政府資料傳輸平臺(T-Road)
資料保護衝擊影響評估報告

委託機關：數位發展部

受託單位：安侯企業管理股份有限公司

中華民國 113 年 4 月

摘要

行政院於 108 年 1 月 10 日核定「智慧政府推動策略計畫」，數位發展部(以下簡稱 本部)以政府骨幹網路(Government Service Network，以下簡稱 GSN)為基礎，建置跨機關資料傳輸專屬通道及管理平臺(以下簡稱 T-Road)，欲介接 T-Road 之各級機關須預先將資訊服務集中於資料中心，或建立資料傳輸專屬網段，於通過審核後方可介接 T-Road，其資料傳輸專屬網段不與外部服務網段連通。資料傳輸機制建立前，須由資料需求機關依法向資料提供機關提出申請，經資料提供機關通過審核後才可使用 T-Road 傳輸資料；此外，為確保各級機關資料在 T-Road 上之資通安全與隱私保護措施無虞，資料傳輸過程均以政府憑證管理中心所核發之憑證（Government Certification Authority，以下簡稱 GCA)全程加密，並附加數位簽章與時戳。

T-Road 管理平臺並不保存各級機關間之傳輸資料內容，僅保存傳輸紀錄，且傳輸紀錄均以區塊鏈方式儲存，以確保其不可否認及資料傳輸之透明性。

本部以設計保護隱私概念(Privacy by design/default, PbD&D)，確保 T-Road 服務規劃於開發及設計時，即已導入隱私保護之概念及防護措施，並依資訊發展趨勢每年定期檢視。參考個人資料保護法、個人資料保護法施行細則及 NIST 800-122、ISO 29134、APEC 隱私權保護九大原則、ISO 27001、ISO 27701 之國際標準相關要求，以資料流程導向，從資料蒐集、傳輸、處理與利用之適法性、安全性及介接機關之角色與權責，評估各項已知或潛在風險。透過法規遵循分析、隱私保護與資安防護管理要求、控制措施、技術防護、日誌監控與稽核活動，不斷精進與持續改善，提供安全且可信賴的資料傳輸服務。

目　錄

壹、概述

一、 政府資料傳輸平臺簡介

T-Road以政府骨幹網路(GSN)為基礎，規劃專屬資料傳輸通道，於資料提供機關基於業務之權責，透過專屬網段與資料需求機關進行資料傳輸。T-Road 為跨機關之政府資料傳輸平臺，針對資料傳輸提供應用程式介面服務(以下簡稱 API 服務)及管理，確保資料傳輸紀錄之可追溯性，T-Road 傳輸概念簡述如下：

(一) 資料提供機關及資料需求機關(兩者合稱介接機關)之資料傳輸時間、服務名稱、傳輸成功或失敗等資料傳送紀錄，均由資料傳輸功能管理平臺(以下簡稱T-Road管理平臺)完整記錄，惟T-Road 管理平臺及 T-Road 維運機關並不留存介接機關間相互傳輸之內容。

(二) 提供單一客服聯絡電話，協助障礙排除、操作安裝諮詢；另提供資通安全事件緊急應變措施，隨時監控系統運作情形。

(三) T-Road 資料傳輸情境說明

1. 資料需求機關如有資料創新應用、便民服務等公務需求時，依循個人資料保護法(以下簡稱 個資法)規範，確認資料傳輸適法性要求，如個資法蒐集、處理及利用之要求。
2. 資料需求機關與資料提供機關須事先向 T-Road 維運機關申請安裝安控伺服器(Security Server，以下簡稱 SS)，並將 SS 註冊至 T-Road 管理平臺，T-Road 管理平臺由 T-Road 維運機關負責維運。
3. 資料提供機關將可提供資料之清單註冊至 T-Road 管理平臺。
4. 資料需求機關透過安控伺服器知悉資料提供機關可提供之資料清單。
5. 資料需求機關透過 SS 向資料提供機關申請使用資料。
6. 資料提供機關審核並設定資料需求機關之查調權限，並將查調結果同步至 T-Road 管理平臺。

7. 資料需求機關通過身分驗證後，透過 T-Road 向資料提供機關取得資料。
8. 資料傳輸紀錄歷程均紀錄於介接機關間之 SS，並同步保存於 T-Road 管理平臺。

二、 資料保護衝擊分析(DPIA)

(一) DPIA(Data Protection Impact Assessments)，資料保護衝擊評估，為考量個人資料之生命周期執行其隱私相關的評估，包含辨識、分析可能產生資料保護風險，著重於保護隱私資料的準確性、保密性、完整性、實際安全性。

(二) 政府骨幹網路資料保護衝擊評估(DPIA)基本概念，為透過早期施行 DPIA，可在事前就評估資料處理可能面臨的風險，並非在取得資料後才規劃各項安全控管，更能提高資料應用的合規，並且透過事前充分的安全評估，強化政府施政透明度、可靠性、穩定性及民眾對個人資料的掌控，涉及資料傳輸之公務機關，均應遵循資安、個資相關法令要求，若能早期鑑別需要遵守的法令，俾利各公務機關明確了解應遵循各項安全控管作為，其執行概念如下：

1. 應於資料蒐集前事前進行資料侵害可能性評估，並優先規劃安全控管措施。
2. 應確認資料利用合於法規要求，當事人不必額外採取其他保護資料的作為。
3. 應確認資料處理是否具足夠強度的安全控管措施，且盡可能提高控管規格。
4. 確認系統規劃與實作各階段，均考慮到隱私應用風險。
5. 確認安全控管措施是否涵蓋資料生命週期。
6. 是否提前強化政府政策溝通與民眾意見回饋，使資料處理透明化，且確保當事人知情的權利。
7. 是否具適當措施，充分尊重當事人個資權利，使民眾利益獲得保障。

三、 資料保護衝擊資料風險評估執行範圍

(一) 政府資料傳輸平臺之 DPIA 範圍，包含系統開發、維運等各階段，及介接機關於系統發展週期內之應辦事項，包含：

1. 系統開發、維運安全評估項目。

2. 資料傳輸安全評估項目。

3. 介接機關介接 T-Road 前、後之安全評估項目。

(二) 評估期間為 113 年 1 月 29 日至 3 月 31 日。

(三) T-Road 之 DPIA 應持續進行，搭配 T-Road 管理平臺開發、維運等各階段，進行全部或一部分之評估。

四、 評估方法

(一) 針對 T-Road 開發團隊，以人員訪談、文件審查與實地檢視方式，依據 T-Road 開發管理、運作方式等規範進行安全評估，並依 T-Road 傳輸功能區分為下列角色，依各角色之應辦事項進行評估：

1. T-Road 維運機關。

2. 資料中心設置機關安全要求。

3. 介接機關安全要求。

(二) T-Road 建置期間風險評估方法

1. T-Road 維運機關建置 T-Road 時，需於整體開發期間，確認各項開發過程風險，如：

(1) 系統開發安全規則。

(2) 開發過程中系統功能變更安全管理程序。

(3) T-Road 運作平臺運作程式、軟體之弱點檢查與修補。

(4) 軟體套件修改限制。

(5) T-Road 系統架構安全弱點修補，如傳輸方式、資料運用、應用系統輸入、輸出等技術面安全。

(6) 委外開發監督安全。

(7) 系統安全測試及測試資料保護。

(8) 驗收系統安全方法。

2. 由外部提供之各項服務安全。

3. 服務提供者安全協議。

4. 服務提供整體供應鏈安全。

5. 服務提供者監視與審查。

6. 服務提供者服務變更安全。

(三) T-Road 整體安全管理風險評估項目，包含：

1. 實體安全防護作業之安全，如評估是否將重要伺服器以安全周界保護，並給予適當之人員、設備進出管理措施，放置重要設備之區域應有防備意外災害之措施，並管制人員在內工作時之工作守則。

2. 資訊設備管理之安全，如評估是否提供足夠的安全保護，降低來自環境之威脅及危害造成的風險，以及未經授權存取之機會。

3. 基礎建設服務安全，如評估電源、水、空調等公用服務持續性是否足夠。

4. 訊息傳輸之安全，如評估資料傳送是否可能遭竊取或正確性受影響。

5. 人員管理之安全，如評估介接機關承辦人員之專業素養、教育訓練、存取權限管理等。

6. 介接機關之資料進階處理方式之法律適切性評估。

7. 資料儲存之安全性評估。

(四) 介接機關服務上線前之風險評估項目：

1. 資料傳輸前是否確認已可進行資料傳輸，並具備適法傳輸證明。

2. 資料需求機關取得資料後續運用與保存期限規範整備程度。

3. 資料介接機關因應資安法、資安責任等級應辦事項達成度。

4. 資訊系統分類分級及防護基準達成度。

5. 個資法施行細則安全維護要求。

6. 已進行之資訊安全及個人資料保護風險評估及風險處理方式。

7. 事前鑑別介接機關承辦人員、單位及制定管理要求。

8. 機關處理資料介接人員管理、存取權限方式。

9. 資料處理軌跡紀錄保存方法，包含內部人員存取紀錄。

(五) 介接機關服務上線後風險評估項目

1. 鑑別處理個資所涉之硬體、軟體、基礎建設、人員、資料，並進行風險評估，確認安全管理措施妥適。

2. 資料需求/提供機關資料保存期限/特定目的消失處理方式。

3. 資料處理違規嚴重性之評估，包含資料遭非授權存取、修改、滅失等。

4. 資料備份及業務營運持續。

5. 使用者於資料需求機關查詢/應用資料之具體作業程序。

6. 服務供應商管理及監督方法。

7. 資訊安全 ISO 27001、 BS 10012、ISO 27701 等外部驗證。

8. 認知訓練、內部稽核、缺失矯正、持續改善等要求。

貳、T-Road DPIA 風險評估參考標準

一、本案 T-Road DPIA 風險評估方法採用之國際標準說明

(一)APEC 隱私保護原則

1. APEC 電子商務指導小組(A PEC Electronic Commerce Steering Group)於 2003 年成立個人資料隱 私權保護分組(Data Privacy Sub-Group)，研擬制訂 APEC 隱私權保護原則(APEC Privacy Principles)以供亞太區域內之企業、消費大眾、法律協會以及保護隱私權的專家參考，APEC 隱私保護原則共有九項：

(1) 避免損害原則：有關個人資料之蒐集、處理與利用，不得損害當事人之權益。

(2) 告知原則：對個人資料進行蒐集時，應告知當事人 蒐集者名稱、蒐集資料之目的、種類與用途等必要 事項。

(3) 限制蒐集原則：個人資料的蒐集應符合蒐集之目的，且不得逾越必要之範圍，與目的無關之資料， 不得任意蒐集。

(4) 利用個人資料原則：有關個人資料之利用，應符合 當初進行蒐集之目的，未經當事人同意或另有法律 規定，該資料不得作其他利用。

(5) 當事人選擇原則：個人資料之蒐集或利用，當事人有權得選擇「進入」(opt-in)或「退出」(opt-out)模式，資料蒐集者或保有者應尊重當事人之選擇。

(6) 個人資料完整原則：保有個人資料檔案者，有責任隨時更新或補充資料，力求該資料之完整正確，避免當事人因不正確之資料，讓其權益遭受損害。

(7) 安全維護原則：保有資料者應採取必要之安全維護措施，避免個人資料被偷竊、遺失、毀損或外洩。

(8) 當事人查詢及更正原則：當事人隨時有權查詢或閱覽其個人資料，如發現有錯誤或欠缺者，得請求補充或更正。

(9) 責任原則：對於違法蒐集或利用個人資料者，應課以法律責任，以保護資料當事人之權益。

2. APEC 隱私保護原則評估方法

(1) 為將 APEC 隱私保護原則落實於本 DPIA 評估方法，故將 9 大原則與臺灣個人資料保護法(以下簡稱個資法)公務機關應辦事項進行對應：

■ 告知原則：個資法第 8 條、9 條。

■ 蒐集限制原則：個資法第 6 條、15 條。

■ 個資利用原則：個資法第 6 條、16 條。

■ 當事人自主原則：個資法第 3 條、11 條。

■ 查閱及更正原則：個資法第 10、11、13 條。

■ 完整性原則：個資法第 11 條。

■ 安全管理原則：個資法第 18 條、施行細則第 12 條。

■ 責任原則：個資法第 12 條、施行細則第 8 條。

(2) 由前述可見，APEC 隱私原則與臺灣個資法高度對應，故 APEC 隱私原則評估又可稱個資法適法性評估(以下簡稱適法性評估)，因介接 T-Road 進行個資交換運用，屬個資法第 16 條原蒐集目的以外之利用行為，需符合法定要件方可進行利用，故 T-Road 維運機關、資料需求機關、資料提供機關，若因 T-Road 而於原特定目的之外蒐集、處理或利用個人資料，均可以適法性評估確認個資法律遵循性。

3. ISO 29134 風險評估方法

(1) ISO 組織於 2017 年發展出隱私衝擊評鑑的國際標準「ISO 29134：隱私衝擊評鑑指引(Guidelines for privacy impact assessment)」，並受歐盟採納做為資料保護衝擊評鑑(DPIA)的方法，ISO 29134 所包含之管理要求，可直接做為對於國際隱私管理風險評估的合規展現。

(2) 本案 DPIA 方法，將採納 ISO 29134 做為 DPIA 評估方法之核心框架，ISO 29134 所要求之 DPIA 執行內容應包含如下之項目：

- 決定 DPIA 執行之時機、範圍(業務流程、系統等)、執行 DPIA 之單位/人員。
- 決定 DPIA 執行所依循之標準、風險接受準則，並確認對 DPIA 報告負責之人/單位。
- 識別可能涉及個資之處理及可能因處理個資而受影響之利害關係人。
- 規劃溝通計畫，使 DPIA 評估結果可對利害關係人進行溝通，溝通內容應包含對利害關係人可能面臨的隱私風險及處理方法，溝通的頻率和對象取決於可能受影響的嚴重性及個資當事人數量。
- 是否將溝通計畫尋求利害關係人之意見，做為對外溝通事項之參考。
- DPIA 應包含下列事項之描述：
  - 個資處理方法經上層機關或主管機關之核准結果。
  - 處理個資之目的。
  - 內部蒐集、處理或利用個資之方法。
  - 涉及個資處理之應用程式安全開發、獲取及維護方法。
  - 涉及個資處理之各單位，其內部相關負責人員執掌及描述。
  - 保留個資之期限及銷毀方法。
  - 若涉及個資處理委外，確保安全方法。
  - 若涉及個資跨境傳輸，個資傳輸之適法性確認結果。
- 定義整體個資作業流程所需之各類型使用紀錄(包含但不限於包含可鑑別各方使用者、管理者行為之 Log、資料庫稽核紀錄等)以及保存期限。

