

Secpaas 操作手冊(填答問卷者)

目錄

I.	系統概述.....	2
II.	資安評級填答單位管理(UNIT).....	3
A.	填答單位透過收到問券填答通知信，透過「填寫問卷」連結，可以進行問券填寫的動作。.....	3
B.	除了透過連結，也可透過入口(HTTPS://RATINGS.SECAAS.ORG.TW)進行填答.....	3
C.	填寫問卷.....	4
D.	若問卷具有「資安曝險分析」.....	11
	狀態: 已送出申請，表示已送出，待審核結果.....	11
E.	問卷結果-填答明細.....	11
F.	問卷結果-比較分析.....	12
G.	問卷結果-顧問建議.....	14
H.	可指派同一公司人員填寫與檢視.....	14
I.	填答人員可新增複測問卷.....	17

I. 系統概述

本系統共有三個後台，分別為：

- 資安評級平台管理(platform)
- 資安評級租戶管理(tenant)
- 資安評級填答單位管理(unit)

◎資安評級平台管理(platform)

為工研院方管理其下之租戶、管理資安問卷題庫、管理線上之資安評級問卷範本及查看各單位之問卷填寫紀錄等等。

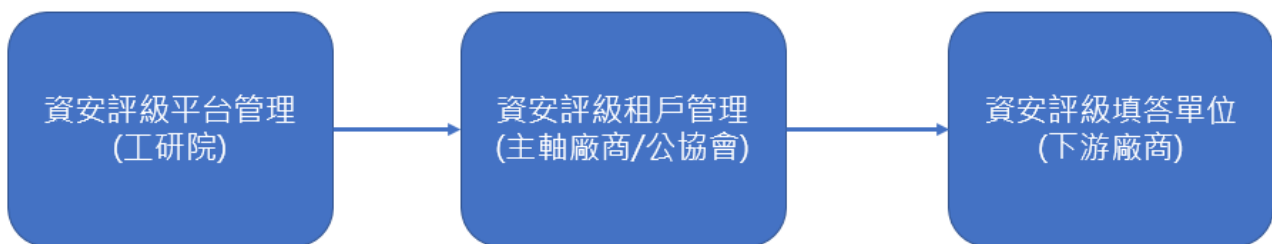
◎資安評級租戶管理(tenant)

為租戶方(主軸廠商/公協會)管理其下填答單位、問卷管理(引用問卷範本)、查看問卷填寫紀錄等等。

◎資安評級填答單位管理(unit)

為填答單位方接收租戶方提出填寫問卷要求、填寫問卷、查看問卷填答明細&比較分析。

下圖為管理階層示意：



II. 資安評級填答單位管理(Unit)

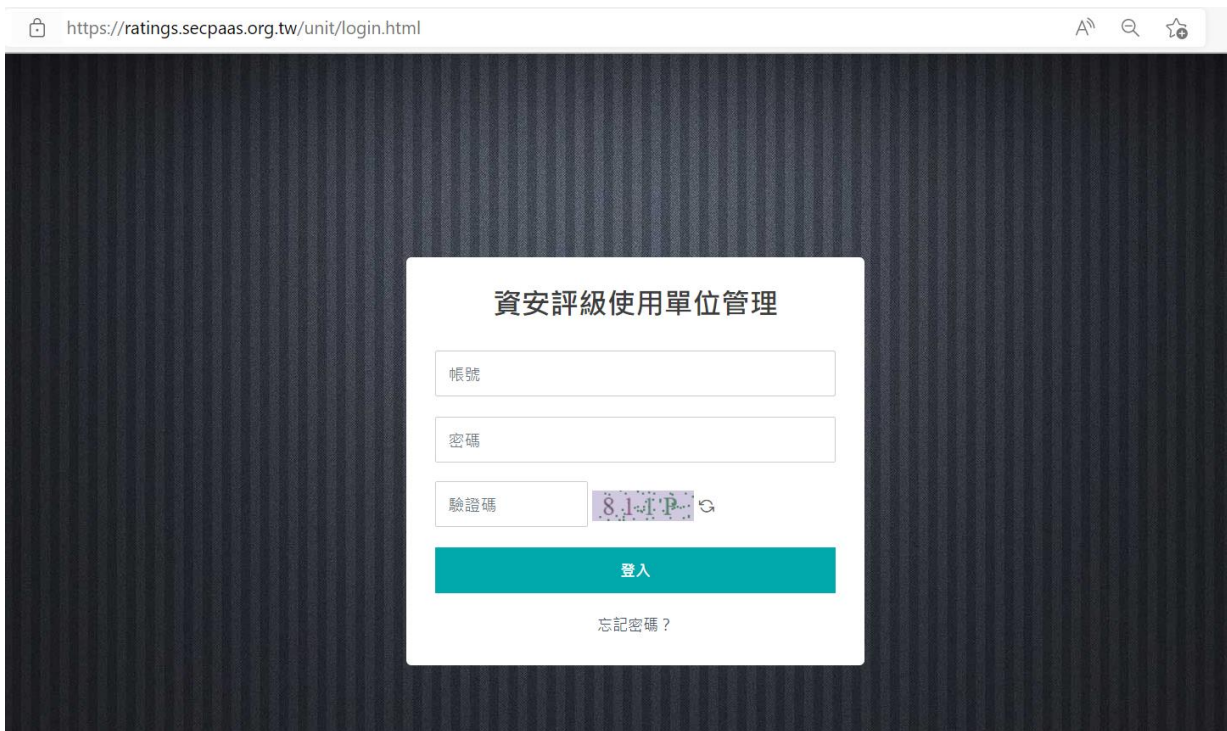
A. 填答單位透過收到問券填答通知信，透過「填寫問卷」連結，可以進行問券填寫的動作。



