of 5.3.1.1 and 5.3.1.3. **5.4.2** Documentation of software update project resulting from the requirement of 5.3.1.2. **5.4.3** Rationale for tailored activities, if applicable, resulting from the requirement of 5.3.2.2. **5.4.4** Documentation of confirmation of interoperability resulting from 5.3.3.1. **5.4.5** Documentation of processes to preserve integrity from 5.3.4.1

系統評估標準（持續優化）

Evaluation of the findings according to table 1 in ISO/PAS 5112:2022, section 6.4.8

Objective evidence regarding full achievement of all objectives	Conformity
Minor deviations were observed	Minor nonconformity
Major deviations were observed, one or more objectives are not achieved	Major nonconformity

Deriving the audit result according to table 2 in ISO/PAS 5112:2022, section 6.4.9

There are no major nonconformities and no minor nonconformities.	Pass
There is one or more minor nonconformities, but no major nonconformities. Identified minor nonconformities do not call into question the overall effectiveness of the CSMS.	Conditional pass
One or more major nonconformities or several minor nonconformities that, due to their number or in their dependencies, call into question the overall effectiveness of the CSMS.	Fail

軟體更新管理系統(Software Update Management System, SUMS)：係指定義組織的過程和程序之系統方法，以符合提交軟體更新之要求。

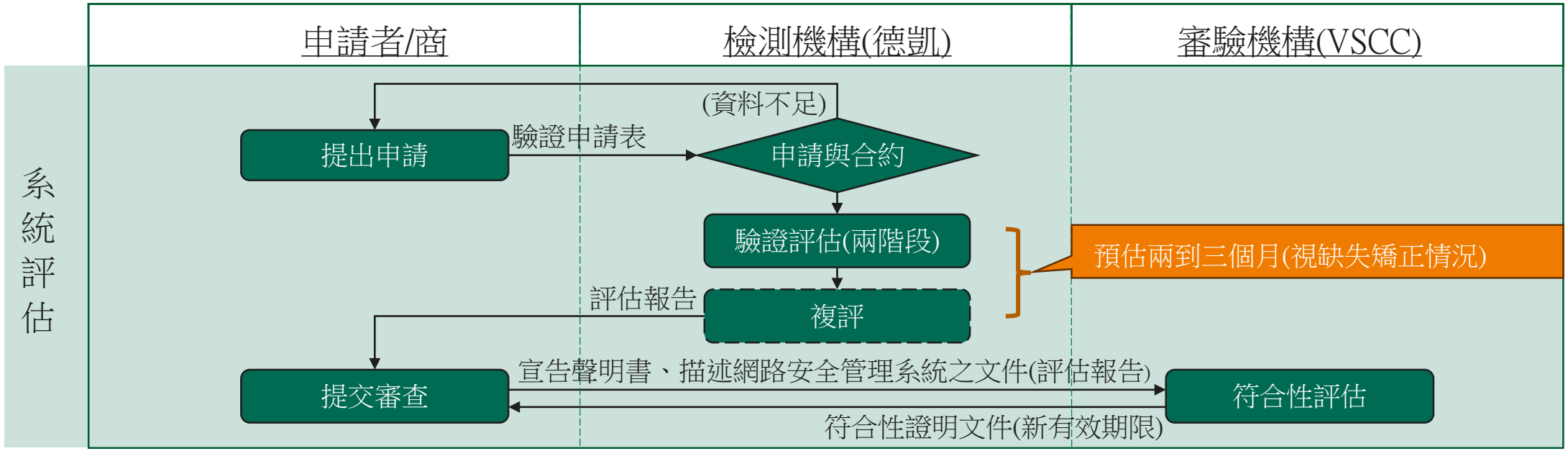
"Software Update Management System (SUMS)" means a systematic approach defining organizational processes and procedures to comply with the requirements for delivery of software updates according to this Regulation.

