本文件使用說明:

1. 在「網路安全實務與社會」的課程中，諮詢小組在下半學期會組成資安健檢團服務組織。目前規劃多場諮詢會議的核心目的，是在幫助諮詢小組能夠釐清組織想解決的資安問題，並考量自身的能力與組織的負荷程度後提出解決方案或指引。本文件中諮詢會議的次數、形式、訪談對象皆為參考，教學團隊可視實際與組織互動的情況靈活調整。
2. 本文件為資安院基於參考國外網路安全診所聯盟建議之資源(如:MIT 線上課程)與社會科學研究法調查法之經驗，初步設計的諮詢會議討論指引。請讀者注意：這份指引的題項敘述，並不包含真實問題。
3. 在真實訪談與晤談場合時，發問者需要考量到前後文的脈絡，產出真實的問題。也需要確保提出的問題不會冒犯到受訪者，使其感到不舒服。
4. 訪談綱要並非固定不變，而是可依各小組需求進行客製化。我們鼓勵教學團隊根據自身專業領域和健檢內容，靈活調整訪談題項，包含修改、增加或刪減問題。我們也很期待各校之團隊若後續有針對本指引或範例中的建議，給予我們建議與反饋，我們會持續調整，並運用於未來的課程中。
5. 本指引預計會持續推出新版本。使用時請留意文件的版本號，以確保您參閱到的是最新的內容。對於此文件有任何問題歡迎聯繫俐霏（lfkung@nics.nat.gov.tw）。

1、初始會議（建議次數：1次）

1. 與會者：諮詢小組、授課教師、助教、服務對象的資安專案小組成員（或連繫窗口）

會議內容	建議諮詢小組要了解的內容（從觀察、提問中掌握）	諮詢小組真實提問的敘述範例
雙方相見歡	● 雙方自我介紹、說明目的與來由 ● 找出組織中誰是專案的負責人？誰有決策權？要推行資安方案要找誰？ ● 雙方保密的義務，學生隱去本名的必要性。	e.g.，對於我們接下來要討論的內容，有哪些需要特別注意保密的部分嗎？
服務對象介紹自己的核心業務	● 組織內有哪些重要的核心業務？各個核心業務的承辦人是誰？ ♦ 若有多個業務，最重要的是哪個? □ 界定範圍 ♦ 可以多留意在諮詢小組可以解決的資安業務 ● 核心業務使用到的系統有哪些? ♦ 核心系統的使用情境（如果可以現場 demo 更好）：組織內部如何使用？外部人員如何使用？ ♦ 系統目前委外/自營? 原始碼是否可以取得? ♦ 系統的負責人?	e.g.， ● 想請教貴單位最主要的核心業務是什麼？ ● 在執行這些核心業務時，您們主要使用哪些資訊系統？ 能否簡單說明一下這些系統的使用流程？
諮詢小組了解服務對象想解決的資安問題	● 組織想參加健檢的動機與脈絡： ♦ 什麼契機之下想提升組織資安？ ♦ 之前有接觸過哪些資安單位或是活動嗎？接觸後有什麼樣的想法？ ♦ 目前組織在資安上面臨的挑戰？	e.g.，想請教____（組織名）__是在什麼樣的契機下想要提升資安環境？
教學團隊說明未來的規劃	● 了解組織忙的時間：哪些時間適合開會？哪些時間適合落實資安解決方案？ ● 確認組織對於之後的會議地點、頻率以及要配合的事項都同意 ● 確定下一次會議的時間與地點與討論的項目	

2、 需求訪談會議（建議次數：2-3 次）

（1） 訪談對象：核心業務承辦人/若組織有涉及捐款業務，也可詢問該業務承辦人

會議內容	諮詢小組要掌握的內容（從觀察、提問中掌握）	諮詢小組真實提問的敘述範例
盤點業務風險	● 了解組織的核心業務細節： ♦ 這個業務本身的重要性為何？ ♦ 這個業務處理的是什麼事情？ ♦ 這個業務會觸及到哪些人員？ ♦ 這個業務的主要產出為何？ ● 了解業務風險： ♦ 您覺得這份業務在執行的過程中，可能對於組織有哪些資安風險? ♦ 如果這個風險發生了，會造成哪些方面的影響或後果？（經濟方面/社會觀感面/情緒方面/個人資料方面） ♦ 過往有從捐款人的回饋中，收到資安相關的建議或是回饋嗎？ ♦ 組織內是否已經有針對可能的風險或建議回饋做應對措施或規劃？	E.g.，謝謝您剛才對於目前業務內容的介紹，接著想邀請您更多分享，您覺得這份業務在執行過程中，可能有哪些資安風險，若不幸發生可能會影響到組織?
了解核心業務系統的安全性	● 盤點核心業務會使用到的系統: ♦ 請問在執行這個工作的過程中，會使用到哪些資訊系統或設備呢？ ♦ 這個資訊系統或設備的主要用途為何？ ♦ 這個資訊系統或設備會記載什麼重要資訊？ ♦ 這個資訊系統目前是誰在管理的呢? ● 了解實際系統操作狀況(備份/權限管理/帳號密碼設定)，洞察可能的資安風險： ♦ 您平時都如何操作這個系統呢? ♦ 系統的資料是如何備份的呢?多久備份一次呢？	

	♦ 除了您之外，還有其他人可以操作這個系統嗎? 是如何決定這些人可以操作這個系統的呢?	