B. 除了透過連結，也可透過入口(<https://ratings.secpaas.org.tw>)進行填答



若未取得密碼，可透過忘記密碼的方式，設定新密碼。



C. 填寫問卷

說明：填答單位在此可查看所有租戶向自己提出的問卷填寫要求。點擊填寫問卷，即可開始填寫作答。

被指派之問卷 / 被指派之問卷

搜尋條件

關鍵字 狀態 查詢

問卷名稱	租戶問卷描述	租戶	狀態	填寫日期	完成時間	
112年SIG輔導問卷-171題	SIG 輔導問卷	工業技術研究院	未繳交成績			填寫問卷

4 筆

- 進入後會先看到使用條款，使用條款內容設定請見【租戶：系統基本設定】。

※ 使用條款

本網站由「SecPaas資安整合服務平台」所經營。本網站重視每一個使用者所享有的服務，特此說明本網站的使用政策，以保障您的權益。請您細讀本使用條款之內容：

1. 關於《使用條款》

1) 在您決定使用本網站所提供的服務(以下簡稱本服務)前，請仔細閱讀本使用條款。您必須在完全同意以下條款的前提下，才能使用本服務。本使用條款與其他附加條件或其他特殊條款相矛盾時，以附加條件或特殊條款為準。

2) 本網站有權於任何時間修改或變更本使用條款之內容，您應經常查看以瞭解您當前的權利及義務。若您於本網站為任何修改或變更本使用條款後仍繼續使用本服務，視為您已同意接受本使用條款之修改及變更。

2. 服務內容

1) 本服務的具體內容由本網站根據實際情況提供，並對其所提供之服務擁有最終解釋權。

2) 本服務係透過網際網路提供您各項網路資訊服務，您必須自行配備上網所需的各項電腦設備，並承擔所需的費用。

3. 授權

在本使用條款的約束下，本網站僅此授予您有限、僅供個人使用、非商業用途（家裡或工作中使用）、非專屬和不可轉讓的使用本服務。

4. 使用者的行為

您在使用本網站服務過程中，必須遵循以下原則：

(a) 遵守中華民國有關的法律和法規；

(b) 遵守所有與網路服務有關的網路協定、規定和程式；

(c) 不得為任何非法目的而使用網路服務系統；

(d) 不使用任何設備、軟體或程序，干擾或試圖干擾本網站、本網站之正常運作；

(e) 不允許侵入、強行入侵、接通、使用或企圖侵入、接通、使用本網站伺服器及未經本網站對您發出許可的任何資料區；

- 若先前有答題記錄，則系統會詢問是否引用先前的作答紀錄並將評級結果繳交給租戶，即可不用再次做同一份問卷內容。

是否引用先前的成績？

您最近已有填答完成之紀錄：

分數	67.26
評級	C
檢測時間	2022/06/30 15:00:54

是否將此成績上傳給租戶？
(即可不用再次作答相同問卷)

取消 確定

Step1.開始答題。

- 具有「不適用」、「否」、「是」選項: 「不適用」, 目前此題目與企業無相關性、「否」, 企業還未做到此題資安合規。由上至下為答題進度條、資安評級場域、題號、題目、選項、下一題按鈕。每題皆須選擇答案後才可進入下一題。