稽核重點（Verification）

- **管理系統已存在（Exist）**：對應所有要求的流程文件已建立並實施。
- **管理系統已落實（Execution）**：管理系統相關活動均有正式紀錄，如內部稽核、管理審查、軟體更新等。
- **管理系統確認有效（Effectiveness）**：確認規劃的做法有效，同時團隊有能力執行。

申請流程圖 – 重新評估

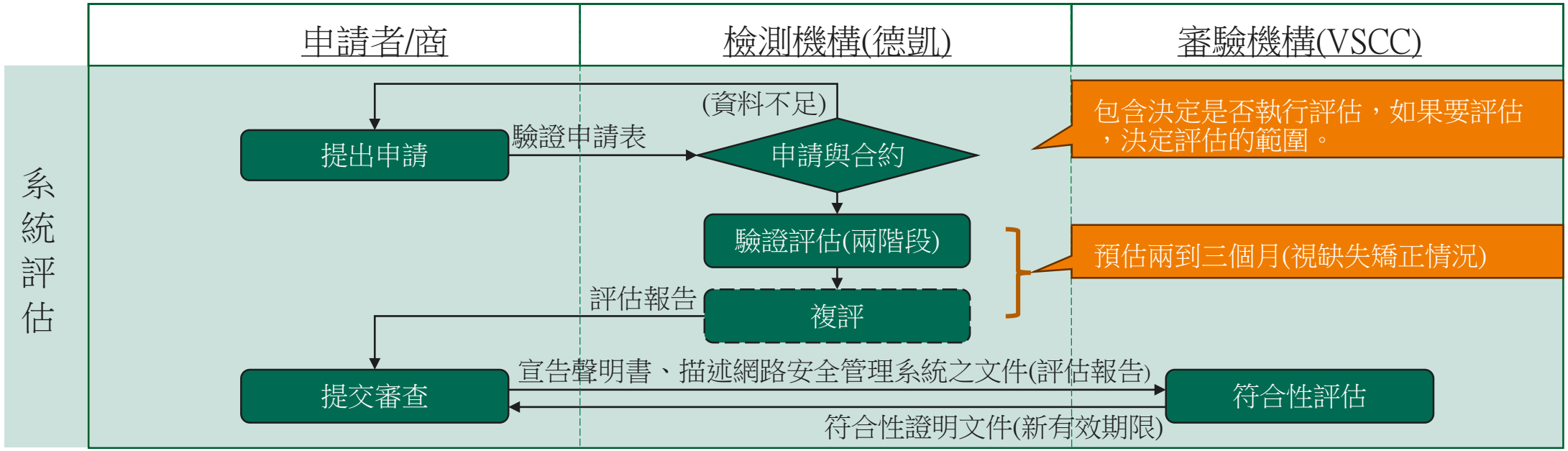
ISO 17021-1Conformity assessment — Requirements for bodies providing audit and certification of management systems



- 執行依據
  - 在軟體更新管理系統符合性證明文件有效期屆滿前，申請者應向審驗機構申請新符合性證明文件或延伸現有SUMS符合性證明文件，經審驗機構正向評估(positive assessment)同意後，核發新的軟體更新管理系統符合性證明文件或展延其有效期三年。(VSTD 97 / 4.7)
- 驗證評估所需資料
  - 自我評估表、管理系統、執行紀錄。

申請流程圖 – 變更評估

ISO 17021-1Conformity assessment — Requirements for bodies providing audit and certification of management systems