（2） 訪談對象：秘書長(或其他組織內決策高層）

會議內容	諮詢小組要掌握的內容（從觀察、提問中掌握）
了解組織整體業務的理念與價值	● 了解組織脈絡與核心理念
決策者的資安意識	● 資安風險意識（個人/組織）： ♦ 您覺得組織可能會面臨哪些資安風險？ ♦ 組織有收到過釣魚郵件嗎？如果有，大約收到多少封，多久收到一次？ ● 資安事件應變意識： ♦ 如果組織不幸遇到資安事件，組織會如何應對？您覺得可能造成的損失有哪些？ ● 積極度: ♦ 您過往有參與過資安相關的培訓嗎？如果有，是什麼時候？當時培訓的內容是什麼呢？ ♦ 您平常會關注資安相關的事件嗎?最近有印象的資安事件是什麼呢?
了解主管機關與利害關係人的期待	● 您過往有跟其他非營利組織討論過資安議題嗎？可以跟我們更多分享當時討論的內容嗎？ ● 過往有跟主管機關討論過組織的資安狀況嗎?或是尋求資安相關的協助?若有，是誰呢?也想邀請您更多與我們分享當時討論的內容。 ● 過往董監事會有討論過資安相關議題嗎？當時討論的內容是什麼呢？ ● 您覺得組織的各方利益關係人，對於組織的資安期待是什麼?

會議內容	諮詢小組要掌握的內容（從觀察、提問中掌握）
了解組織資安任務分配	● 組織目前有規劃資安預算嗎？若有，預算大約多少呢？ ● 組織目前有資安專案小組嗎？若有，資安小組人數有多少呢？ ● 組織目前在資安業務的作為為何呢？ ● [optional]您多久會收到一次關於機構網絡安全狀況的簡報?

（3） 訪談對象：MIS（若組織有配置資訊人員，可以問）

會議內容	諮詢小組要掌握的內容（從觀察、提問中掌握）
詢問日常工作內容與資訊系統狀況	● 了解 MIS 平常的工作內容： ♦ 請您跟我們介紹一下您在資訊單位的工作有哪些？ ♦ 請問您值班的一天通常如何度過？（prompt: 大概大概就好，不用很細節） ♦ 就我們所知，基金會裡的重要系統包含_(自評表提及之內容)__，請問您平常工作有觸及這些系統或設備嗎？ ● 了解組織各式系統的安全控制設計： ♦ 請問這些系統和應用軟體有設置哪些資安防護功能的設計？例如：使用者驗證（登入）、存取控制、加密和日誌記錄等 ♦ 是由誰負責管理這些功能的設定？ ♦ 目前組織所有的資訊系統和操作軟體版本是否都是最新的呢？

會議內容	諮詢小組要掌握的內容（從觀察、提問中掌握）
資訊人員資安意識	● 您過往有參與過資安相關的培訓嗎？ ● 如果有，是什麼時候？ ● 當時培訓的內容是什麼呢？ ● 培訓後，您是否有將學到的內容應用於組織?
資安事件應變知識	● 了解組織目前資安事件應變流程： ♦ 如果您在網路監控中看到任何可疑情況，您知道該聯繫誰以及如何聯繫嗎？ ♦ 如果您注意到您的電腦或系統遭受攻擊，您會如何回應？ ♦ 組織目前有訂定作業流程可以參考嗎?

3、解決方案提案會議

1. 與會者：諮詢小組、助教、服務對象的資安專案小組成員（或連繫窗口）
2. 會議目標：了解目前提案的可行性，並基於服務對象提出的組織現況調整方案。

會議內容	諮詢小組要掌握的內容（從觀察、提問中掌握）
諮詢小組呈現目前要解決的問題與範圍	● 諮詢小組簡潔的呈現先前的健檢結果，聚焦要解決的問題 ♦ 詢問組織有沒有要補充或是釐清的地方?
提案可能的解決方向或指引	● 諮詢小組從問題延伸出解決方案，若有餘裕可提 2-3 個解決方案。 ♦ 詢問組織對於方案的看法，有沒有哪些解方是因為現實考量而窒礙難行的? ♦ 當組織提出困難點時，諮詢小組可以試著更多詢問這個困難點的原因。 ♦ 腦袋轉得快的話，可以同步微調解方，並詢問服務對象的想法。

4、解決方案落實會議

1. 與會者：諮詢小組、助教、服務對象的資安專案小組成員（或連繫窗口）

2. 會議目標：討論諮詢小組提出的解方可以如何落實，並討論最終解方定案的目標。

會議內容	諮詢小組要掌握的內容（從觀察、提問中掌握）
諮詢小組呈現調整後的方案	● 呈現調整後的解決方案，詢問組織有沒有要補充或是釐清的地方?
諮詢小組與服務對象討論方案落實的詳細規畫	● 解決方案在落實上是否有窒礙難行之處? ● 鼓勵組織發展落實解方的具體行動計畫。計畫內容可包含： ♦ 方案落實的具體實行時程、任務與負責人 ♦ 盤點落實解方所需要的資源