- 鑑別可能取得個資之使用者，或使用新興科技、數位設備可能帶來的隱私風險。
- 應包含整體作業流程中，所應符合要求之法令清單，如臺灣個人資料保護法、資安法等及其他應遵循之特別法等。
- DPIA 應包含取得資料後之未來應用，包含資訊系統或流程可能帶來的額外風險進行評估。
- DPIA 應鑑別可能發生風險之個資及相關資訊資產之漏洞和隱私風險的處理方法，風險分析過中應充份紀錄風險及處理方法。
- DPIA 風險處理決策應考慮利益相關者的風險承受能力，包括個資當事人、組織等，且應參考法令法規和其他要求做出風險處理之方法、優先順序等。
- DPIA 應包含影響程度與發生之可能性，並確認處理風險的方法和選項。
- 應列出風險處理措施的處理選項列表，並制定風險處理計畫。

(3) DPIA 風險處理計畫應包含：

- 風險處理方式。
- 負責執行單位/人員。
- 所需資源。
- 完成期間。
- 如何評估風險處理結果。
- 與利害關係人溝通風險處理結果。
- 風險擁有者批准隱私處裡計畫，並接受剩餘風險，透過正式簽屬流程承接管理責任。
- 確認 DPIA 結果應對外公開部分。
- 遵循隱私風險處理計畫所列示之處理措施。
- 確認 DPIA 報告是否需經第三方審查。

(4) 經確認T-Road所涉及之個資蒐集、處理或利用之各單位，若需進行風險評估， 相關 DPIA 方法除應依循前述要求採納 ISO 29134 做為 DPIA 評估方法之核心框架外，亦應將辦理方式文件化。

二、應執行 DPIA 之單位及依法應辦事項

(一)應執行 DPIA 之單位

1. T-Road運作過程中，包含T-Road維運機關、資料中心建置機關、介接接關，均應針對 T-Road相關資通系統安全防護妥適程度進行評估。
2. T-Road 運作功能範圍內之各項資通系統，應由權責管理機關依資通安全責任等級分級辦法之規定，進行資通系統防護需求分級，並依資通系統防護基準執行控制措施。
3. 依個人資料保護法第 2 條之定義，若涉及如下所示之個資相關行為，應進行適法性評估：
   (1) 蒐集：指以任何方式取得個人資料。
   (2) 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
   (3) 利用：指將蒐集之個人資料為處理以外之使用。
4. 於 T-Road運作功能範圍內，若介接機關符合個資法第 2 條定義蒐集、處理或行為，自應符合個資法令各項要求，且執行 DPIA。

(二)T-Road 維運機關應辦事項

1. T-Road 應符合個資法要求(適法性評估)。
2. T-Road 應確認是否符合國內資安法、個資法對資通系統委外安全要求：
   (1) 資安法對資通系統委外辦理之要求：
      ■ 受託者是否具備完善之資通安全管理措施或通過第三方驗證。

- 受託者是否配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業開發人員。
- 受託者是否得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。
- 確認受託業務是否涉及國家機密，若有則執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。
- 受託業務包括客製化資通系統開發故受託者應提供該資通系統之安全性檢測證明，T-Road 維運機關應自行或另行委託第三方進行安全性檢測。
- 若非受託者使用自行開發之系統或資源者，並應標示自行開發之內容與其來源及提供授權證明。
- 應要求受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，立即通知委託機關及採行之補救措施。
- 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。
- 明定受託者應採取之其他資通安全相關維護措施。
- 委託機關應明定受託者配合稽核或其他適當方式確認受託業務之執行情形之方式。
- 若受託業務所涉及國家機密，應視機密等級及內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核：
  - 是否曾犯洩密罪、或通緝有案尚未結案。
  - 曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。
  - 曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

(2) 確認個資法針對業務委外之要求是否已滿足：

■ 明文說明受委託蒐集、處理或利用個人資料，於本法適用範圍內，視同委託機關。

■ 監督受託者辦理下列事項：

- 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
- 若有複委託者，約定之受託者。
- 明文約束受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
- 委託機關如對受託者有保留指示者，其保留指示之事項。
- 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。
- 各項監督應定期確認受託者執行之狀況，並將確認結果記錄之。
- 約定受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。
- 受託者應有配置個資管理之人員及相當資源。
- 事先界定受託處理個人資料之範圍。
- 事先制定個人資料之風險評估及管理機制。
- 事先制定事故之預防、通報及應變機制。
- 事先制定個人資料蒐集、處理及利用之內部管理程序。
- 事先制定資料安全管理及人員管理。
- 事先制定認知宣導及教育訓練。
- 事先制定設備安全管理。
- 事先制定資料安全稽核機制。

- 事先制定使用紀錄、軌跡資料及證據保存。
- 事先制定個人資料安全維護之整體持續改善。

3. T-Road 運作期間，維運機關應符合國內資通安全管理法之各項要求，如針對資通系統安全防護需求進行分級，並依照分級結果落實資通系統防護基準。
4. T-Road 運作期間，若維運機關保有個人資料，應符合個資法之應辦事項及安全維護要求。
5. T-Road之運作包含資料傳輸安全監控，建立T-Road之傳輸系統、網路、系統發展與維護等事項，為確保T-Road整體系統傳輸通道之穩定、可靠與安全，故T-Road整體功能應至少包含下列要求，且需納入評估項目：
   (1) T-Road 應具安全傳輸方法。
   (2) 事前應有審核機制，確認各機關之安控機制與適法性程序。
   (3) 應事前審核資料提供機關之服務清單，並正確的發布。
   (4) 資料傳輸各方之訊息紀錄(Message Log)與稽核紀錄(Audit Log)應能妥善保存，供追蹤軌跡及查證。
   (5) T-Road 整體系統與網路效能應有監控與回應功能。
   (6) T-Road 應有作業系統漏洞修補及更新通知方法。
   (7) T-Road 應有系統程式版本控管及安全派送機制，確保派送過程未經竄改。
   (8) T-Road 應有標準組態安全更新方法，包括作業系統版本、套件版本及相關組態設定等。
   (9) T-Road 應有專屬資料傳輸網段，控管網域及核發 IP 位址。
   (10) T-Road 應有安全傳輸協定及機制。
   (11) 對 T-Road 介接機關之稽核權力。

(三)設置資料中心機關應辦事項

1. 設置資料中心之機關，應符合國內資通安全管理法之各項要求，如針對介接 T-Road 部分之資通系統安全防護需求進行分級，並依照分級結果落實資通系統防護基準。
2. 若資料中心保有個人資料，應符合個資法之應辦事項及安全維護要求(適法性評估)。
3. 負責集中網路出口及 T-Road 傳輸資安監控。
4. 負責介接 T-Road 之各項硬體環境之管理及維護。
5. 當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，避免惡意程式蔓延至其他機關，並追查惡意程式來源及通知 T-Road 管理平臺、來源機關（單位）。
6. 如發生資安事件時，應儘速通知 T-Road，並採取必要之因應控管措施。

(四)T-Road 介接機關應辦事項

1. 介接 T-Road 期間，應符合國內資通安全管理法之各項要求，如針對介接 T-Road 部分之資通系統安全防護需求進行分級，並依照分級結果落實資通系統防護基準。
2. T-Road 運作期間，介接機關應符合個資法之應辦事項及安全維護要求(適法性評估)。
3. 負責管理介接 T-Road 之安控伺服器作業系統以及軟體環境，確保該伺服器服務可用性並提供服務。
4. 配合 T-Road 發布之安控伺服器作業系統更新。
5. 於安控伺服器安裝防毒軟體並定期更新病毒碼，對於傳送或接收之資料、附檔需進行掃描，偵測有無感染電腦病毒。
6. 資料提供機關需對資料需求機關提出之服務請求進行審核，並於同意後設定適當權限給資料需求機關。
7. 視需要稽核資料需求機關。

三、T-Road DPIA 評估時機

(一)T-Road 系統功能開發階段

1. 整體 T-Road 系統開發階段，T-Road 維運機關應符合資安法所要求之資通系統委外要求，針對開發團隊進行安全管理。
2. 針對 T-Road 未來各項系統功能，應進行事先評估，確保未來系統上線後，能符合資安法、個資法、各項已鑑別之法令要求、資安國際管理標準要求，故應事先進行評估。

(二)T-Road 系統功能大幅度變動

1. 若 T-Road 系統功能大幅度異動，為確保功能異動後仍符合資安法、個資法之要求，應重新進行評估。
2. 若 T-Road 異動委託外部辦理，應令符合資通系統委外要求，針對開發團隊進行安全管理。

(三)介接機關提供資料傳輸前

1. 資料提供機關於提供資料前，應事前針對資料提供之適法性進行研究，確認資料提供之範圍、特定目的、資料使用機關之未來運用方法後，方可提供。
2. 應事先針對資料需求機關之資料需求進行彙整，確認資料蒐集後不會對當事人產生額外風險或影響當事人權利。
3. 資料提供機關應於提供資料前，針對個資提供外部機關利用，進行完整評估，後續資料提供範圍異動亦同。
4. 資料提供機關經過審核，開始透過 T-Road 傳輸資料前，資料需求機關應事先確認取得資料後之利用方式，不會對當事人產生額外風險或影響當事人權利。
5. 事先規劃各項安全防護措施，針對取得外部機關提供之個資(個資蒐集、處理)，進行完整評估及安全控管，後續資料蒐集、處理範圍異動亦同。

(四)定期或不定期進行評估

1. 每年定期針對介接 T-Road 部分相關安全防護措施，進行資料保護安全評估。

2. 收到外界通報最新資安或個資風險情資後進行評估。

四、風險處理方式

依目前國際標準常見風險處理方法，分為下列 4 種：

(一)規避風險：消極躲避風險。

(二)預防風險：採取措施消除或者減少風險發生的因素。例如為了防止資料侵害，採取加密、資料遮蔽等措施，可減少因資料外洩導致的損失。

(三)接受風險：確認風險胃納後承擔風險。

(四)轉移風險：在風險發生前，通過採取出售、轉讓、保險等方法，將風險轉移。

五、風險發生機率評估方式

依目前國際標準常見評估風險發生機率之方法，分為下列 3 種：

(一)風險時常發生，或幾乎確定會發生：指參考機關內、外部稽核發現、控管措施嚴謹度，依評估者辦理業務之經驗，認為風險事件過去時常發生，預測未來發生機率相當高。

(二)風險偶而發生，發生機率中等：指參考機關內、外部稽核發現、控管措施嚴謹度，依評估者辦理業務之經驗，認為風險事件過去發生過，但並非時常發生。

(三)風險甚少發生：指參考機關內、外部稽核發現、控管措施嚴謹度，依評估者辦理業務之經驗，認為風險事件過去沒發生過，在認為該項風險甚少發生。

六、風險發生嚴重性評估方式

(一)非常嚴重：指經評估者針對風險評估標的之機密性(如資料非授權揭露)、完整性(如資料錯誤或遭竄改)、可用性(如系統中斷)或法律遵循性(如風險事件影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任)發生侵害後，對機關之營運、資料、信譽、資產，發生非常嚴重、災難性、難以回復之影響。

(二)嚴重影響：指經評估者針對風險評估標的之機密性(如資料非授權揭露)、完整性(如資料錯誤或遭竄改)、可用性(如系統中斷)或法律遵循性(如風險事件影響他人合法權益或機關執行業務之公正性及正當 性，並使機關所屬人員負刑事責任)發生侵害後，對機關之營運、資料、信譽、資產，發生嚴重之影響。

(三)有限影響：指經評估者針對風險評估標的之機密性(如資料非授權揭露)、完整性(如資料錯誤或遭竄改)、可用性(如系統中斷)或法律遵循性(如風險事件影響他人合法權益或機關執行業務之公正性及正當 性，並使機關所屬人員負刑事責任)發生侵害後，對機關之營運、資料、信譽、資產，發生有限、可回復之影響。

(四)經評估風險事件發生之可能性及嚴重程度後，應以風險地圖方式，描繪機關風險分布，並規劃風險處理計畫，風險地圖下表所示：

T-Road DPIA 風險地圖			
可能性 嚴重程度	甚少發生(低)	偶而發生(中)	時常發生(高)
非常嚴重(高)	中度風險，管理階層需定期關注相關風險，且需以風險處理計畫進行風險降低措施。	高度風險，管理階層需立即督導風險處理計畫並提供適當資源，直至風險下降為止。	高度風險，管理階層需立即督導風險處理計畫並提供適當資源，直至風險下降為止。
嚴重(中)	低度風險，持續依現有管理制度監控。(接受風險)	中度風險，管理階層需定期關注相關風險，且需以風險處理計畫進行風險降低措施。	高度風險，管理階層需立即督導風險處理計畫並提供適當資源，直至風險下降為止。

T-Road DPIA 風險地圖			
有限(低)	低度風險，持續依現有管理制度監控(接受風險)。	低度風險，持續依現有管理制度監控(接受風險)。	中度風險，管理階層需定期關注相關風險，且需以風險處理計畫進行風險降低措施。

參、T-Road 風險評估方法說明

一、T-Road 個資法適法性評估方法

(一)評估方法說明

1. 個資法適法性評估，對照 APEC 九大原則如下，除預防損害原則為涵蓋整部個資法，故列為通用性上位原則外，其於原則評估方式如下表，因介接、維運 T-Road 之各單位若保有個人資料，均應以此表進行個資法適法性評估：