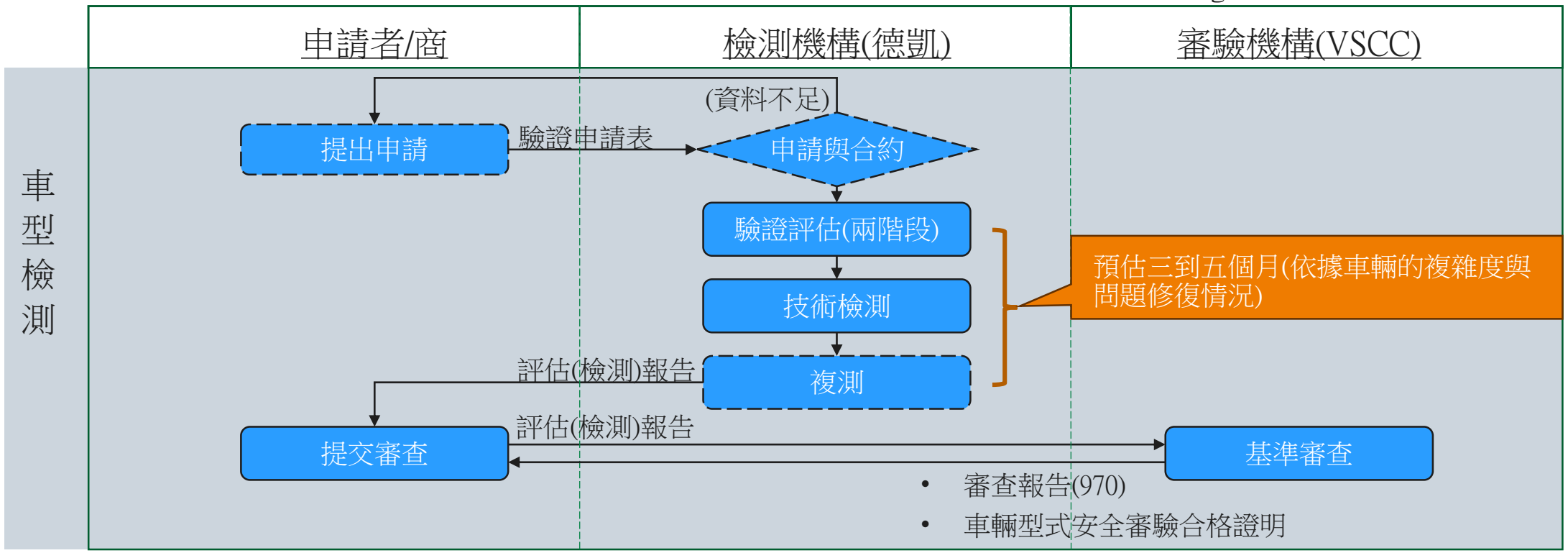
- 執行依據
  - 申請者應向審驗機構或其檢測機構通知有關任何影響軟體更新管理系統符合性證明文件之變化情形，並經與申請者協調確認後，應由審驗機構或其檢測機構決定是否有重新進行檢查之必要性。(VSTD 97 / 4.6)
  - 如已向審驗機構或其檢測機構申請變更時，則應重新評估後，核發新的符合性證明文件。(VSTD 97 / 4.7)
  - 若申請者所取得之軟體更新管理系統符合性證明文件因逾期而失其效力時，不影響先前據此所取得之車輛型式安全審驗合格證明之有效性。(VSTD 97 / 4.8)
- 驗證評估所需資料
  - 自我評估表、管理系統、執行紀錄。

《車輛安全檢測基準》附件九十七

軟體更新及軟體更新管理系統 - 車輛型式要求

ISO 17021-1Conformity assessment — Requirements for bodies providing audit and certification of management systems、
ISO 17025 Testing and calibration laboratories

申請流程圖 – 車型檢測



- 申請商已取得SUMS「符合性證明文件」
- 範圍認定標準(VSTD 97 / 3)
  - 車輛廠牌相同。
  - 設計之軟體更新過程相同。
- 檢測依據：
  - 「5.2 對車輛型式的要求」(VSTD 97 / 5.2共17項)。

