TLP: WHITE

# 勒索軟體防護成熟度自評說明

## -使用美國 CISA CSET RRA 軟體模組

Version 1.0

2021 年 7 月 6 日

TLP: WHITE

# 1. 簡介

為了因應日益猖獗的勒索軟體攻擊，美國國土安全及基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA) 的資訊安全評估工具 (Cyber Security Evaluation Tool, CSET) 已納入新模組 – 勒索軟體防護機制自評工具(Ransomware Readiness Assessment, RRA)，協助組織診斷自身資安防護機制是否健全與足夠應對勒索軟體攻擊。

CSET 為一評估工具之平台，可協助組織根據不同的成熟度評估模組 (如: ACET、CMMC、EDM、RRA)，系統性的評估組織資訊安全性。而 RRA 則是 CSET 的新增模組，專門用來評估組織應對勒索軟體時的防禦與恢復能力， RRA 亦納入不同等級的勒索軟體威脅防護成熟度，藉以評估組織應對勒索軟體攻擊的狀況。評估結果以透過儀表板的圖形與表格方式呈現評估結果，其中亦包含摘要與細節，提供增強防護之建議。

RRA 評估模組以下列十大防護面向進行組織自評:

1. Robust Data Backup (DB), 備份機制:
   檢視備援政策的適當性，如採用定期與自動化資料與系統設定備份，並以安全方式儲存 (加密)等。

2. Web Browser Management and DNS Filtering (BM), 瀏覽器管理與 DNS 過濾機制:
   檢視瀏覽器管理與 DNS 過濾機制，即時過濾與可疑惡意域名的連線。

3. Phishing Prevention and Awareness (PP), 釣魚威脅防治:
   檢視反釣魚防護機制措施，並定期於組織內進行提升釣魚威脅意識之教育訓練。

4. Network Perimeter Monitoring (NM), 網路邊界監控:
   檢視網路邊界監控機制，採用可結合威脅情資與入侵指標(IoC)之網路防護設備，並即時監控與防堵可疑網路流量。

5. Asset Management (AM), 資產管理:
   檢視資產管理政策，如定期盤點更新組織資產設備，並移除已不被支援的軟體與硬體設備等。

6. Patch and Update Management (PM), 更新修補管理:
   檢視設備軟體與韌體更新管理機制，如定期置換已不被支援的 OS、應用程式及硬體設備等。

7. User and Access Management (UM), 使用者存取控管:
   檢視使用者權限管理政策，如採取帳戶最小權限原則、密碼強度政策及監控分析使用者異常行為等。

8. Application Integrity and Allowlist (AI), 應用程式安全性:
   訂定組織可允許使用之應用程式清單，並定期檢視應用程式檔案的完整性等。

9. Incident Response (IR), 資安事件應變:
檢視資安事件處理計畫，並定期進行資安事件演練。

10. Risk Management (RM), 風險管理:
檢視組織提升資安威脅意識政策，如定期進行教育訓練與演練等。

RRA 評估項目分為 ‘Basic’、‘Intermediate’與 ‘Advanced’ 三個成熟度等級，旨在提供組織了解目前各等級防護成熟度與改善措施之優先度。建議會員可依序完成 ‘Basic’等級之所有措施之後再持續完善 ‘Intermediate’與 ‘Advanced’ 之防護措施。相關各等級對應之問題可於 ‘Deficiency Report’中檢視，建議措施細節可參照 ‘RRA report’。