113年SIG輔導問卷-NIST-800-171 - 02750963 - 工業技術研究院

1 / 171

請文字說明，貴企業哪個場域要做資安合規

* 資安評級場域

請填寫貴公司廠區名稱 / 辦公地點

1 【題目分類：防護能力 / 存取控制】組織可透過授權帳戶或程式來限制使用者、設備(包含其他資訊系統)存取系統

不適用

否

是

為每位使用公司重要電腦的員工提供使用者帳號和密碼

只將使用者帳號和密碼提供給有權使用該系統的員工

員工離職後立即禁用其使用者帳號和密碼

佐證備註

佐證備註請盡可能地描述

- 具有「複選」：若沒有適合的答案，該題視為未選擇，可直接填寫下一題。

8 / 171

8 【題目分類：識別能力 / 風險管理】分開管理不受供應商支持的產品（例如，壽命終止），並根據需要進行限制以降低風險。

- 有掌握已End of Service產品的風險破口
- 有在組織的網路中隔離End of Service的產品
- 有規劃End of Service的產品執行升級、更換或報廢的時程

佐證備註

佐證備註請盡可能地描述

判斷您讀過條件:必須按上一題、下一題、題號

上一題 下一題

選擇題號 1-20 21-40 41-60 61-80 81-100 101-120 121-140 141-160 161-171

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Step2.若問卷具有「資安曝險分析」，請注意填寫內容，如下：

171 / 171

171 【題目分類：防護能力 / 系統和資訊完整性】利用沙箱來偵測或阻止潛在的惡意電子郵件。

不適用

否

是

有設置電子郵件沙箱分析環境

電子郵件經過沙箱測試確定安全後才允許通過

依據備註

備註

寫完最後一題，需填寫掃描資訊

申請掃描

* 公司名稱

* 主網域名稱

方法1：主網域名稱不帶端口取網址www後方的文字
例：公司網站網址為「www.itri.org.tw」，主網域名稱輸入「itri.org.tw」。方法2：抓取公司的 mail @後置的文字
例：mail為「nico@itri.org.tw」，主網域名稱輸入「itri.org.tw」。* 主網域名稱只能填寫主網域名稱 (maindomain)，填寫子網域名稱 (subdomain) 會無法正確進行掃描服務