APEC 隱私原則	評估項目
1 告知原則	機關向當事人蒐集個人資料時，除個資法第八條第二款情形之一者外，是否明確告知當事人下列事項？ 一、機關名稱。 二、蒐集之目的。 三、個人資料之類別。 四、個人資料利用之期間、地區、對象及方式。 五、當事人依第三條規定得行使之權利及方式。 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。
	機關蒐集非由當事人提供之個人資料，除個資法第九條第二款情形之一者外，是否於處理或（首次）利用前，向當事人告知個人資料來源及個資法第八條第一項第一款至第五款所列事項？
2 蒐集限制原則	機關是否已規範，除個資法第六條第一項各款所列情形之一外，不得蒐集、處理或利用病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料？

APEC 隱私原則	評估項目
	機關對個人資料之蒐集或處理，除個資法第六條第一項所規定資料外，是否有特定目的，並符合個資法第十五條第一項各款情形之一者（須備註符合之情形）？
3 個人資料利用原則	機關對個人資料之利用，除個資法第六條第一項所規定資料及個資法第十六條第一項各款情形之一者外，是否於於執行法定職務必要範圍內為之，並與蒐集之特定目的相符？
	機關是否已規範對個人資料特定目的外之利用，需符合下列各款情形之一者？ 一、法律明文規定。 二、為維護國家安全或增進公共利益。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。 六、有利於當事人權益。 七、經當事人同意。
4 當事人自主原則	機關是否已規範接受當事人權利行使程序，且應保護該權利，不得要求當事人預先拋棄或以特約限制之。
	機關是否已規範如個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用？(但因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限)
	機關是否已規範當個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料？(但因執行職務或業務所必須或經當事人書面同意者，不在此限)
	機關是否已規範違反個資法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料？
5 查閱及更正原則	機關是否除個資法第十條各款除外情形之一者外，已規範依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本？

APEC 隱私原則	評估項目
	機關是否已規範，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象？
	機關是否已規範受理當事人依個資法第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人？
	機關是否已規範受理當事人依個資法第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人？
6 個人資料完整性原則	機關是否已規範維護個人資料之正確，並應主動或依當事人之請求更正或補充之？
7 安全管理原則	機關保有個人資料檔案者，是否已應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏？
	機關是否已規範保有個人資料檔案者，應指定具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員並接受相關專業之教育訓練，辦理個資法施行細則第十二條第二項之十一款安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏？
8 責任原則	機關是否已規範違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，查明後以適當方式通知當事人？
	機關是否已規範，委託他人蒐集、處理或利用個人資料時，對受託者之監督事項至少包含個資法施行細則第八條所規定之事項？
	機關是否已規範，違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人？

2. 前述個資法適法性評估後之結果，應交由組織高階管理階層檢視，若有不符合之處應納入風險處理計畫改善。

(二)各介接機關應於傳輸資料前，事先確認個資蒐集、處理或利用之適法性，確認方可申請介接。

(三)個資法適法性評估風險處理方法

1. 個資法適法性評估結果，因均屬法令強制規定，除未實際蒐集、處理個人資料，產生不適用外之不符合情形，應強制改善。

2. 改善措施施行後，應再次進行評估，確認均已獲得改善。

二、保有之個資重要性評估方法

(一)經鑑別因介接、維運 T-Road 而保有個人資料之單位，應針對保有之個人資料，進行重要性評估，若評估結果為高重要性，應強化組織保護資料之強度。

保有個資重要性評估項目	說明
可識別性	評估之資料識別到特定個人之容易程度，如身分證字號、姓名、電話區碼、log 的保留資訊等。
個資數量	評估之個人資料之數量，可以旺季或淡季方式進行區間識別。
資料欄位敏感程度	如個人的身分證字號、銀行帳號碼、存取網頁內容，如可識別的當事人搜尋「藥物濫用」，組織也須評估結合使用個資欄位的敏感性。
使用情境(蒐集、儲存、使用、處理、公開、傳輸 PII 之目的)	(1) 如公布個人姓名及聯絡方式對個人造成之危害。 (2) 如組織保留之 Log 紀錄。 (3) 如將個資提交給特定單位(如舞弊、濫用等，製作黑名單)。
存取個資位置	(1) 如資訊可以任意被存取。 (2) 如個資易透過遠距使用。 (3) 僅有少數人能夠存取 DB，並僅能透過組織內部系統存取該 DB。
損害當事人信譽	資料若發生侵害，對個人的影響程度。
損害組織信譽	資料若發生侵害，對組織的傷害嚴重程度。

(二)前述保有個資重要性評估方法，評估結果應能與後續資料保護重要性評估方法介接，確認組織保護資料之強度已足夠。

三、委外開發 T-Road 安全評估方法

(一)維運 T-Road 單位若由外部單位進行 T-Road 各項功能之開發，應有委外安全評估方法，相關評估項目如下所示：

項次	評估項目	評估內容
1	專案管理資訊安全	組織是否將以確保將識別並處理資訊安全風險管理作為委外專案管理之一部份，如在專案的早期階段實施資訊安全風險評鑑以識別必要的控制措施，並定期審查委外專案資訊安全之符合性，並界定委外專案內對特定角色界定予配置資訊安全責任。
2	人員管理安全	組織是否針對所有可能被委託聘用者所進行基本背景調查，依相關法律、法規，並應相稱於營運要求及其將存取之資訊的保密等級及組織所察覺之風險，確認是否聘用。
3	人員管理安全	組織是否針對委外承包者簽訂契約化協議書，敘明雙方對資訊安全的責任。
4	人員管理安全	(1) 組織是否要求所有承包者，遵守組織之資安規範，並應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。 (2) 組織是否對委外承包者定義且傳達於聘用終止或變更後，資訊安全責任及義務仍保持有效，並落實執行。
5	系統獲取、開發及維護	開發過程中的安全要求，應納入新系統開發過程要求，如： (1) 對使用者宣稱身分之信賴等級要求， 以便導出使用者鑑別之要求。 (2) 存取權限提供及授權過程， 營運使用者以及特權或技術使用者。 (3) 告知使用者及操作者其職責及責任。 (4) 涉及資產所需的保護需要， 特別是關於可用性、機密性、完整性者。 (5) 來自營運過程之要求， 如交易紀錄及監視、不可否

項次	評估項目	評估內容
		認性要求。 (6) 其他安全控制措施規定之要求，例如紀錄(Log)及監視之介面或資料洩露偵測系統。 (7) 網路傳輸安全協議。 (8) 外部購買之產品，應針對是否涉及使用危害國家資通安全產品情形。 (9) 評估及實作該系統最終軟體/服務堆疊之產品安全組態調校的可用指引。 (10) 界定接受產品之準則，例如在功能性方面，給予保證達到已識別之安全。
6	軟體開發過程安全	組織是否界定軟體開發規則包含： (1) 開發環境之安全。 (2) 軟體開發安全、程式語言安全編碼原則。 (3) 軟體開發方法之安全。 (4) 所用每一程式語言之安全編碼指導綱要。 (5) 設計階段內安全要求。 (6) 計畫期程內之安全查核點。 (7) 保全資料庫。 (8) 版本控制之安全。 (9) 必要之應用系統安全知識。 (10) 開發者避開、找出及修補脆弱性之能力。
7	系統變更管理	組織是否議定安全變更要求，如： (1) 維持所議定之變更授權等級的紀錄。 (2) 確保變更是由經授權的使用者提出。 (3) 審查控制措施與完整性程序，以確保其未被變更所破壞。 (4) 識別所有需要改善的軟體、資訊、資料庫個體及硬體。 (5) 識別及查核安全關鍵程式碼以將已知安全弱點可能性降至最小。 (6) 在變更工作開始前，應有詳細的提案，且獲得正式核准。

項次	評估項目	評估內容
		(7) 變更實作之前，經授權的使用者應接受該變更。 (8) 確保在每次完成變更後，就更新系統文件組，並將舊文件歸檔或作廢。 (9) 維持所有軟體更新作業的版本控制。 (10)維持所有變更請求的稽核日誌。 (11)確保作業文件與使用者程序根據需要作適切變更。 (12)確保在正確的時機實作變更，且不會擾亂所涉及的營運過程。
8	開發環境保全	組織應針對系統委外開發之環境，進行安全控管，包含： (1) 系統處理、儲存及傳輸之資料的敏感性。 (2) 適用之外部及內部要求事項，如來自法規或政策。 (3) 支援系統發展組織已實作之安全控制措施。 (4) 環境內工作人員之可信賴性。 (5) 與系統發展有關之外包程度。 (6) 不同發展環境間區隔之需要。 (7) 對發展環境存取之控制措施。 (8) 對環境及存於其中程式碼變更之監視。 (9) 備份儲存於保全之異地位置。 (10)環境中資訊搬遷進入及移出之控制措施。
9	軟體委外開發監督	針對軟體委外開發業務，應有進行下列安全要求： (1) 版權使用、程式碼所有權及智慧財產權 (2) 安全設計、程式編碼及測試實務之契約要求。 (3) 對開發者提供已發現之軟體威脅。 (4) 交付產品之品質及精確性的驗收測試。 (5) 可接受安全及隱私權品質。 (6) 提供已應用足夠測試以避免交付時包含惡意內容的證據。 (7) 提供已應用足夠測試以防衛免於出現已知脆弱性的證據。 (8) 如原程式碼不再可用時之協議。 (9) 稽核開發過程及控制措施之契約權利。 (10)用以產生交付產品之編譯環境的有效文件。

項次	評估項目	評估內容
		(11)負責適用法律之遵循及控制措施效率之查證證據。
10	系統驗收	組織針對系統驗收測試應包括資訊安全要求之測試， 並嚴守保全系統開發實務。如利用諸如程式碼分析工具或弱點掃瞄系統等自動化工具， 並查證有關安全缺陷的修補。
11	測試資料保護	組織應針測試應用系統進行安全規劃： (1) 適用於運作之應用系統的存取控制程序亦宜適用於測試應用系統。 (2) 每次複製作業之資訊到測試環境均宜經過個別授權。 (3) 在測試完成後宜立即將作業之資訊從測試環境中清除。 (4) 宜保存開發作業資訊的複製與使用，以便提供稽核日誌。
12	供應者安全要求	組織應針對服務供應者可取得之資訊資產進行保護，如： (1) 識別及文件化組織將允許委外供應者存取之資訊型式，例如IT 服務、後勤、公用設施、財務服務、IT 基礎建設組件等。 (2) 管理供應者關係之標準化過程及生命週期。 (3) 界定不同供應者將被允許之資訊存取型式， 並監視及控制其存取。 (4) 每一資訊型式及存取型式之最低資訊安全要求， 以作為基於組織營運需求及要求以及其風險剖繪與個別供應者協議之基礎。 (5) 對每一供應者型式及存取型式監視嚴守已建立資訊安全要求的過程及程序，包括第三方審查及產品驗證。 (6) 準確度及完全性控制措施以確保資訊或各方提供資訊處理之完整性。 (7) 適用於供應者之義務型式以保護組織資訊。 (8) 與供應者存取有關的處置事故及應變，包括組織與供應者雙方之責任。

項次	評估項目	評估內容
		(9) 必要時之回復及應變安排，以確保資訊或各方提供資訊處理之可用性 (10)涉及獲取的組織人員關於適用政策、過程及程序之認知訓練。 (11)與供應者人員互動的組織人員關於基於供應者型式及供應者存取組織系統 (12)資訊安全要求及控制措施之情況將由雙方簽署一書面協議。 (13)管理必要之資訊、資訊處理設施及其他任何需要移動之物品的傳送， 並確保整段傳送期間之資訊安全。
13	委外供應者安全協議	組織應針對委外供應者進行相關安全協議要求： (1) 存取資訊方法描述。 (2) 依據組織分級方案的資訊分類與分級，對映組織本身資訊存取分級方案與供應者分級方案。 (3) 鑑別法律及法規要求， 包括資料保護、智慧財產權及版權，以及將如何確保落實。 (4) 每一契約方實作協議的包括存取控制、績效審查、監視、通報及稽核等整套控制措施之義務。 (5) 資訊可接受之使用的規定，必要時包括不可接受之使用。 (6) 明確的授權存取或接收組織資訊之供應者人員清單，或是供應者人員存取或接收組織資訊的授權以及移除授權之程序或情形。 (7) 與特定契約有關之資訊安全政策。 (8) 事故管理要求及程序（特別是事故修補期間之通知及合作）。 (9) 特定程序及資訊安全要求之訓練及認知要求， 例如事故回應、授權程序。 (10)分包之相關法規，包括需要實作之控制措施。 (11)相關協議夥伴，包括資訊安全議題之聯絡窗口。 (12)如有篩選要求，若篩選未完成或其結果導致懷疑或關切時，包括執行篩選及通知程序之供應者人員的

項次	評估項目	評估內容
		責任。 (13)缺陷解決及衝突解決過程。 (14)供應者定期交付控制措施有效性的獨立報告之義務，與即時修正報告內所提出相關議題之協議。 (15)供應者遵循組織安全要求之義務。
14	供應鏈安全要求	組織應針對資通訊服務及產品供應鏈，進行安全管理： (1) 除一般供應者關係資訊安全要求以外，界定適用於資訊及通訊技術產品或服務之獲取的資訊安全要求。 (2) 對資訊及通訊技術服務，若供應者分包部份提供給組織的資訊及通訊技術服務，則要求供應者對整個供應鏈傳播組織之安全要求。 (3) 對資訊及通訊技術產品，若上述產品包括採購自其他供應者之組件，則要求供應者對整個供應鏈傳播適切的安全實務。 (4) 實作監視過程及可接受之方法，以驗證交付之資訊及通訊技術產品及服務 (5) 嚴守指定的安全要求。 (6) 實作識別維護功能性重要的產品或服務組件，因此在組織外部建立時需要增加注意及安全性，特別是若最高層供應者將產品或服務組件層面委外至其他供應者。 (7) 取得關鍵組件及其起源在整個供應鏈可被追溯的保證。 (8) 取得交付之資訊及通訊技術產品如預期運作，無任何非預期或非所欲特徵的保證。 (9) 界定組織及與供應者間關於供應鏈與任何潛在議題及危害等資訊共享之規則。 (10)實作資訊及通訊技術組件生命週期及可用性與相關安全風險的特定管理過程。包括管理組件由於供應者不再營運而不再可用，或供應者由於技術進展而不再提供上述組件等之風險。
15	交付管理	組織應有文件化程序，針對交付項目進行管控：