VSTD 97 / 5.2 對車輛型式的要求

- 5.2.1 對軟體更新的要求
  - 5.2.1.1 應保護軟體更新的真實性和完整性，以合理地防止其被破壞，並合理地防止無效更新。
  - 5.2.1.2 在車輛型式使用RXSWIN時：
    - 5.2.1.2.1 每個RXSWIN應是唯一可識別的。當申請者修改型式認證相關軟體時，如果導致型式認證延伸或新的型式認證，應更新RXSWIN。
    - 5.2.1.2.2 每個RXSWIN應通過使用電子通訊界面，至少通過標準介面（OBD埠），以標準化的方式易於讀取。如果車輛未擁有RXSWIN，申請者應向審驗機構聲明車輛或單個ECU的軟體版本，並與相關型式認證連結。每次更新所聲明的軟體版本時，應更新該聲明。在這種情況下，軟體版本應通過使用電子通訊界面，至少通過標準介面（OBD埠），以標準化的方式易於讀取。
    - 5.2.1.2.3 申請者應保護車輛上的RXSWIN和/或軟體版本，以防止未經授權修改。在進行型式認證時，應以保密方式提供申請者作為防止未經授權修改RXSWIN和/或軟體版本所採取的措施。

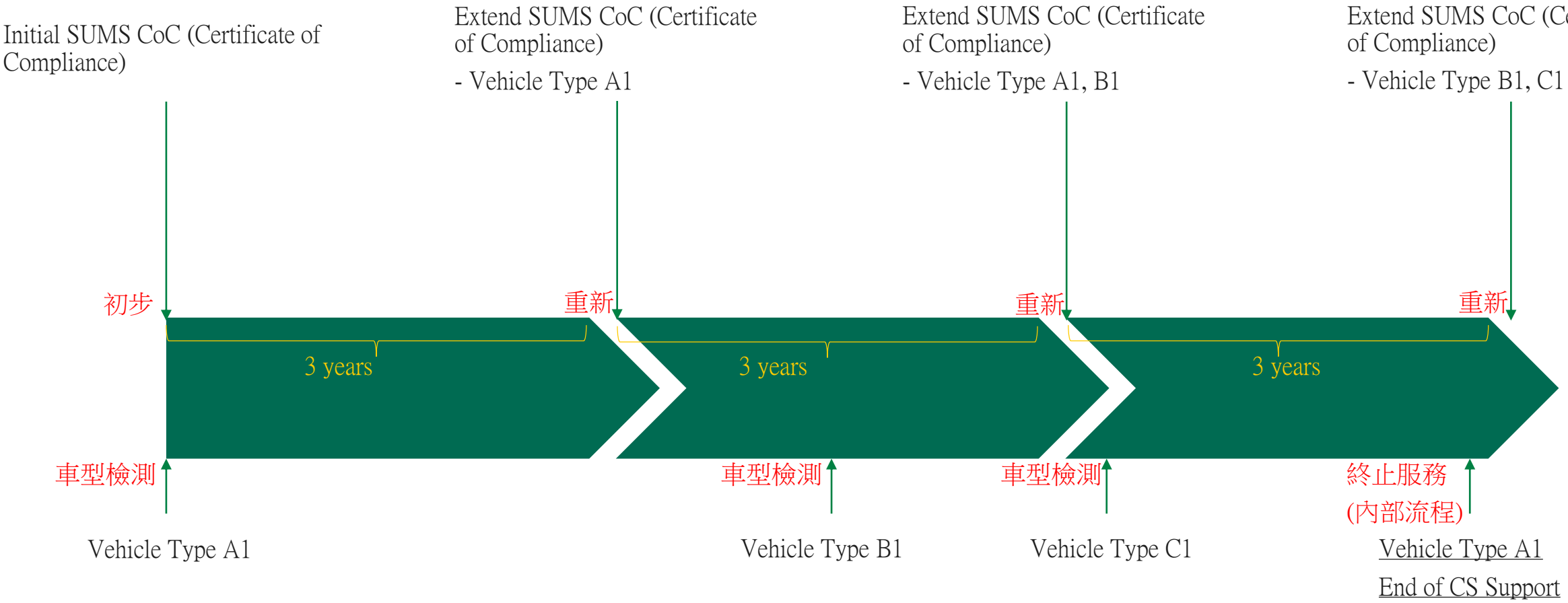
VSTD 97 / 5.2 對車輛型式的要求(cont.)