* 期望掃描日期

請寫主網域，勿填寫subdomain

掃描日期不可填今日，需大於今日

技術窗口：蔡先生 03-5914502 / itri820511@itri.org.tw

Step3.答題完畢即會提示作答完畢。點擊 OK 就會回到【被指派之問卷】列表頁。

33 / 33

33 針對內部開發、內部

風險領域。

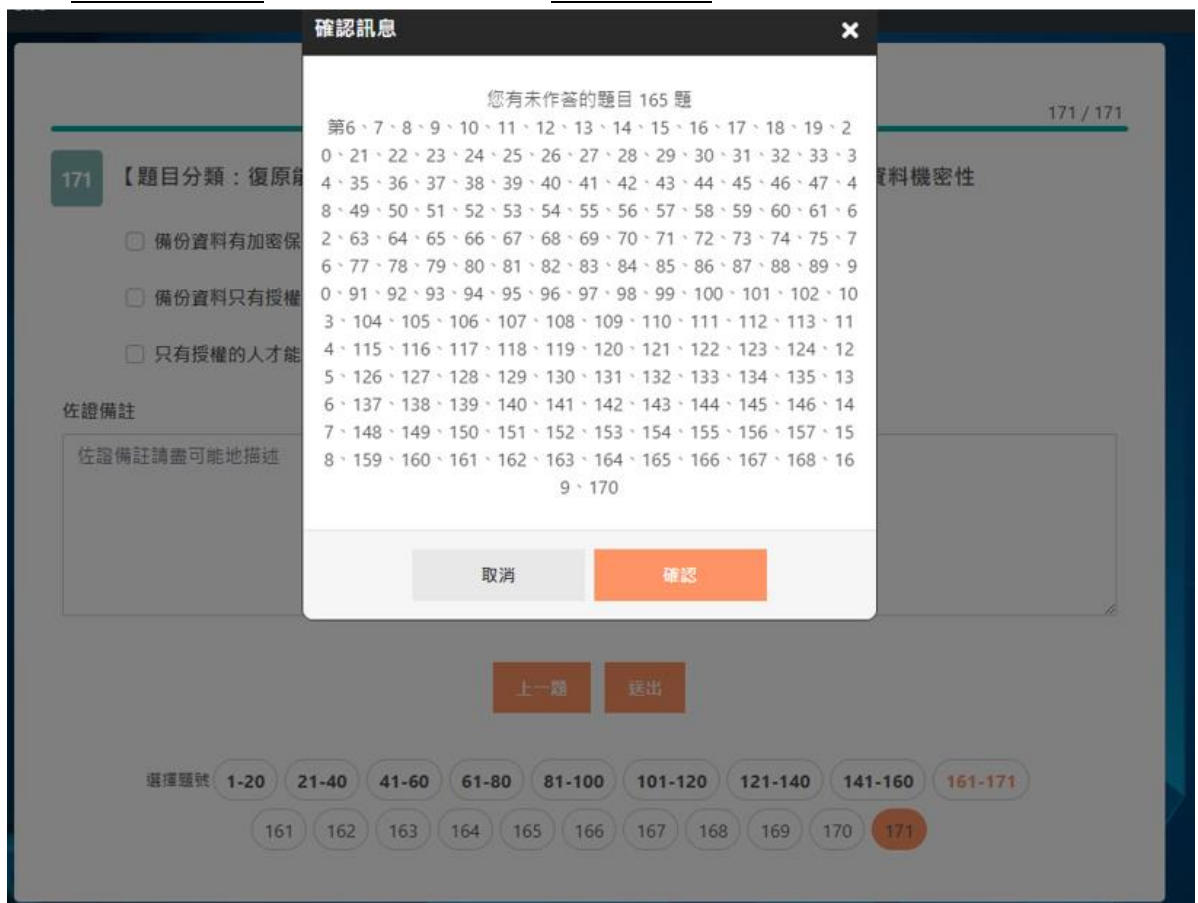
組織軟體都有執行

每個軟體更新都有

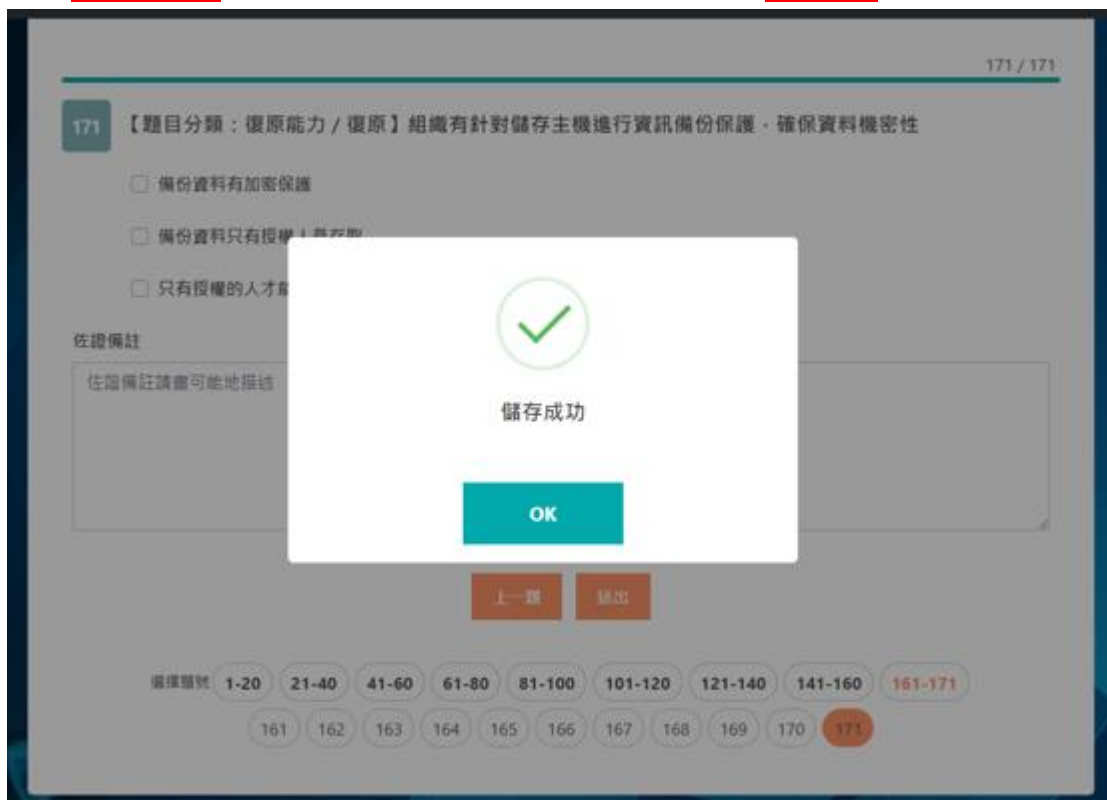
填寫完畢

OK

- 出現未作答的題目，則您需要點選相關未作答題目，並審慎檢視與作答。



- 出現儲存成功，則您寫的問卷題目已儲存，但您還有未填完的題目。



Step4.答題完畢後，於被指派之問卷頁面可點選資安掃描服務申請按鈕，即可看到掃描狀況。

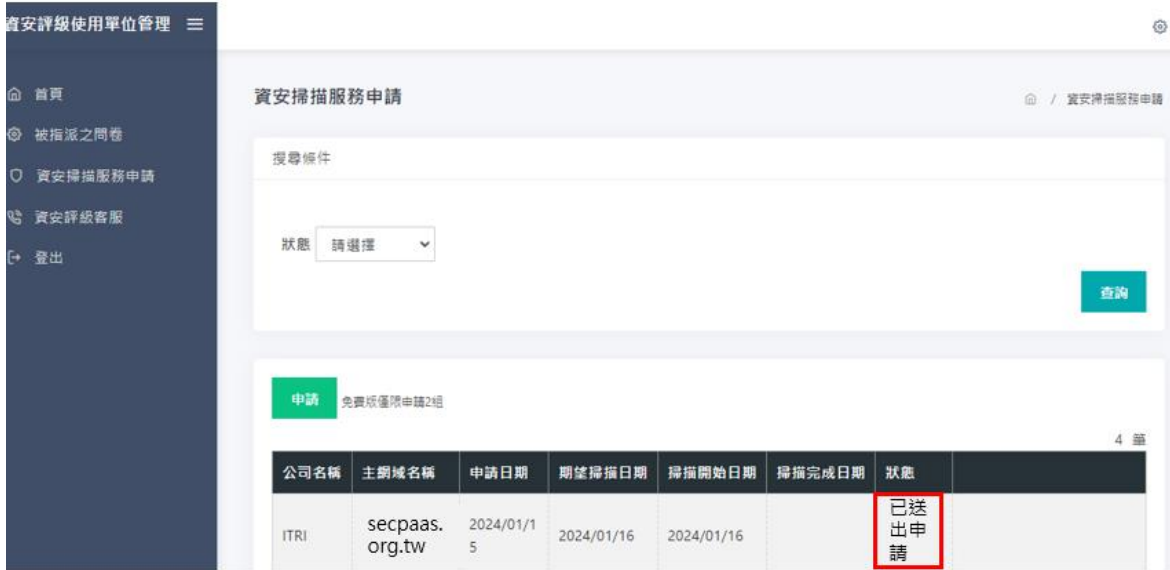


Step5.答題完畢後，於被指派之問卷頁面可點選填答明細與比較分析按鈕，即可看到成績。(同時平台端、租戶端的問卷填答紀錄也可查看到成績)。



D. 若問卷具有「資安曝險分析」

➤ 狀態: 已送出申請，表示已送出，待審核結果



E. 問卷結果-填答明細

Step1.顯示填答結果

➤ 有資安評級場域: 點選填答明細按鈕，可逐題查看方才所填的結果、資安場域地點、分數與評級。



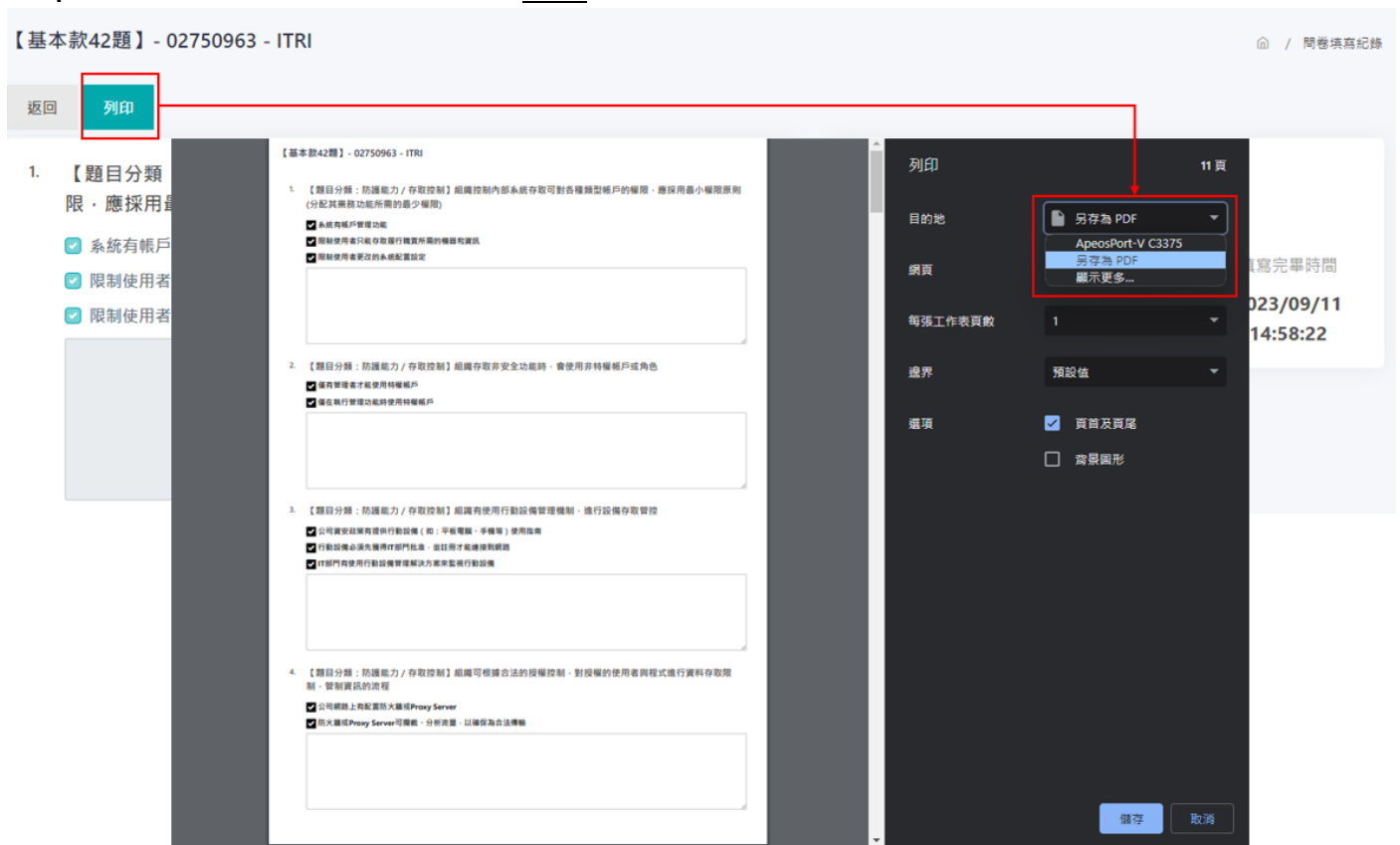