項次	評估項目	評估內容
		(1) 組織應監視服務效能等級以查核委外協議的遵守程度。 (2) 按協議要求審查供應者產出的服務報告，並安排定期的進度會議。 (3) 實施供應者的稽核，若可取得，同時審查獨立稽核報告，以及發現問題之後續行動。 (4) 按協議與任何支援指導綱要與程序之要求，提供關於資訊安全事故的資訊，並審查該資訊。 (5) 審查與所交付服務相關的安全事件、運作之問題、失效、失誤追蹤及中斷等的第三方稽核日誌與紀錄。 (6) 解決並管理所有已識別出的問題。 (7) 審查供應者與其本身供應者關係之資訊安全層面。 (8) 確保供應者維持足夠的服務容量以及設計可行之計畫，確保重大服務失效或災害之後能維持議定之服務持續等級。
16	資安事故管理	組織是否要求所有委外承包者，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。

(二)上表各項安全評估項目，若發現不符合之處，應在專案進行階段交付之前進行改正。

四、T-Road 維運機關資通安全管理措施評估方法

(一)維運機關開發 T-Road 政府骨幹網路資料傳輸，亦應符合國內資安法之要求，資通系統之應辦事項如下：

1. 管理面

(1) 滿足資通安全責任等級 A 級之公務機關應辦事項，包含進行資通系統分級及防護基準確認。

(2) 核心系統通過第三方驗證。

(3) 若 T-Road 屬於核心資通系統，每年應辦理 2 次內部資安稽核，應先安排執行時間。

(4) 若 T-Road 屬於核心資通系統，每年應辦理 1 次營運持續演練，應先安排執行時間。

(5) 限制使用危害國家資通安全產品。

2. 技術面：

(1) 若 T-Road 屬於核心資通系統，每年應辦理 2 次網站安全弱點檢測。

(2) 若 T-Road 屬於核心資通系統，每年應辦理 1 次系統滲透測試。

(3) 每年應辦理 1 次資通安全健診。

(4) 1 年內完成資通安全威脅監測管理導入。

(5) 1 年內完成政府組態基準導入。

(6) 1 年內完成資通安全防護導入。

(二)維運機關應針對 T-Road 欲達成之功能，進行功能面安全評估，評估方式如下所示：

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
1	機關資安責任等級應辦事項	T-Road 維運機關未符合機關資安責任等級 A 級之應辦事項，恐有資安風險。	N/A	N/A
2	資通系統防護需求及防護基準	各機關自行或委外開發之資通系統未依法進行資通系統防護需求分級，或未依資通系統防護基準執行控制措施。	N/A	N/A
3	系統組態設定與安控伺服器註冊管理	(1) 於系統需求訪談階段，未識別資料輸出入之機敏性，造成不當存取的風險 (2) 未檢核資料輸入正確性，導致資料庫異常或遭惡意注入之風險。 (3) 使用或未定時更新已知存有漏洞風險之函式庫，導致系統遭惡意入侵，遭植入惡意	A.14 系統取得、開發及維護	6.11 系統獲取、開發和維護

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
		程式進行資料竊取或影響系統服務。 (4) 未加密或遮罩敏感資料，致使機敏資料遭不當冒用之風險。 (5) 未遵循政府組態基準設定相關安全參數，致使伺服器組態不一致或植入惡意程式之風險。 (6) 防火牆政策未以最小化設定為原則管理，可能存有惡意連線存取、已開啟之服務遭利用之風險。 (7) 未即時更新即將過期之憑證，致使網站未被信任或可能遭冒用之風險。 (8) 未設有系統校時機制，致使系統軌跡留存時間錯置、可能接受過期憑證，或是讓許多必須檢驗時間的訊息傳輸無法進行。 (9) 未設有系統異常自動告警機制，致使系統服務異常無法於可容忍中斷時間內回復，或於系統備份失敗時無法即時排除。 (10) 未確實評估系統服務所需之記憶體大小，致使系統可用性不足，造成服務異常。 (11) 未正確註冊、變更或註銷安控伺服器之來源目的端，致		

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
		使未經授權資料遭盜用、偽冒或惡意利用之風險。		
2	安控伺服器組態的下載服務及更新服務。 (一)組態設定管理 (二)下載組態設定	(1) 未遵循政府組態基準設定相關安全參數，致使伺服器組態不一致或植入惡意程式之風險。 (2) 未落實安控伺服器於資料傳輸時之憑證有效性檢核，致使未經授權之傳輸，或遭中間人偽冒攻擊之風險。 (3) 未確實評估系統服務所需之記憶體大小，致使系統可用性不足，造成服務異常。	A.14 系統取得、開發及維護	6.11 系統獲取、開發和維護
3	紀錄、蒐集、彙整各安控伺服器及管理平臺的操作紀錄，並保存查調紀錄的相關 Log (一)監控提供服務 API (二)使用者操作紀錄限，並自動備份 (三)異常告警功能 (四)查詢異常紀錄功能可查詢用戶端操作異常紀錄	(1)未自動備份 API 使用軌跡，致使資料傳輸出錯時，無法有效查找問題。 (2)未確實留存使用者操作軌跡，致使資料外洩、錯誤或發生異常時，無法有效釐清責任歸屬。 (3)未設有系統異常自動告警機制，致使系統服務異常無法於可容忍中斷時間內回復，或於系統備份失敗時無法即時排除。 (4)未確實評估系統服務所需之記憶體大小，致使系統可用性不足，造成服務異常。 (5)未正確設定系統異常告警通知人員，導致於系統出錯時無法快速排除或應通報而未通報負責人員。	A.14 系統取得、開發及維護	6.11 系統獲取、開發和維護

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
4	監控環境功能	(1)未設有系統異常自動告警機制，致使系統服務異常無法於可容忍中斷時間內回復，或於系統備份失敗時無法即時排除。 (2)未確實評估系統服務所需之記憶體大小，致使系統可用性不足，造成服務異常。 (3)未正確設定系統異常告警通知人員，導致於系統出錯時無法快速排除或應通報而未通報負責人員。	A.14 系統取得、開發及維護	6.11 系統獲取、開發和維護
5	安控伺服器(Security Server 功能	(1)未定期檢視各機關安控伺服器之作業環境作業系統版本、套件版本及相關組態設定，致使已知漏洞遭利用之風險。 (2)未使安控伺服器透過防火牆或其他安全設施管控與其他主機間之資料傳輸及資源存取，造成未經授權之存取風險。 (3)未使用較高強度之加密措施進行傳輸加密，導致已知弱加密遭破解，造成資料外洩之風險。 (4)未定期執行安控伺服器主機作業系統之更新，致使已知漏洞遭利用之風險，導致資料不當外洩。	A.14 系統取得、開發及維護	6.11 系統獲取、開發和維護

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
6	Log 查調紀錄保存五年	(1)未確實評估系統服務所需之記憶體、磁碟大小，致使系統可用性不足，造成服務異常。 (2)未設有系統校時機制，致使系統軌跡留存時間錯置、可能接受過期憑證，或是讓許多必須檢驗時間的訊息傳輸無法進行。 (3)未設定僅有權限之人員能夠存取訊息記錄及稽核紀錄，導致人員不當刪除、外洩其機敏存取軌跡。 (4)未定期備份安控伺服器之訊息紀錄及稽核紀錄，致使問題查找、責任歸屬無法釐清。	A.12.4.1 事件存錄	6.9.7 資訊系統稽核考量
7	核定資料中心設置機關申請介接	未依照「行政院資通安全責任等級分級辦法」之A級公務機關應辦要求，定期執行程式碼弱點掃描、系統弱點掃描、滲透測試等弱點管理之要求，致使系統已知漏洞遭不當嘗試利用之風險。	5.3 組織角色、責任及權限	5.2.1 瞭解組織及其全景
8	T-Road 傳輸系統之規劃與開發設計及傳輸資料加密等安全性評估與考量	(1) 於系統需求階段是否已針對系統安全需求(含機密性、完整性、可用性)進行確認 (2) 於系統需求訪談階段，未識別資料輸出入之機敏性，造成不當存取的風險 (3) 未檢核資料輸入正確性，導致資料庫異常或遭惡意注入之風險	A.14 系統取得、開發及維護	6.11 系統獲取、開發和維護

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
		(4) T-Road 傳輸未使用較高強度之加密措施進行傳輸加密，導致已知弱加密遭破解，造成資料外洩之風險。 (5) 於系統設計階段，未依據系統功能與要求識別可能影響系統之威脅，進行風險分析及評估，造成系統有遭不當破解之風險。		
9	定期審視作業系統漏洞修補訊息，評估作業系統變更對T-Road傳輸系統運作及安全產生之影響，並依據評估及測試結果，對系統做必要調整，並對各安控伺服器安裝機關發布作業系統漏洞修補更新通知。	未定時追蹤作業系統之漏洞修補測試，或未更更新已知漏洞風險之作業系統、軟體、元件，致使不當存取之風險。	A.12.6.1 技術脆弱性管理	6.13.1.3 通報資訊安全弱點
10	建立 T-Road 傳輸系統程式版本控管及安全派送機制，對所派送之版本應予以憑證簽章，確保派送過程未經竄改	(1) 未落實系統程式版控，且未區分版本控制人員之存取權限，導致程式碼遭惡意盜用之風險。 (2) 未遵循程式更新安全派送機制，導致系統更新失敗，部分系統無法使用。 (3) 未對程式碼執行完整性及不可竄改之確認。	A.9.4.5 對程式源碼之存取控制	6.11.2.2 系統變更控制程序
11	對各機關安控伺服器之作業環境建立標準組態列表，包括作業系統版本、套件版本及相關組	未建立安控伺服器之作業環境組態標準，致使各安控伺服器作業環境設定不一，導致傳輸錯誤、服務失效或未更新之組態遭已知漏洞攻擊之風險。	A.12 運作安全	6.11.2.4 軟體套件變更之限制

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
	態設定等作為系統安全維護設定之準則。			
12	訂定 T-Road 資料傳輸網段，接受資料中心設置機關申請安控伺服器網域及核發 IP 位址。	未正確區隔 T-Road 與其他服務之網段區隔，致使未經授權之機關或其他連線來源端不當存取之風險。	A.9.1.2 對網路及網路服務之存取	6.11.1.2 保護公共網路之應用服務
13	訂定本平臺安全傳輸協定及機制，確保資料傳遞過程均進行通道加密及驗簽，防止未經授權之機關或外界連接本平臺。	(1) T-Road 傳輸未使用較高強度之加密措施進行傳輸加密，導致已知弱加密遭破解，造成資料外洩之風險。 (2) 未加密或遮罩敏感資料，致使機敏資料遭不當冒用之風險。	A.14.1.3 保護應用服務交易	6.11.1.2 保護公共網路之應用服務
14	管理平臺僅負責 T-Road傳輸通道之安全性及可用性，資料正確性由各資料提供機關負責。	(1) 未提供足夠網路頻寬供各介接機關使用，致使資料上傳失敗，導致需求機關未能提供服務。 (2) 未加密或遮罩敏感資料，致使機敏資料遭不當冒用之風險。	A.14.1.3 保護應用服務交易	6.11.1.2 保護公共網路之應用服務
15	若經發現因資料傳輸效能對整體平臺運作造成影響或有發生資安事故之考量，有權暫時終止提供介接機關服務或安控伺服器連線。	未於發生資安事件時即時排除，且未即時終止發生事件機關之連線，致使其他機關與 T-Road 管理平臺遭橫向攻擊之風險。	A.16 資訊安全事故管理	6.13 資訊安全事故管理

(三)維運機關針對前項 T-Road 欲達成之功能，若有無法滿足安全要求之項目，應進入風險處理，在開發過程中盡早滿足。

五、T-Road 資料中心設置機關資通安全管理措施評估方法

(一) 資料中心設置機關針對 T-Road 欲達成之功能，應有安全要求項目，在介接前應盡早滿足：

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
1	機關資安責任等級應辦事項-技術面	資料中心設置機關未符合機關資安責任等級 A 級之技術面應辦事項，恐有資安風險。	N/A	N/A
2	資通系統防護需求及防護基準	各機關自行或委外開發之資通系統未依法進行資通系統防護需求分級，或未依資通系統防護基準執行控制措施。	N/A	N/A
3	安控伺服器環境安全與連線	(1) 伺服器未安裝於機櫃中或實體管制隔離區(如：機房)，可能因人員誤觸或未經授權人員有機會碰觸，而造成設備損壞、資料外洩或服務中斷。 (2) 伺服器擺放位置，未考量安全環境(如：溫度、濕度、電力、監控等)，可能因安全環境背景，造成伺服器損壞或服務中斷。 (3) 未管制個人電腦內建式燒錄機或USB連接埠，透過可攜式媒體將資料複製攜出，致使資料於未授權情況下，造成資料外洩、遺失或遭受其他侵害。 (4) 存放設備之實體門禁未進行出入管制或長時間不使用時未將設備妥善收存，造成同仁、外部訪客或廠商可能無意/故意將設備攜出，致使	A.11.1.1 實體安全周界 A.11.1.4 對外部與環境的威脅的保護	

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
		設備遺失、資料外洩或遭受其他侵害。		
4	資料中心憑證管理	資料中心設置機關未向政府憑證管理中心申請憑證，造成簽章金鑰強度不足或憑證效期過長，致使增加憑證遭冒用之風險。	A.10.1.2 金鑰管理加密金鑰使用、保護與存續期間的政策，應加以發展與實作於整個生命週期。	
5	安控伺服器備援環境	(1) 機房未設有不斷電系統或備援發電機，停電時造成系統主機無法得到足夠供電，致使業務無法持續運作或主機無法正常關機。 (2) 電子類之個資檔案未有適當備援、備份或其他符合當前技術水準之備援措施，並定期測試有效性(備註)，致使個資遭遺失或其他侵害後，難以即時復原。 (3) 安控伺服器未準備足夠之備份設施，致使必要的資訊和軟體在災難或儲存媒體失效後無法即時復原。 (5) 資料提供機關未使用完整性驗證工具驗證備援資料，致使無法偵測未經授權變更之特定軟體及資訊。	12.3.1 資訊備份 A14.2.6 安全發展環境	6.9.3.1 資訊備份