- 5.2.2 對軟體無線（空中）更新的額外要求
  - 5.2.2.1 車輛應具備以下有關軟體更新的功能：
    - 5.2.2.1.1 申請者應確保在更新失敗或中斷的情況下，車輛能夠將系統恢復到以前的版本，或者在更新失敗或中斷後，車輛能夠置於安全狀態。
    - 5.2.2.1.2 申請者應確保車輛只在有足夠的電力完成更新過程時才能執行軟體更新（包括可能恢復到以前的版本或將車輛置於安全狀態所需的電力）。
    - 5.2.2.1.3 當執行更新可能影響車輛的安全時，申請者應展演如何安全地執行更新。此應通過技術手段實現，以確保車輛處於可以安全執行更新的狀態。
  - 5.2.2.2 申請者應證明，在執行更新之前，車輛使用者能夠被告知有關更新的情況。所提供的資訊應包括：
    - (a) 更新的目的。這可能包括更新的關鍵性，以及更新是否是為了召回、安全和/或防護性(security)目的。
    - (b) 對車輛功能更新所實施的任何改變；
    - (c) 完成更新執行的預期時間；
    - (d) 在執行更新期間可能無法使用的任何車輛功能；
    - (e) 任何可能幫助車輛使用者安全執行更新的指示；
    - 在內容相似的更新群體情況下，一個資訊可以覆蓋一個群組。
  - 5.2.2.3 在駕駛時執行更新可能不安全的情況下，申請者應證明：
    - (a) 確保在執行更新的過程中不能駕駛車輛；
    - (b) 確保駕駛者不能使用車輛的任何功能，以免影響車輛的安全或更新的成功執行。
  - 5.2.2.4 在執行更新後，申請者應證明如何執行以下內容：
    - (a) 告知車輛使用者更新成功（或失敗）；
    - (b) 通知車輛使用者所實施的改變以及對使用手冊的任何相關更新（如果適用）。
  - 5.2.2.5 車輛應確保在執行軟體更新前必須滿足所需的先決條件。

車型檢測申請說明

- 驗證與檢測所需資料
  - 系統架構圖，包含功能元件(如IVI、TBOX)、連接界面(如USB、Ethernet)、連線技術(如CAN、ETH、Wireless)等。
  - 整車風險評估分析與控制說明。
  - 資安檢測基本規格調查表。
  - 更新流程說明、連線車輛終端機制、車內網路的設定值(如CAN之相關DBC檔)。
  - 韌體檔案、SBOM/HBOM、ECU清單(含軟韌體版號)。
  - (其他依車輛情況而定)
- 檢測執行說明
  - 需準備一台已完成開發的車輛供檢測用。
  - 廠商需提供車輛依據管理系統的相關作為(執行紀錄)與風險管控說明(更新部分)。
  - 以車輛本身的更新安全為準(不含主機端)。
  - 車輛測試在檢測機構認可的環境內檢測。
  - 必要時，需要廠商提供特規工具與派員協助檢測。
- 車型檢測重點
  - 已識別風險：驗證風險已被適當緩解。
  - 未識別風險：驗證是否存在潛在未發現的風險或問題。
- 技術檢測評估判定標準
  - 符合：測試結果符合安全性要求。
  - 不符合：測試結果不符合安全性要求。
  - 不適用：本測試項目不適用，如無此功能等。

運作與維護情境(取得符合性證明文件後)



服務聯繫窗口

Lucy Chen

lucy.chen@dekra.com

+886-976-850-158

+886-2-8911-5035

www.dekra.com.tw

DEKRA

自1925年起成為安全與可持續發展世界裡的全球合作夥伴。