➤ 無資安評級場域: 點選填答明細按鈕，可逐題查看方才所填的結果、分數與評級。



Step2. 點選訂正後按鈕，可逐題查看顧問所填的結果、分數與評級



Step3.若要輸出或轉成 PDF，則可按列印按鈕。



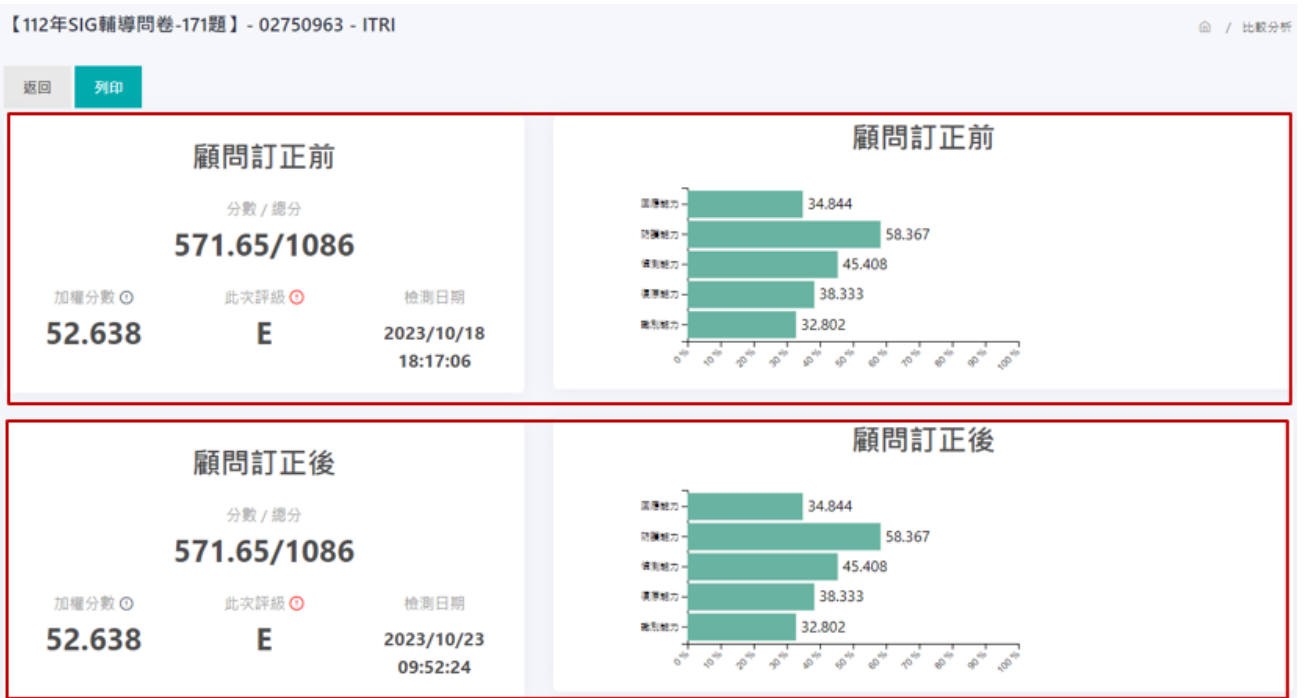
F. 問卷結果-比較分析

Step1.點選比較分析按鈕。

問卷名稱	租戶問卷描述	公司名稱	統一編號	狀態	完成時間	分數	評級	
112年SIG輔導問卷-171題	SIG 輔導問卷	ITRI	02750963	已繳交成績	2023/09/22 14:10	53.927	E	填答明細 比較分析 顧問建議
評級問卷	此份是由工研院開放給廠商填答之完整評級問卷 (第三次填答)	ITRI	02750963	已繳交成績	2023/09/22 14:07	52.638	E	填答明細 比較分析

Step2. 檢視訂正前(填答單位)與訂正後(顧問)之分數、評級與各項能力分數，若顧問還未審

核，則訂正後就沒資料。



Step3.往下滑，點選詳細分析按鈕，可檢視(訂正前、後)填答單位之各項能力的分數與評級。

詳細分析(顧問訂正前) 詳細分析(顧問訂正後) 改善建議(顧問訂正前) 改善建議(顧問訂正後) 比較分析(顧問訂正前) 比較分析(顧問訂正後)

回應能力(顧問訂正前)

分類	分數	評級
事件通報	34.844	E

防護能力(顧問訂正前)

Step4.點選改善建議按鈕，可檢視分數較低的項目顯示，其包含所參考標準、風險係數、具體改善建議。