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
6	安控伺服器硬體環境之管理及維護	(1) 伺服器擺放位置，未考量安全環境(如：溫度、濕度、電力、監控等)，可能因安全環境背景，造成伺服器損壞或服務中斷。 (2) 伺服器超過廠商保固期限，未定期編列經費維護或汰換，造成設備可能因零件損壞時無料可維修，致使服務中斷。	A.11.1.1 實體安全周界 A.11.1.2 安全區域入口保護	
7	資料中心容量管理	網路服務頻寬不足，未能滿足作業需求，致使影響營運品質或服務水準。		
8	惡意程式處理及通知	(1) 資料中心未降低可能被惡意軟體利用之脆弱性，致使增加遭惡意攻擊之可能性。 (2) 對於支援重要營運程序之系統與資料內容未定期審查，致使出現未經核准的檔案或未經授權的更新作業，影響系統安全。 (3) 資料中心未界定惡意軟體的管理程序及責任，致使無法由所通報之惡意軟體攻擊中復原，影響系統運作。 (4) 資料中心未即時將惡意程式警訊進行通報，致使增加其他機關遭侵害之風險。	A.12.2.1 防範惡意軟體之控制措施防範惡意碼的偵測 A.16.1.3 通報資訊安全弱點 A.16.1.7 證據的收集	

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
9	資安事件因應	(1) 組織未設置資安事件監控及告警系統，致使無法即時通報資安事件及掌握個資當事人遭侵害之情形。 (2) 組織未依照資安事件通報及處理程序即時通報，無法控制及追蹤後續處理情形，致使災難性風險。	A.16.1.1 責任與程序。 A.16.1.2 通報資訊安全事件 資訊安全事件應循適切的管理管道儘速通報。	6.13.1.1 組織應建立識別和記錄個人識別資訊(PII)侵害行為的責任和程序。 6.13.1.5 對資訊安全事故之回應料

(二)資料中心設置機關若有安全要求無法滿足，應進入風險處理計畫，改善後方可進行介接。

六、T-Road 介接機關資通安全管理措施評估方法

(一)公務機關於介接前，應針對介接 T-Road 之功能面進行安全評估，避免各項介接風險。

(二)公務機關若有安全要求無法滿足，應進入風險處理計畫，改善後方可進行介接。

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
1	機關資安責任等級應辦事項-技術面	資料需求機關未符合機關資安責任等級 A 級之技術面應辦事項，恐有資安風險。	N/A	N/A
2	資通系統防護需求及防護基準	各機關自行或委外開發之資通系統未依法進行資通系統防護需求分級，或未依資通系統防護基準執行控制措施。	N/A	N/A

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
3	安控伺服器安全維護	(1) 安控伺服器非為專機使用，且安裝未經許可之軟體，機關未進行嚴格安全管控，致使資料傳輸不安全、資料外洩、軟體遭惡意攻擊或其他損害。 (2) 安控伺服器未啟用資通安全防護，如防毒軟體、防火牆、APT 防禦措施等，致使資料不當存取、資料傳輸不安全、資料外洩或其他損害。 (3) 安控伺服器未遵守 T-Road 管理規範，未限制網際網路存取，致使網路缺口導致之資料外洩、惡意攻擊或其他侵害。 (4) 安控伺服器未有 TLS 憑證驗證及傳輸通道未加密，致使資料外洩或其他損害。 (5) 未定期檢視安控伺服器憑證效期，導致憑證過期，不安全連線致使資料外洩或其他損害。	A.12.2.1 防範惡意軟體之控制措施 A.13.1.1 網路控制措施 A.13.2.2 資訊傳送協議 A.13.2.3 電子傳訊	N/A
4	安控伺服器作業系統以及軟體環境安全。	(1) 伺服器未落實作業系統更新/軟體及套件更新/漏洞修補，致使漏洞遭利用入侵、惡意攻擊或其他侵害。	A.12.2.1 防範惡意軟體之控制措施 A.13.1.1 網路控制措施 A.13.2.2	N/A

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
		(2) 未購買合適之作業系統、軟體及套件之授權，致使遭受廠商求償或抗議。 (3) 伺服器未適時汰換已停止支援更新之作業系統，導致無法執行更新檔，致使漏洞遭利用入侵、惡意攻擊或其他侵害。 (4) 伺服器未安裝適當防毒軟體並更新病毒碼，致使漏洞遭利用入侵、惡意攻擊、資料外洩或其他侵害。 (5) 未建立身分驗證機制，致使身分遭冒用、系統帳密遭竊取及冒用之風險。 (6) 未定期審查機關之權限，導致未即時移除或調整無使用需求之帳號，致使未經授權之存取、資料遭竊取或其他侵害。	資訊傳送協議 A.13.2.3 電子傳訊 A.18.1.2 智慧財產權	
5	介接機關之資料使用。	資料需求機關取得之資料，違反法令法規之要求，致使資料遭不當利用後，影響法律規章遵循或損害機關信譽。	A.18.1.3 紀錄之保護	N/A
6	API 格式規範	機關註冊之 API 未符合數位發展部訂頒之「共通性應用程式介面指引」，導致未符合 API 安全機制之風險。	A.12.6.2 對軟體安裝之限制 A.18.1.1 適用之法規及契約的要求事項之識別	6.15.1.1 適用之法規及契約的要求事項之識別

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
7	安控伺服器錯誤管理。	機關未定期確認加密憑證發布之漏洞資訊，導致漏洞遭有心人士利用/中間人攻擊，致使資料遭竊取、外洩或其他損失。	A.12.2.1 防範惡意軟體之控制措施	N/A
8	安控伺服器紀錄管理。	安控伺服器未自動產生完整的簽章和帶時間戳記的訊息紀錄於資料庫或檔案中，且未定期審查，導致未能即時發現異常，致使發生事件時未能即時追蹤。	A.12.4.1 事件存錄	6.9.4.1 事件日誌記錄
9	資料傳輸紀錄保存	未完整並妥善保存資料傳輸紀錄，保存時間不足，致使無法追查傳輸紀錄並即時處理。	A.12.3.1 資訊備份 A.13.2.3 電子傳訊 A.12.4.1 事件存錄	6.9.3.1 資訊備份 6.9.4.1 事件日誌記錄
10	安控伺服器紀錄備份	機關未定期將安控伺服器訊息紀錄及稽核紀錄備份至外部裝置或資料庫，致使發生資通安全事件時無法即時追查並處理。	A.12.3.1 資訊備份 A.16.1.2 通報資訊安全事件	6.9.3.1 資訊備份
11	紀錄之正確性及有效性	未定期審查管理者、操作者及使用者之活動日誌，未能即時偵測或阻止資安事件或事故之發生。	A.12.4.3 管理者及操作者日誌	N/A
12	介接機關安全評估	(1) 資料中心設置機關需考量是否有足夠資源達成「行政院資通安全責任等級分級辦法」A 級公務機關應辦事項技術面之要求。 (2) 資料中心設置機關未將跨資料傳輸之軟、硬體設備納入 SOC 監控範圍，致使	資通安全責任等級分級辦法 A.13.2.2 資訊傳送協議 A.16.1.2 通報資訊安全事件	N/A

項次	T-Road 功能面	功能面風險	對應領域(資安)	對應領域(個資)
		未能即時發現異常狀況，而影響服務之提供。 (3) 資料中心設置機關未符合法令法規之資料傳輸要求，致使資料遭竊取或外洩，影響法律規章遵循或損害機關信譽。 (4) 未遵循資通安全事件通報及應變辦法規範，未即時通報及執行後續追蹤，導致服務中斷及遵法性風險。		
13	安控伺服器服務身分驗證	(1) 安控伺服器未進行身分驗證，導致身分遭冒用風險，致使不當存取服務造成之資料外洩、竊取或其他侵害。 (2) 身分驗證紀錄保存時間不足，導致追查不利，致使無法即時追查事件紀錄並處理。	A.12.4.1 事件存錄 A.18.1.4 個人可識別資訊之隱私及保護	6.9.4.1 事件日誌記錄

肆、T-Road 風險評估結果

一、T-Road 維運機關適法性評估結果

(一)T-Road 維運機關適法性評估結果如附表一所示。

(二)T-Road 維運機關已依據「個人資料保護法」、「資通安全管理法」等各項法令法規進行T-Road功能增修及維運，於評估區間，未發現有違反上述法規之事實。

(三)T-Road 維運機關適法性評估總結

1. 實際檢視T-Road維運機關因介接機關之系統介接聯繫作業之必要，於 T-Road 單一登入平台模組(SSO)保留介接機關之承辦人員姓名、公務電話號碼、公務電子郵件及承辦人員自然人憑證卡號，上述保留之個人資料欄位均已使用明碼轉置亂碼化之技術，於完成去連結化後保存，其保留目的為執行介接業務之必要保存，係為特定目的之必要，資料欄位已依資料需求最小化保存，符合適當比例原則。
2. 實際檢視T-Road維運機關並未蒐集、處理、利用民眾個人資料；T-Road 維運機關係提供介接機關進行資料傳輸使用，其傳輸過程並未保留所傳輸之資訊。
3. 實際檢視T-Road維運機關未收集各介接機關之相互傳輸資料，T-Road 維運機關僅提供資料傳輸服務，其資料傳輸係建立於GSN VPN之加密通道傳輸；另系統查核傳輸紀錄檔均已正常保存，如發生異常或糾紛情事，可檢視傳輸紀錄檔確認是否異常，並確保資料傳輸是否符合法令依據之要求，符合使用紀錄、軌跡資料及證據保存之規範。
4. 實地檢視T-Road維運機關暨政府資料傳輸平臺已通過資訊安全之國際標準及取得第三方外部驗證之有效證書，T-Road 之日常維運亦遵循隱私保護之國際標準要求，預計於 113 年進行第三方外部驗證。惟應持續關注相關資訊安全暨隱私保護國際標準之改版差異與營運現況是否相符。並關注國內外個

人資料外洩事件等情境之風險（本部預計於 113 年度執行 ISO / CNS 27001 資訊安全、網宇安全及隱私保護－資訊安全管理標準新版驗證作業，確保本部之安全管控措施接軌最新標準之要求）。

5. 依據「政府資料傳輸平臺管理規範」第八點：「透過 T-Road 資料傳輸前，應確認該資料傳輸符合資通安全管理法、個人資料保護法、本管理規範及該介接機關所定資料傳輸規定等相關法令規定。」，因介接機關透過 T-Road 傳輸之資料可能包括個人資料，故維運機關暫存24小時之介接資料，若無法判別為是否含有個人資料時，宜留存相關軌跡紀錄。建議維運機關設計新增識別個人資料之選項，由資料提供機關於進行資料傳輸前，先行鑑別所傳輸之資料是否含有個人資料之欄位。

二、T-Road 維運機關安全性評估結果

(一)維運機關資訊安全管理評估內容如附表二所示。

(二)T-Road 維運機關已依據「個人資料保護法」、「資通安全管理法」、ISO27001、ISO27701 等法令法規及國際標準要求完成 T-Road 建置及維運，未有違反相關安全控管要求之事實。

(三)T-Road 安全管理措施評估結果總結

1. T-Road 於開發、測試及維運過程中，均已要求維運廠商定期依照專案進度、安控措施、異常狀態進行月報彙總，並已定期執行災害復原演練，假想系統服務異常時，可立即於最大可容忍中斷時間進行復原，其系統安全發展週期已受完整監督。

2. T-Road 係政府資料傳輸之基礎建設，其資通安全之控管措施均已遵循資通安全管理法之資通系統防護基準管控，故建議維運機關持續維護 T-Road 之資訊安全暨隱私保護制度之有效。

3. T-Road 維運機關已訂定「政府資料傳輸平臺管理規範」，提供介接機關基於 T-Road 傳輸管理之遵循，並定期或不定期進

行介接機關稽核，確保介接機關均已符合「政府資料傳輸平臺管理規範」辦理相關要求。

三、T-Road 委外開發安全評估

(一)T-Road 委外開發安全評估內容如附表三所示。

(二)T-Road 維運機關已依據「個人資料保護法」、「資通安全管理法」、ISO27001、ISO27701 等法令法規及國際標準要求辦理 T-Road 委外開發安全管理，未有違反相關安全控管要求之事實。

(三)T-Road 委外開發安全評估結果總結

1. T-Road 維運機關已通過資訊安全管理制度第三方驗證，其已具有系統委外開發安全管理要求，並預計於 113 年完成隱私保護國際標準之第三方外部稽核。
2. T-Road 系統開發由委外廠商執行，委外廠商於開發過程中，已符合 T-Road 維運機關之資通系統委外開發安全管理相關要求，如：
   (1) 資安法第 9 條、資安法施行細則第 4 條，對資通系統委外開發、維運之資通安全要求與監督。
   (2) 個資法施行細則第 8 條業務委外監督、第 12 條安全管理措施等。
   (3) 資訊安全暨隱私保護管理制度相關委外要求，如專案管理要求、資訊安全要求規格分析、供應鏈安全管理要求、委外開發安全、驗收測試、委外廠商資訊安全要求等。

(四)T-Road 委外開發安全經評估後，已依法規規範及機關現有安全管理規範進行各項監督，尚無需要立即處理之風險。

四、T-Road 運作功能安全管理措施評估結果總結

(一)T-Road 安全管理功能尚稱完備：

1. 中央控管功能：負責各安控伺服器的憑證管理、登錄註冊、提供的服務、各項異動即時通知等。
2. 設定管理功能：管理各安控伺服器組態之下載及更新。
3. 運作監控功能：記錄、蒐集、彙整各安控伺服器及管理平臺的操作記錄，並保存相關查調記錄。
4. 環境監控功能：記錄、蒐集各安控伺服器及管理平臺的環境使用及運作狀態，並依狀況啟動相關備援機制，如 CPU、記憶體、磁碟空間狀態等。
5. 時間戳記管理功能：紀錄透過 T-Road 傳輸之各項資料之時間，並具不可否認性之驗證。

(二)安控伺服器已有適當安全管理設計：介接機關透過安控伺服器達成 T-Road 點對點資訊傳輸之功能，除須遵循「政府資料傳輸平臺管理規範」之要求外，各安控伺服器間具備安全之傳輸層、訊息層及檔案傳送等功能，安控伺服器若需進行系統更新，亦有通知機制，要求各機關承辦人員進行更新。