詳細分析(顧問訂正前) 詳細分析(顧問訂正後) 改善建議(顧問訂正前) 改善建議(顧問訂正後) 比較分析(顧問訂正前) 比較分析(顧問訂正後)

參考標準: CMMC modification of Draft NIST SP 800-171B 3.12.1e, CIS Controls v7.1 20.2, NIST SP 800-53 Rev 4 CA-8

種類名稱: 定義和管理安全控制 風險係數: ▲▲▲▲▲

建議組織應該建立必要的復原措施，這樣就可以在遇到安全問題時繼續保護資訊安全。這意味著，即使某種安全解決方案或系統出現問題，也有其他機制可以代替且保持安全。此外，組織需要備援設備，以確保整個系統在失敗時可以自動切換到其他設備來繼續提供保護，例如：如果防火牆失效了，系統會自動切換到其他的防火牆，直到問題得到解決。通過設置備援方案，組織就可以繼續運作，因為資訊安全任務仍可以正常執行。建議導入資安解決方案：自動化滲透測試工具

參考標準: FAR Clause 52.204-21 b.1.J, NIST SP 800-171 Rev 1 3.1.1, CIS Controls v7.1.1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11

種類名稱: 建立系統存取要求 風險係數: ▲

建議組織建立處理敏感資料的流程，透過流程可以確定哪些是敏感資料並實施存取控制來保護，包括規定誰可以接收、傳輸、儲存和銷毀這些資料，以及確保它們在所有時候都受到嚴格控制。其中流程還需考慮實體和數位資料妥善的保護和管理處理。建議導入資安解決方案：資通安全威脅偵測管理(SOC)服務

提供建議資安解決方案

G. 問卷結果-顧問建議

Step1.點選比較分析按鈕。

問卷名稱	租戶問卷描述	公司名稱	統一編號	狀態	完成時間	分數	評級	
112年SIG輔導問卷-171題	SIG 輔導問卷	ITRI	02750963	已繳交成績	2023/09/22 14:10	53.927	E	填答明細 比較分析 顧問建議
評級問卷	此份是由工研院開放給廠商填答之完整評級問卷 (第三次填答)	ITRI	02750963	已繳交成績	2023/09/22 14:07	52.638	E	填答明細 比較分析

Step2.檢視顧問各別題目之輔導建議。

112年SIG輔導問卷-171題 - 02750963 - ITRI (顧問訂正後)

返回
列印

1 【題目分類：防護能力 / 存取控制】組織可透過授權帳戶或程式來限制使用者、設備(包含其他資訊系統)存取系統

	使用單位作答	輔導建議
為每位使用公司重要電腦的員工提供使用者帳號和密碼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
只將使用者帳號和密碼提供給有權使用該系統的員工	<input type="checkbox"/>	<input type="checkbox"/>
員工離職後立即禁用其使用者帳號和密碼	<input type="checkbox"/>	<input type="checkbox"/>

佐證備註

此次分數
52.638 → **52.638**

此次評級
E → E

填寫時間
2023/10/18
06:06:17

H. 可指派同一公司人員填寫與檢視

Step1.租戶指派主要填答者進行填寫，主要填答者可指派同一公司人員進行填寫，請選擇「問卷作答群組」選擇人員

被指派之問卷 / 被指派之問卷

搜尋條件

關鍵字 狀態

[查詢](#)

問卷名稱	租戶問卷描述	租戶	狀態	填寫日期	完成時間	
評級問卷	smepass評級問卷	ITRI	已繳交成績	2024/01/11 10:08	2024/01/11 10:46	填答明細 比較分析
112年SIG輔導問卷-171題	SIG 輔導問卷	工業技術研究院	未繳交成績	2024/01/11 09:27		填寫問卷 問卷協作群組

Step2.選擇「新增」

設定填答名單

搜尋條件

關鍵字

新增

全部寄送問卷填答通知



無資料

Step3.選擇相關人員，並按下儲存

新增使用單位



請勾選答單位協作人員

16 筆

<input type="checkbox"/>	統一編號	公司名稱	聯絡人姓名	聯絡人Email
<input type="checkbox"/>	02750963	ITRI		
<input checked="" type="checkbox"/>	02750963	ITRI		aquancai5@gmail.com
<input checked="" type="checkbox"/>	02750963	ITRI		aquancai9@gmail.com
<input type="checkbox"/>	02750963	工研院		
<input type="checkbox"/>	02750963	工研院		
<input type="checkbox"/>	02750963	工研院		
<input type="checkbox"/>	02750963	ITRI		
<input type="checkbox"/>	02750963	ITRII		
<input type="checkbox"/>	02750963	ITRI		
<input type="checkbox"/>	02750963	ITRI		

1 2 > Last

取消

儲存

Step4.點選「寄送問卷填答通知」，請相關人員進行填寫

新增填答單位協作人員

搜尋條件

關鍵字

公司名稱	統一編號	聯絡人姓名	聯絡人Email		
ITRI	02750963	蔡育註	aquancai5@gmail.com	<input type="button" value="刪除"/>	<input type="button" value="寄送問卷填答通知"/>
ITRI	02750963	蔡育註	aquancai9@gmail.com	<input type="button" value="刪除"/>	<input type="button" value="寄送問卷填答通知"/>

2 筆

Step5.被指派填寫的填答者，可從「填答問卷」進行填寫

aquancai9@gmail.com

被指派之問卷

搜尋條件

關鍵字 狀態

問卷名稱	租戶問卷描述	租戶	狀態	填寫日期	完成時間		
評級問券	smepass評級問卷	ITRI	已繳交成績	2024/01/11 10:08	2024/01/11 10:46	<input type="button" value="填答明細"/>	<input type="button" value="比較分析"/>
服務業問卷_TsaiTest_改Category	改Category3	工業技術研究院	已繳交成績	2023/12/12 14:33	2023/12/12 14:34	<input type="button" value="填答明細"/>	<input type="button" value="比較分析"/>
112年SIG輔導問卷-171題	SIG 輔導問卷	工業技術研究院	未繳交成績	2024/01/11 09:27		<input type="button" value="填寫問卷"/>	
基本款42題	基本款42題	工業技術研究院	已繳交成績	2023/12/08 17:23	2023/12/12 13:09	<input type="button" value="填答明細"/>	<input type="button" value="比較分析"/>
基本款42題	基本款42題	工業技術研究院	未繳交成績	2023/12/20 22:11		<input type="button" value="填寫問卷"/>	

5 筆

Step6.最終填答結果，主要填答者與被指派填答者，都可從「填答明細」與「比較分析」功能查看填答結果



I. 填答人員可新增複測問卷

Step1.請選擇「新增問卷(複測)」



問卷名稱	租戶問卷描述	租戶	狀態	填寫日期	完成時間	
基本款42題	基本款42題	工業技術研究院	未填寫	2024/01/11 10:08	2024/01/11 10:46	填寫問卷 問卷協作群組

Step2.請勾選相對應複測問卷，並按下儲存

查詢 ✕

請勾選問卷 1 筆

<input type="checkbox"/>	問卷名稱	租戶問卷描述
<input type="checkbox"/>	基本款42題	113年複測問卷(42題)

取消 儲存

Step3.即可進行「複測」！

新增問卷(複測) 2 筆

問卷名稱	租戶問卷描述	租戶	狀態	填寫日期	完成時間	
基本款42題	113年複測問卷(42題)	工業技術研究院	未填寫			填寫問卷 問卷協作群組
基本款42題	基本款42題	工業技術研究院	未填寫			填寫問卷 問卷協作群組