(三)API 介接規格具備監督功能：各機關介接 T-Road 時，須符合數位發展部「共通性應用程式介面指引」」Open API 開發之要求，平臺使用者可以一致性之 API 規格取得資料，管理平臺具備 API 監控機制，可即時監督 API 連線狀態、回應時間、授權狀態及錯誤狀態。

(四)資料傳輸具適當加密功能設計：為使透過 T-Road 傳輸之資料獲得安全保障，T-Road 全程將透過 GSN VPN 之加密通道進行傳輸，並以 GCA 憑證進行傳輸資料之加密保護。

(五)加密演算法具適當強度：為確保資料傳輸完整性、正確性及不可否認性，採用 RSA2048 bits 長度非對稱式加密金鑰演算法，搭配 AES256 bits 長度對稱式加密金鑰演算法，強化資料傳輸機密性。

(六)資料留存已最小化：T-Road 維運平臺僅負責安全管理，介接機關間傳輸之資料僅留存於資料需求機關及資料提供機關，T-

Road 除須進行安全管理所必要留存之傳輸紀錄外，並不留存其傳輸之資料。

(七)T-Road 運作安全功能已保存各項文件化資訊，尚屬完備：

1. 分析設計階段，開發團隊針對未來運作時之系統安全需求，進行安全設計，並且保留文件化資訊：
   (1) 系統存取控制與身分認證機制。
   (2) 機敏資料保護、加密機制。
   (3) 資料備份需求與容量。
   (4) 系統當機回復程序。
   (5) 避免系統資料未經授權之修改措施。
   (6) 系統操作手冊。
2. 架構設計階段，已有相關資訊提供設計人員進行架構開發：
   (1) 程式開發安全規則。
   (2) 已針對 T-Road 評估為資通系統分級中級，並依據分級結果對應之資通系統防護基準設計安全控管。
   (3) 設計權限分離機制。
   (4) 設計密碼管理、傳輸加密機制。
   (5) 設計連線時間管理機制。
   (6) 設計端點回應機制。
   (7) 設計強制存取路徑。
3. 程式實作階段，已設計系統各項參數輸入控管與防護，針對未預期錯誤或異常狀況有安全的處理程序，避免透露重要資訊，且針對系統稽核與登入紀錄的管理，已有保護及定期紀錄備份和分析。
4. 系統測試已具文件化控管措施，檢查系統測試流程含跨系統各項控管機制與防護，包含 T-Road 導入時可能影響之既有系統，進行事前相關的防護措施，並留存各項測試紀錄。

5. 已設有程式版本控制措施，並於程式變更佈署前，確認各項安全控管機制與防護措施的運作狀況，確保其變更管理之有效。

6. 委外廠商已每年定期進行資安教育訓練。

7. 已控管資安防護措施之持續性及變更管理。

(八)已有 T-Road 針對運作安全功能要求落實及佈達之具體證據：

1. T-Road 傳輸平臺已通過第三方稽核完成資訊安全之國際標準驗證，並預計於 113 年完成隱私保護之國際標準外部稽核驗證。

2. T-Road維運機關已針對T-Road資料傳輸訂定「政府資料傳輸平臺管理規範」，定義 T-Road 維運機關與介接機關之各項所須遵循之要求。

3. 若 T-Road運作發生任何異常，則視異常情況依相關法令要求進行通報、處理。

(九)T-Road 維運機關針對 T-Road 各項運作安全功能及管理，已依據資訊安全暨隱私保護之國際標準要求規範進行開發、維運及管理，尚無需要立即處理之風險。

五、T-Road 介接機關適法性評估

(一)T-Road 介接機關評估結果

1. 實地檢視介接機關須提出介接申請，依資安法之各項要求進行資訊安全管理，並透過T-Road傳輸模組進行資料傳輸。相關要求均於「政府資料傳輸平臺管理規範」進行列示，並搭配整體稽核規劃，確認完整性及有效性。

2.介接機關依個人資料保護法及施行細則，規劃各項安全管理措施，確保個資當事人權利受到適當保護，包含機關之告知義務、公示義務、個資違失通知義務、安全維護義務、當事人權利行使機制等。

(二)T-Road 介接機關適法性風險處理方向

1. T-Road維運機關收到介接機關申請介接，經T-Road維運機關核可後方能進行介接。
2. 介接機關間透過T-Road進行資料傳輸前，遵循資安法及個資法之各項要求：
   (1) 介接機關滿足資安責任等級各項應辦事項之證明。
   (2) 介接機關已完成資通系統分類分級作業及資安防護基準證明。
   (3) 介接機關已針對個人資料之傳輸、利用等作業，鑑別應符合之法令要求。
   (4) 介接機關已完成個資法施行細則要求各項安全管理措施之證明。
   (5) 介接機關已依據「政府資料傳輸平臺管理規範」進行各項安控措施。
3. T-Road維運機關保留准駁申請T-Road介接權利，並定期與不定期稽核介接機關是否已依據「政府資料傳輸平臺管理規範」進行資料傳輸；實地檢視 112 年度介接機關稽核作業之相關紀錄，均已依「政府資料傳輸平臺管理規範」辦理T-Road介接作業。
4. 依據「政府資料傳輸平臺管理規範」第八點：「透過 T-Road 資料傳輸前，應確認該資料傳輸符合資通安全管理法、個人資料保護法、本管理規範及該介接機關所定資料傳輸規定等相關法令規定。」，故資料提供機關透過 T-Road 傳輸之資料，應事先鑑別傳輸資料是否含有個人資料，以利於發生個資事故時，得進行相關追查以及責任釐清，以確保符合法規要求。
5. 依據個人資料保護法第 17 條：「公務機關應將下列事項（個人資料檔案名稱、保有機關名稱及聯絡方式、個人資料檔案保有之依據及特定目的、個人資料之類別)公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同。」及個人資料保護法施行細則第 23 條：「公務機關依本法第十七條

規定為公開，應於建立個人資料檔案後一個月內為之；變更時，亦同。公開方式應予以特定，並避免任意變更。」。故資料需求機關若有透過T-Road取得之個人資料檔案者，應於特定目的結束後儘速刪除，如有保存之必要者，應依上開規定辦理。

伍、持續關注議題

本部業已訂定「政府資料傳輸平臺管理規範」，規範介接機關利用 T-Road 進行資料傳輸之資訊安全及隱私保護措施。惟事關民眾個人資料之安全性議題，亦應持續掌握可能影響民眾權益之相關事件。如：109 年間，境外網站遭揭露於暗網拍賣我國民眾個人資料，其資料筆數達 2 千萬筆以上，並稱係我國內政部戶政資料外流一事，引起社會關注。而職掌戶政資料之內政部戶政司現已成為 T-Road 介接機關，並預計透過 T-Road 傳輸戶政資料。故整體 T-Road 營運之資訊安全及隱私保護，除了本部（T-Road 維運機關）持續堅守T-Road之安全性之外，介接機關亦應時刻確保民眾個人資料之保護。

此外，行政院依據憲法法庭 111 年憲判第 13 號判決意旨，已在 112 年 12 月 15 日設立個人資料保護委員會籌備處，以落實資訊隱私權保障，並促進個人資料之合理利用。目前該籌備處已著手研擬個人資料保護法之修正草案，研擬重點包含：對於公務機關之監督、公務機關發生個人資料侵害事故之通報義務及公務機關個人資料安全維護措施標準等，以強化公務機關個人資料保護事務之責任。依上開憲法判決意旨，個人資料保護委員會最晚需於 113 年 8 月前成立，未來，該委員會也將職掌對公務機關個人資料保護事務之監督、查核、通報、陳情等相關機制之規劃。

由上開引起社會關注之新聞及憲法法庭判決等效應影響下，本部未來將持續關注個人資料相關議題，如：當事人之權利行使、識別個人資料以及公務機關個資保護責任等發展趨勢，並遵循相關程序規定，以符合社會環境變遷、民眾需求及法令趨勢之變革。

陸、附表

附表一、T-Road 維運機關適法性評估結果

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
1	告知原則	機關向當事人蒐集個人資料時，除個資法第八條第二款情形之一者外，是否明確告知當事人下列事項？ 一、機關名稱。 二、蒐集之目的。 三、個人資料之類別。 四、個人資料利用之期間、地區、對象及方式。 五、當事人依第三條規定得行使之權利及方式。 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。	目前尚未針對可能蒐集到的個人資料，規劃告知程序及內容，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
		機關蒐集非由當事人提供之個人資料，除個資法第九條第二款情形之一者外，是否於處理或（首次）利用前，向當事人告知個人資料來源及個資法第八條第一項第一款至第五款所列事項？	目前尚未針對可能蒐集到的個人資料，規劃告知程序及內容，故風險發生機率較高。	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
2	蒐集限制原則	機關是否已規範，除個資法第六條第一項各款所列情形之一	目前尚未針對可能蒐集到的	嚴重影響	高度風險	目前尚未針對介接機關可能

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		外，不得蒐集、處理或利用病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料？	個人資料進行清查，故風險發生機率較高。			包含之直接、間接識別當事人之資料進行清查，應進行清查後評估該項目。
		機關對個人資料之蒐集或處理，除個資法第六條第一項所規定資料外，是否有特定目的，並符合個資法第十五條第一項各款情形之一者（須備註符合之情形）？	目前尚未針對可能蒐集到的個人資料，規劃清查程序並釐清保有依據及特定目的，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
3	個人資料利用原則	機關對個人資料之利用，除個資法第六條第一項所規定資料及個資法第十六條第一項各款情形之一者外，是否於於執行法定職務必要範圍內為之，並與蒐集之特定目的相符？	目前尚未針對 T-Road 可能包含之直接、間接識別當事人之資料進行清查，並確認是否符合法定職務及特定目的，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		機關是否已規範對個人資料特定目的外之利用，需符合下列各款情形之一者？ 一、法律明文規定。 二、為維護國家安全或增進公共利益。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。 六、有利於當事人權益。 七、經當事人同意。	目前尚未針對 T-Road 可能包含之直接、間接識別當事人之資料進行清查，並確認特定目的，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
4	當事人自主原則	機關是否已規範接受當事人權利行使程序，且應保護該權利，不得要求當事人預先拋棄或以特約限制之。	目前組織尚未規劃個資當事人權利行使程序，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
		機關是否已規範如個人資料正確性有爭議者，應主動或依當事	目前組織尚未規劃當事人針	嚴重影響	高度風險	T-Road 已參考國際標準

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		人之請求停止處理或利用？(但因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限)	對爭議個資處理程序，故風險發生機率較高。			ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
		機關是否已規範當個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料？(但因執行職務或業務所必須或經當事人書面同意者，不在此限)	目前組織尚未規劃個資內部蒐集、處理或利用程序，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
		機關是否已規範違反個資法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料？	目前組織尚未規劃個資內部蒐集、處理或利用程序，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
5	查閱及更正原則	機關是否除個資法第十條各款除外情形之一者外，已規範依當事人之請求，就其蒐集之個人資料，答覆	目前組織尚未規劃當事人行使個資權利之內部	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		查詢、提供閱覽或製給複製本？	處理程序，故風險發生機率較高。			27701 建置資安、個資管理制度，應可滿足該項要求。
		機關是否已規範，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象？	目前組織尚未規劃個資內部蒐集、處理或利用程序，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
		機關是否已規範受理當事人依個資法第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人？	目前組織尚未規劃當事人行使個資權利之內部處理程序，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
		機關是否已規範受理當事人依個資法第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應	目前組織尚未規劃當事人行使個資權利之內部處理程序，故風	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		將其原因以書面通知請求人？	險發生機率較高。			個資管理制度，應可滿足該項要求。
6	個人資料完整性原則	機關是否已規範維護個人資料之正確，並應主動或依當事人之請求更正或補充之？	目前組織尚未規劃當事人行使個資權利之內部處理程序，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
7	安全管理原則	機關保有個人資料檔案者，是否已應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏？	目前組織尚未規劃個資檔案安全防護程序，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應可滿足該項要求。
		機關是否已規範保有個人資料檔案者，應指定具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員並接受相關專業之教育訓練，辦理個資法施行細則第十二條	目前組織尚未規劃個資檔案安全防護程序，故風險發生機率較高。	嚴重影響	高度風險	T-Road 已參考國際標準 ISO 27001、ISO 27701 建置資安、個資管理制度，應

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		第二項之十一款安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏？				可滿足該項要求。
8	責任原則	機關是否已規範違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，查明後以適當方式通知當事人？	目前組織尚未規劃個資事故侵害應變通報程序，故風險發生機率較高。	嚴重影響	高度風險	T-Road已參考國際標準ISO 27001、ISO 27701建置資安、個資管理制度，應可滿足該項要求。
		機關是否已規範，委託他人蒐集、處理或利用個人資料時，對受託者之監督事項至少包含個資法施行細則第八條所規定之事項？	目前組織尚未規劃T-Road委外管理安全要求，故風險發生機率較高。	嚴重影響	高度風險	T-Road已參考國際標準ISO 27001、ISO 27701建置資安、個資管理制度，應可滿足該項要求。
		機關是否已規範，違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人？	目前組織尚未規劃T-Road個資侵害管理安全要求，故風險發生機率較高。	嚴重影響	高度風險	T-Road已參考國際標準ISO 27001、ISO 27701建置資安、個資管理

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
						制度，應可滿足該項要求。

附表二、維運機關資訊安全管理評估內容

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
1	機關資安責任等級應辦事項	T-Road 維運機關符合機關資安責任等級 A 級之應辦事項，行恐有違法之虞。	維運機關已完成資安管理制度，發生機率低(甚少發生)	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關要求亦會進行鑑別並落實，應可滿足該項要求。
2	資通系統防護需求及防護基準	各機關自行或委外開發之資通系統依法進行資通系統防護需求分級，或依資通系統防護基準執行控制措施。	維運機關已完成資安管理制度，發生機率低(甚少發生)	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關要求亦會進行鑑別並落實，應可滿足該項要求。
3	(一)系統組態設定及管理 (二)安控伺服器註冊管理	(1) 於系統需求訪談階段，未識別資料輸出入之機敏性，造成不當存取的風險 (2) 未檢核資料輸入正確性，導致資料庫異常或遭惡意注入之風險。	(1)維運機關委託已通過 ISMS 驗證之專業團隊進行開發，相關系統元件交付前均會進行安全檢測並完成修補。 (2)系統開發時已預先針對資通安全責任等級要求之通系統防護需求-中	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關要求亦會進行鑑別並落實，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(3) 使用或未定時更新已知存有漏洞風險之函式庫，導致系統遭惡意入侵，遭植入惡意程式進行資料竊取或影響系統服務。 (4) 未加密或遮罩敏感資料，致使機敏資料遭不當冒用之風險。 (5) 未遵循政府組態基準設定相關安全參數，致使伺服器組態不一致或植入惡意程式之風險。	級進行安全功能設計。 (3)均符合左項要求，故發生機率低(甚少發生)			

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(6) 防火牆政策未以最小化設定為原則管理，可能存有惡意連線存取、已開啟之服務遭利用之風險。 (7) 未即時更新即將過期之憑證，致使網站未被信任或可能遭冒用之風險。 (8) 未設有系統校時機制，致使系統軌跡留存時間錯置、可能接受過期憑證，或是讓許多必須檢驗時間的訊息傳輸				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		無法進行。 (9) 未設有系統異常自動告警機制，致使系統服務異常無法於可容忍中斷時間內回復，或於系統備份失敗時無法即時排除。 (10) 未確實評估系統服務所需之記憶體大小，致使系統可用性不足，造成服務異常。 (11) 未正確註冊、變更或註銷安控伺服器之來源目的端，致使未經授權資料遭				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		盜用、偽冒或惡意利用之風險。				
4	管理各安控伺服器組態的下載服務及更新服務。 (一)組態設定管理 (二)下載組態設定	(1) 未遵循政府組態基準設定相關安全參數，致使伺服器組態不一致或植入惡意程式之風險。 (2) 未落實安控伺服器於資料傳輸時之憑證有效性檢核，致使未經授權之傳輸，或遭中間人偽冒攻擊之風險。 (3) 未確實評估系統服務所需之記憶體大小，致使系統可用	(1)系統開發時已預先針對資通安全責任等級要求之通系統防護需求-中級進行安全功能設計。 (2)系統憑證管理均透過憑證中心，憑證有效性均被檢核。 (3)系統開發後進行測試時，將針對系統效能進行測試，確保系統運作順暢。 (4)均符合左項要求，故發生機率低(甚少發生)	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關要求亦會進行鑑別並落實，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		性不足，造成服務異常。				
5	紀錄、蒐集、彙整各安控伺服器及管理平臺的操作紀錄，並保存查調紀錄的相關Log (一)監控提供服務 API (二)使用者操作紀錄限，並自動備份 (三)異常告警功能 (四)查詢異常紀錄功能可查詢用戶端操作異常紀錄	(1)未自動備份 API 使用軌跡，致使資料傳輸出錯時，無法有效查找問題。 (2)未確實留存使用者操作軌跡，致使資料外洩、錯誤或發生異常時，無法有效釐清責任歸屬。 (3)未設有系統異常自動告警機制，致使系統服務異常無法於可容忍中斷時間內回復，或於系統	(1)系統將會保留使用紀錄五年，各項紀錄應可供查證。 (2)系統開發時已預先針對資通安全責任等級要求之通系統防護需求-中級進行安全功能設計。 (3)系統發生異常時，將有級時警告機制。 (4)資料及軟體程式亦有備援措施。 (5)系統開發後進行測試時，將針對系統效能進行測試，確保系統訊行效率。 (6)均符合左項要求，故發生機率低(甚少發生)	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關要求亦會進行鑑別並落實，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		備份失敗時無法即時排除。 (4)未確實評估系統服務所需之記憶體大小，致使系統可用性不足，造成服務異常。 (5)未正確設定系統異常告警通知人員，導致於系統出錯時無法快速排除或應通報而未通報負責人員。				
6	監控環境功能	(1)未設有系統異常自動告警機制，致使系統服務異常無法於可容忍中斷時間內回復，	(1)系統開發時已預先針對資通安全責任等級要求之通系統防護需求-中級進行安全功能設計。 (2)系統發生異常時，將有	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關要求亦會進行鑑別並落實，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		或於系統備份失敗時無法即時排除。 (2)未確實評估系統服務所需之記憶體大小，致使系統可用性不足，造成服務異常。 (3)未正確設定系統異常告警通知人員，導致於系統出錯時無法快速排除或應通報而未通報負責人員。	級時警告機制。 (3)資料及軟體程式亦有備援措施。 (4)系統開發後進行測試時，將針對系統效能進行測試，確保系統訊行效率。 (5)均符合左項要求，故發生機率低(甚少發生)			
7	安控伺服器(Security Server; 簡稱SS)功能	(1)未定期檢視各機關安控伺服器之作業環境作業系統版本、套件版本及相	(1)維運機關委託已通過ISMS驗證之專業團隊進行開發，相關系統元件交付前均會進行安全	嚴重影響	低度風險	T-Road已參考國際標準ISO 27001建置資安管理制度，資安法相關要求亦會進行鑑別並落實，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		關組態設定，致使已知漏洞遭利用之風險。 (2)未使安控伺服器透過防火牆或其他安全設施管控與其他主機間之資料傳輸及資源存取，造成未經授權之存取風險。 (3)未使用較高強度之加密措施進行傳輸加密，導致已知弱加密遭破解，造成資料外洩之風險。 (4)未定期執行安控伺服器主機作業系統	檢測並完成修補。 (2)系統開發時已預先針對資通安全責任等級要求之通系統防護需求-中級進行安全功能設計。 (3)傳輸之資料均會透過適當強度之通道加密。 (4)均符合左項要求，故發生機率低(甚少發生)			

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		之更新，致使已知漏洞遭利用之風險，導致資料不當外洩。				
8	Log 查調紀錄保存五年	(1)未確實評估系統服務所需之記憶體、磁碟大小，致使系統可用性不足，造成服務異常。 (2)未設有系統校時機制，致使系統軌跡留存時間錯置、可能接受過期憑證，或是讓許多必須檢驗時間的訊息傳輸無法進行。	(1)維運機關委託已通過 ISMS 驗證之專業團隊進行開發，開發過程均符合 ISMS 要求之系統開發安全進行。 (2)系統已規劃校時機制。 (3)系統開發時已預先針對資通安全責任等級要求之通系統防護需求-中級進行安全功能設計。 (4)系統進行測試時，將會針對容量及效能測試。 (5)各項使用紀錄均妥善保存並備份。	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關要求亦會進行鑑別並落實，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(3)未設定僅有權限之人員能夠存取訊息記錄及稽核紀錄，導致人員不當刪除、外洩其機敏存取軌跡。 (4)未定期備份安控伺服器之訊息紀錄及稽核紀錄，致使問題查找、責任歸屬無法釐清。	(6)均符合左項要求，故發生機率低(甚少發生)			
9	核定資料中心設置機關申請介接	未依照「行政院資通安全責任等級分級辦法」之A級公務機關應辦要求，定期執行程式碼弱點掃描、系統弱點掃描、滲透測試等弱點管理之要求，	(1)維運機關已符合A級機關資安責任等級，定期辦理各項應辦事項。 (2)均符合左項要求，故發生機率低(甚少發生)	嚴重影響	低度風險	T-Road已參考國際標準ISO 27001建置資安管理制度，資安法相關安全要求將納入管理，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		致使系統已知漏洞遭不當嘗試利用之風險。				
10	T-Road 傳輸系統之規劃與開發設計及傳輸資料加密等安全性評估與考量	(1) 於系統需求階段是否已針對系統安全需求(含機密性、完整性、可用性)進行確認 (2) 於系統需求訪談階段，未識別資料輸出入之機敏性，造成不當存取的風險 (3) 未檢核資料輸入正確性，導致資料庫異常或遭惡意注入之風險 (4) T-Road傳輸未使用較高強度之加密措施進行傳	(1)系統開發時已預先針對資通安全責任等級要求之通系統防護需求-中級進行安全功能設計。 (2)系統開發時符合行政院SSDLC系統開發安全要求，將資安納入系統開發生命週期。 (3)均符合左項要求，故發生機率低(甚少發生)	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關安全要求將納入管理，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		輸加密，導致已知弱加密遭破解，造成資料外洩之風險。 (5) 於系統設計階段，未依據系統功能與要求識別可能影響系統之威脅，進行風險分析及評估，造成系統有遭不當破解之風險。				
11	作業系統漏洞修補作業及發布作業系統漏洞修補更新通知	未定時追蹤作業系統之漏洞修補測試，或未更新已知漏洞風險之作業系統、軟體、元件，致使不當存取之風險。	(1)系統開發時符合行政院SSDLC系統開發安全要求，將資安納入系統開發生命週期。 (2)安控系統已規劃漏洞修	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關安全要求將納入管理，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
			補及更新機制。 (3)均符合左項要求，故發生機率低(甚少發生)			
12	系統程式版本控管及安全派送機制	(1)未落實系統程式版控，且未區分版本控制人員之存取權限，導致程式碼遭惡意盜用之風險。 (2)未遵循程式更新安全派送機制，導致系統更新失敗，部分系統無法使用。 (3)未對程式碼執行完整性及不可竄改之確認。	(1)系統開發時符合行政院SSDLC系統開發安全要求，將資安納入系統開發生命週期。 (2)程式碼版本控制之存取控制均已定期審核並已留存存取軌跡。 (3)均符合左項要求，故發生機率低(甚少發生)	嚴重影響	低度風險	T-Road已參考國際標準ISO 27001建置資安管理制度，資安法相關安全要求將納入管理，應可滿足該項要求。
13	安控伺服器之作業環境建立標準系統	未建立安控伺服器之作業環境組態標準，致使	(1)安控系統已規劃漏洞修	嚴重影響	低度風險	T-Road已參考國際標準ISO 27001建置資安管理制度，資

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
	安全維護設準則	各安控伺服器作業環境設定不一，導致傳輸錯誤、服務失效或未更新之組態遭已知漏洞攻擊之風險。	補及更新機制。 (2)均符合左項要求，故發生機率低(甚少發生)			安法相關安全要求將納入管理，應可滿足該項要求。
14	T-Road 資料傳輸網段管制及申請	未正確區隔 T-Road 與其他服務之網段區隔，致使未經授權之機關或其他連線來源端不當存取之風險。	(1)僅有透過 GSN VPN 方可連線。 (2)安控系統鎖定機關 IP 與憑證。 (3)均符合左項要求，故發生機率低(甚少發生)	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關安全要求將納入管理，應可滿足該項要求。
15	平臺安全傳輸協定及機制	(1)T-Road 傳輸未使用較高強度之加密措施進行傳輸加密，導致已知弱加密遭破解，造成資料外洩之風險。 (2)未加密或遮罩敏感資料，致	(1)平臺整體資料傳輸，均透過 GSN VPN 進行通安加密。 (2)平臺使用介面呈現之個人資料若需遮蔽，可透過系統更新方式增加此功能。 (3)均符合左項要求，故發	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關安全要求將納入管理，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		使機敏資料遭不當冒用之風險。	生機率低(甚少發生)			
16	管理平臺傳輸通道之安全性及可用性	(1)未提供足夠網路頻寬供各介接機關使用，致使資料上傳失敗，導致需求機關未能提供服務。 (2)未加密或遮罩敏感資料，致使機敏資料遭不當冒用之風險。	(1)平臺上線前已進行功能測試，確實符合機關效能需求。 (2)平臺使用介面呈現之個人資料若需遮蔽，可透過系統更新方式增加此功能。 (3)均符合左項要求，故發生機率低(甚少發生)	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關安全要求將納入管理，應可滿足該項要求。
17	終止提供介接機關服務或安控伺服器連線。	未於發生資安事件時即時排除，且未即時終止發生事件機關之連線，致使其他機關與 T-Road 管理平臺遭橫向攻擊之風險。	(1)平臺具備異常通之功能。 (2)若因介接機關影響 T-Road 安全性，維運機關將可中止連線。 (3)均符合左項要求，故發	嚴重影響	低度風險	T-Road 已參考國際標準 ISO 27001 建置資安管理制度，資安法相關安全要求將納入管理，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
			生機率低(甚少發生)			

附表三、T-Road 平臺委外開發安全評估

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
1	專案管理資訊安全	組織是否將以確保將識別並處理資訊安全風險管理作為委外專案管理之一部份，如在專案的早期階段實施資訊安全風險評鑑以識別必要的控制措施，並定期審查委外專案資訊安全之符合性，並界定委外專案內對特定角色界定與配置資訊安全責任。	(1)T-Road 開發廠商已取得 ISMS 驗證證書，並於專案進行過程進行 DPIA。 (2)專案執行過程之各項安全要求，如系統開發安全、委外人員保密、開發環境安全等，均定期透過專案月會與 T-Road 維運機關報告。 (3)均符合左項要求，故發生機率低(甚少發生)	嚴重影響	低度風險	T-Road 維運機關已取得 ISMS 驗證證書，T-Road 平臺已參考國際標準 ISO 27001 建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。
2	人員管理安全	組織是否針對所有可能被委託聘用者所進行基本背景調查，依相關法律、法規，並應相稱於營運要求及其將存取之資訊的保密等級及組織所察覺之風險，確	(1)T-Road 開發廠商已取得 ISMS 驗證證書，人員進用符合 ISMS 要求。 (2)T-Road 開發案契約已有要求人員資格並簽訂保密協議。 (3)符合左項要求，故發生機率低(甚少發生)。	嚴重影響	低度風險	T-Road 維運機關已取得 ISMS 驗證證書，T-Road 平臺已參考國際標準 ISO 27001 建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		認是否聘用。				
3	人員管理安全	組織是否針對委外承包者簽訂契約化協議書，敘明雙方對資訊安全的責任。	(1)T-Road 開發案為公開招標案，與開發商具有正式委託契約，契約內包含資訊安全責任。 (2)符合左項要求，故發生機率低(甚少發生)。	嚴重影響	低度風險	T-Road 維運機關已取得 ISMS 驗證證書，T-Road 平臺已參考國際標準 ISO 27001 建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。
4	人員管理安全	(1)組織是否要求所有承包者，遵守組織之資安規範，並應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。 (2)組織是否對委外承包者定義且傳達於聘用終止或變更後，資訊安全責任	(1)T-Road 開發案具有正式委外契約，並於專案過程中宣達 T-Road 維運機關應有的資訊安全管理。 (2)委外人員均簽妥保密協議，離職後協議仍然有效。 (3)符合左項要求，故發生機率低(甚少發生)。	嚴重影響	低度風險	T-Road維運機關已取得 ISMS驗證證書，T-Road平臺已參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		及義務仍保持有效，並落實執行。				
5	系統獲取、開發及維護	開發過程中的安全要求，應納入新系統開發過程要求，如： (1)對使用者宣稱身分之信賴等級要求，以便導出使用者鑑別之要求。 (2)存取權限提供及授權過程，營運使用者以及特權或技術使用者。 (3)告知使用者及操作者其職責及責任。 (4)涉及資產所需的保護需要，特別是關於可用性、機密性、完整性者。	(1)T-Road 開發過程符合案具有正式委外契約，並於專案過程中宣達 T-Road 維運機關各項資訊安全管理要求。 (2)委外人員均簽妥保密協議，離職後協議仍然有效。 (3)整體開發過程之安全，包含程式安全、開發環境安全，均由 T-Road 維運機關全程監督。 (4)T-Road 委外開發契約內，已有不得包含使用危害國家資通安全產品之要求。 (5)T-Road 平臺上線前，將進行各項安全檢測，避免漏洞遭利用。 (6)T-Road 契約內已包含資訊安全功能要求，	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺已參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(5)來自營運過程之要求，如交易存錄及監視、不可否認性要求。 (6)其他安全控制措施規定之要求，例如存錄(Log)及監視之介面或資料洩露偵測系統。 (7)網路傳輸安全協議。 (8)外部購買之產品，應針對是否涉及使用危害國家資通安全產品情形。 (9)評估及實作該系統最終軟體/服務堆疊之產品安全組態調校的可用指引。	並納入驗收條件。 (7)符合左項要求，故發生機率低(甚少發生)。			

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(10)界定接受產品之準則，例如在功能性方面，給予保證達到已識別之安全				
6	軟體開發過程安全	組織是否界定軟體開發規則包含： (1)開發環境之安全。 (2)軟體開發安全、程式語言安全編碼原則 (3)軟體開發方法之安全。 (4)所用每一程式語言之安全編碼指導綱要。 (5)設計階段內安全要求。 (6)計畫期程內之安全查核點。 (7)保全資料庫。 (8)版本控制之安全。	(1)T-Road 開發過程已符合行政院 SSDLC 要求，並定期向 T-Road 維運機關報告各項安控落實事宜。 (2)系統開發過程均定期報告專案進度及是否有異常狀況。 (3)符合左項要求，故發生機率低(甚少發生)。	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺已參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(9)必要之應用系統安全知識。 (10)開發者避開、找出及修補脆弱性之能力。				
7	系統變更管理	組織是否議定安全變更要求，如： (1)維持所議定之變更授權等級的紀錄。 (2)確保變更是由經授權的使用者提出。 (3)審查控制措施與完整性程序，以確保其未被變更所破壞。 (4)識別所有需要改善的軟體、資訊、資料庫個體及硬體。 (5)識別及查核安全關鍵程式碼以將已知安全弱點	(1)T-Road 維運機關依照 ISMS 管理標準，定義各項系統功能需求變更，各項變更均須透過維運機關核准後方可進行。 (2)若變更後發現可能造成系統弱點，亦有退版機制。 (3)符合左項要求，故發生機率低。(甚少發生)	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺已參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		可能性降至最小。 (6)在變更工作開始前，應有詳細的提案，且獲得正式核准。 (7)變更實作之前，經授權的使用者應接受該變更。 (8)確保在每次完成變更後，就更新系統文件組，並將舊文件歸檔或作廢。 (9)維持所有軟體更新作業的版本控制。 (10)維持所有變更請求的稽核日誌。 (11)確保作業文件與使用者程序根據需				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		要作適切變更。 (12)確保在正確的時機實作變更，且不會擾亂所涉及的營運過程。				
8	開發環境保全	組織應針對系統委外開發之環境，進行安全控管，包含： (1) 系統處理、儲存及傳輸之資料的敏感性。 (2) 適用之外部及內部要求事項，如來自法規或政策。 (3) 支援系統發展組織已實作之安全控制措施。 (4) 環境內	(1)T-Road 開發過程之開發環境，符合 ISMS 資安管理要求，並全程接受維運機關監督。 (2)符合左項要求，故發生機率低。(甚少發生)	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺已參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		工作人員之可信賴性。 (5) 與系統發展有關之外包程度。 (6) 不同發展環境間區隔之需要。 (7) 對發展環境存取之控制措施。 (8) 對環境及存於其中程式碼變更之監視。 (9) 備份儲存於保全之異地位置。 (10) 環境中資訊搬遷進入及移出之控制措施。				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
9	軟體委外開發監督	應針對軟體委外開發業務，應有進行下列安全要求： (1) 版權使用、程式碼所有權及智慧財產權 (2) 安全設計、程式編碼及測試實務之契約要求。 (3) 對開發者提供已發現之軟體威脅。 (4) 交付產品之品質及精確性的驗收測試。 (5) 可接受安全及隱私權品質。 (6) 提供已應用足夠測試以避免	(1)T-Road 委外開發契約已針對各項軟、硬體交付項目之智慧財產、安全性、弱點檢測等，進行要求。 (2)交付驗收全程接受維運機關監督。 (3)符合左項要求，故發生機率低。(甚少發生)	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺已參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		交付時包含惡意內容的證據。 (7) 提供已應用足夠測試以防衛免於出現已知脆弱性的證據。 (8) 如源程式碼不再可用時之協議。 (9) 稽核開發過程及控制措施之契約權利。 (10) 用以產生交付產品之編譯環境的有效文件。 (11) 負責適用法律之遵循及控制措施效				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		率之查證證據。				
10	系統驗收	組織針對系統驗收測試應包括資訊安全要求之測試，並嚴守保全系統開發實務。如利用諸如程式碼分析工具或弱點掃瞄系統等自動化工具，並查證有關安全缺陷的修補。	(1)T-Road 委外開發契約已針對各項軟、硬體交付項目之弱點檢測等，進行要求。 (2)交付驗收全程接受維運機關監督。 (3)符合左項要求，故發生機率低。(甚少發生)	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺已參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。
11	測試資料保護	組織應針對測試項目進行安全規劃： (1) 適用於運作之應用系統的存取控制程序亦宜適用於測試應用系統。 (2) 每次複製作業之資訊到測試環境均	(1)T-Road 進行測試之測試步驟、環境等，均符合 ISMS 要求。 (2)測試項目之通過均全程受維運機關監督。 (3)交付驗收全程接受維運機關監督。 (4)符合左項要求，故發生機率低。(甚少發生)	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺將參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		宜經過個別授權。 (3) 在測試完成後宜立即將作業之資訊從測試環境中清除。 (4) 宜保存開發作業資訊的複製與使用，以便提供稽核日誌。				
12	供應者安全要求	組織應針對服務供應者可取得之資訊資產進行保護，如： (1) 識別及文件化組織將允許委外供應者存取之資訊型式，例如IT服務、後勤、公用設	(1) T-Road 運行相關服務供應者，均具有正式服務契約，載明各項資訊安全要求。 (2) 服務提供過程均由維運機關全程監督。 (3) 為機關內各項資訊資產可被接受之使用方式，均符合 ISMS 要求。 (4) 測試項目之通過均全程受維運機關監督。	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺將參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		施、財務服務、IT基礎建設組件等。 (2) 管理供應者關係之標準化過程及生命週期。 (3) 界定不同供應者將被允許之資訊存取型式，並監視及控制其存取。 (4) 每一資訊型式及存取型式之最低資訊安全要求，以作為基於組織營運需求及要求以及其風險剖繪	(5) 符合左項要求，故發生機率低。(甚少發生)			

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		與個別供應者協議之基礎。 (5) 對每一供應者及型式存取型視監守已建立資訊安全要求的過程及程序，包括第三方審查及產品驗證。 (6) 準確度及完全性控制措施以確保資訊或各方提供資訊處理之完整性。 (7) 適用於供應者義務型式以保護組織資訊。				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(8) 與供應者存取有關的處置事故及應變，包括組織與供應者雙方之責任。 (9) 必要時之回復及應變安排，以確保資訊或各方提供資訊處理之可用性 (10) 涉及獲取組織關於適用政策、過程及程序之認知訓練。 (11) 與供應者互動的組織人員關於基於供				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		應者型式及供應者存取組織系統 (12) 資訊安全要求及控制措施之情況將由雙方簽署一書面協議。 (13) 管理必要之資訊、資訊處理設施及其他任何需要移動之物品的傳送，並確保整段傳送期間之資訊安全。				
13	委外供應者安全協議	組織應針對委外供應者進行相關安全協議要求： (1) 存取資訊方法描述。	(1) 專案委外契約內已載明各項資訊安全要求。 (2) 委外廠商提供之各項軟、硬體應符合智慧	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺將參考國際標準ISO 27001建置資安管理制度，

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(2) 依據組織分級方案的資訊分類與分級，對映組織本身資訊存取分級方案與供應者分級方案。 (3) 鑑別法律及法規要求，包括資料保護、智慧財產權及版權，以及將如何確保落實。 (4) 每一契約方實作協議的包括存取控制、績效審查、監視、通報及稽	財產等相關法令要求。 (3) 委外廠商存取組織內之資訊資產均應經過核准。 (4) 合約內已要求委外廠商之供應不得使用危害國家資通安全產品情形 (5) 符合左項要求，故發生機率低。(甚少發生)			並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		核等整套控制措施之義務。 (5) 資訊可接受之使用的規定，必要時包括不可接受之使用。 (6) 明確的存取或組織之收資訊應者供人員清單，或是供應者人員或存取收組織資訊的授權以及移除授權之程序或情形。 (7) 與特定有契約之資關訊安政策。				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(8) 事故管理要求及程序（特別是事故修補期間之通知及合作）。 (9) 特定程序及資訊安全要求之訓練及認知要求，例如事故回應、授權程序。 (10) 分包之相關法規，包括需要作之實控制措施。 (11) 相關協議夥伴，包括資訊安全議題之聯絡窗口。 (12) 如有篩選要				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		求，若篩選未完成或其結果導致懷疑或關切時，包括執行篩選及通知程序之供應者人員的責任。 (13)缺陷解決及衝突解決過程。 (14)供應者定期交付控制措施有效性的獨立報告之義務，與即時修正報告內所提出相關議題之協議。 (15)供應者遵循組織安全要求之義務。				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		(16)缺陷解決及衝突解決過程。 (17)供應者定期交付控制措施有效性的獨立報告之義務，與即時修正報告內所提出相關議題之協議。 (18)供應者遵循組織安全要求之義務。				
14	供應鏈安全要求	組織應針對資通服務及產品供應鏈，進行安全管理： (1) 除一般供應者關係資訊安全要求以外，界定適用於資訊及通訊	(1) 專案委外契約內已載明各項資訊安全要求。 (2) 委外廠商提供之各項軟、硬體應符合智慧財產等相關法令要求。 (3) 委外廠商存取組織內之資訊資產均應經過核准。	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺將參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		技術產品或服務之獲取的資訊安全要求。 (2) 對資訊及通訊技術服務，若供應者分包部份提供給組織的資訊及通訊技術服務，則要求供應者對整個供應鏈傳播組織之安全要求。 (3) 對資訊及通訊技術產品，若上述產品包括採購自其他供應者之組件，則要求供應者	(4) 合約內已要求委外廠商之供應不得涉及使用危害國家資通安全產品情形。 (5) 符合左項要求，故發生機率低。(甚少發生)			

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		對整個供應鏈適切的安全實務。 (4) 實作監視過程及可接受之方法，以驗證交付之資訊及通訊技術產品及服務 (5) 嚴守指定的安全要求。 (6) 實作識別維護性功能重要的產品或服務組件，因此在組織外部建立時需要增加注意及安全性，特別是若最高層				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		供應者將產品或服務組件層面委外至其他供應者。 (7) 取得關鍵組件及其起源在整個供應鏈可被追溯的保證。 (8) 取得交付之資訊及通訊技術產品如預期運作，無任何非預期或非所欲特徵的保證。 (9) 界定組織及與供應者間關於供應鏈與任何潛在議題及危害等資				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		訊共享之規則。 (10)實作資訊及通訊技術組件生命週期及可用性與相關安全風險的特定管理過程。包括管理組件由於供應者不再營運而不再可用，或供應者由於技術進展而不再提供上述組件等之風險。				
15	交付管理	組織應有文件化程序，針對交付項目進行管控： (1) 組織應監視服	嚴重影響	低度風險	低度風險	T-Road平臺將參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		務效能等級以查核委外協議的遵守程度。 (2) 按協議要求審查供應者產出的服務報告，並安排定期的進度會議。 (3) 實施供應者的稽核，若可取得，同時審查獨立稽核報告，以及發現問題之後續行動。 (4) 按協議與任何支援指導綱要與程序之要求，提供關於				該項要求。

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		資訊安全事故的資訊，並審查該資訊。 (5) 審查與付所交相服務的安關全事件、運作之問題、失效、失誤及追蹤中斷等的第三方稽核日誌與紀錄。 (6) 解決並管理所有已識別出的問題。 (7) 審查供應者與其本身供應者之供應關係資訊安全層面。 (8) 確保供應者維				

項次	評估項目		風險發生機率	風險嚴重性	風險地圖	風險處理方法
		持足夠的服務容量以及設計可行之計畫，確保重大服務失效或災害之後能維持議定之服務持續等級				
16	資安事故管理	組織是否要求所有委外承包者，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。	(1) 維運機關內各項資訊資產可被接受之使用方式，均符合ISMS 要求。 (2) 委外專案執行受維運機關監督。	嚴重影響	低度風險	T-Road維運機關已取得ISMS驗證證書，T-Road平臺將參考國際標準ISO 27001建置資安管理制度，並通過外部第三方驗證，應可滿足該項要求。