## 2. 安裝與使用說明

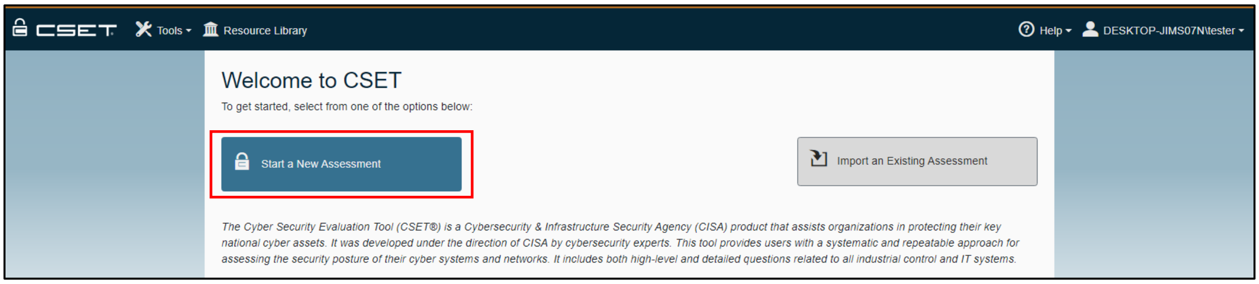
美國 CISA 已透過 GitHub 釋出含有 RRA 模組之 CSET 自評工具，TWCERT/CC 建議企業組織利用此工具進行自我評估。以下為安裝步驟與使用說明。

1. 透過美國 CISA 官網或 GitHub 下載並安裝 CSET。下載網址請參考:
美國 CISA 官網: https://us-cert.cisa.gov/ics/Downloading-and-Installing-CSET
GitHub 網站: https://github.com/cisagov/cset/releases

2. 啟動 CSET 應用程式。

3. 點選 ‘Start a New Assessment’ 建立新評估專案，如圖 1 所示。

圖 1、建立新評估專案



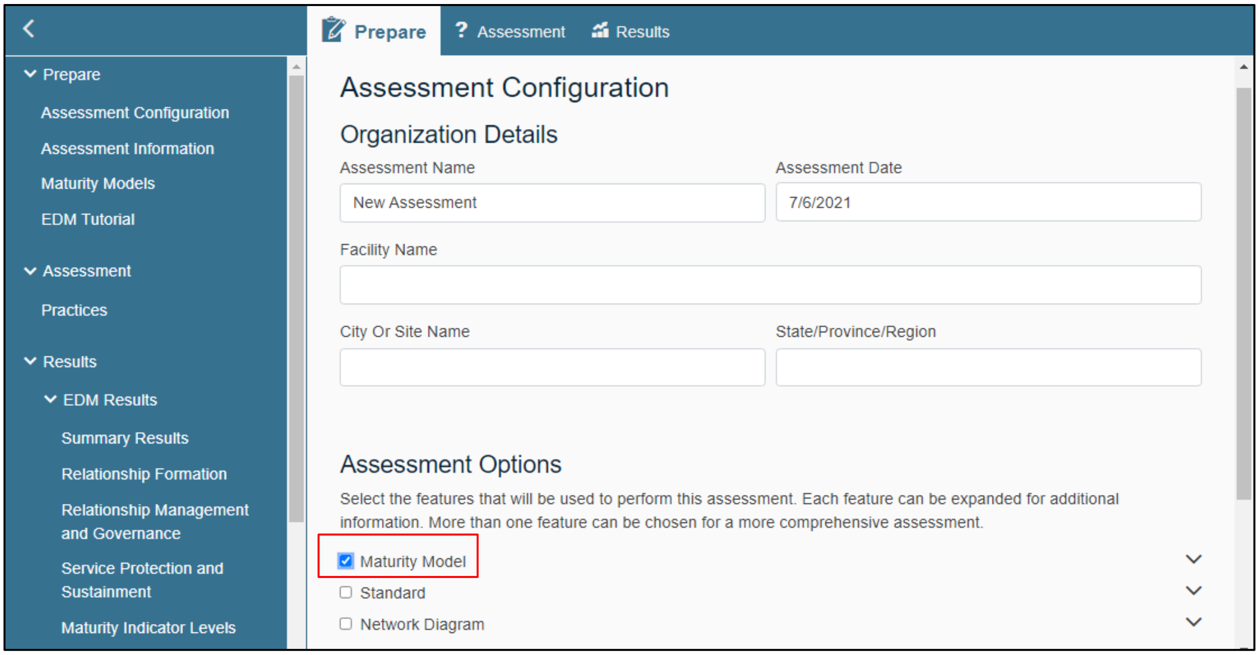
Welcome to CSET

To get started, select from one of the options below:

*The Cyber Security Evaluation Tool (CSET®) is a Cybersecurity & Infrastructure Security Agency (CISA) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of CISA by cybersecurity experts. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.*

4.	於 Assessment Options 勾選 ‘Maturity Model’並點擊 ‘Next’ 按鈕，如圖 2 所示。

圖 2、選取 Maturity Model



Assessment Configuration

Organization Details

Assessment Name: New Assessment

Assessment Date: 7/6/2021

Facility Name:

City Or Site Name:

State/Province/Region:

Assessment Options

Select the features that will be used to perform this assessment. Each feature can be expanded for additional information. More than one feature can be chosen for a more comprehensive assessment.

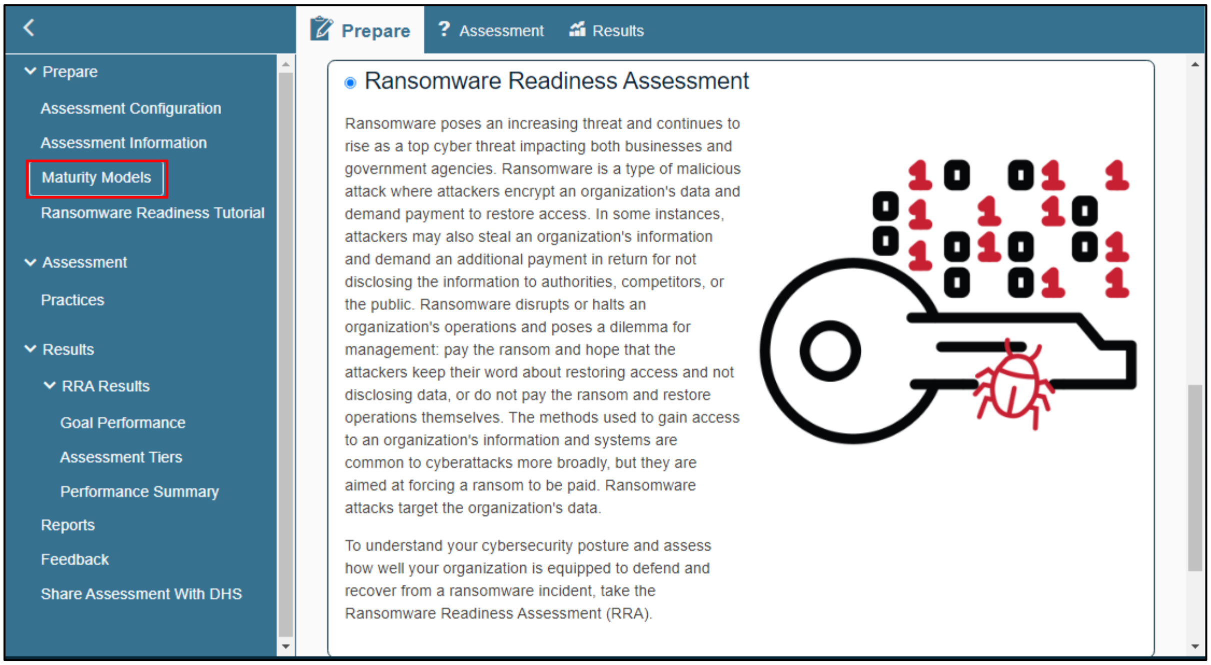
☑ Maturity Model

☐ Standard

☐ Network Diagram

5.	從左邊選單點選 ‘Maturity Models’，並勾選 Ransomware Readiness Assessment 項目，點擊 ‘Next’ 按鈕，如圖 3 所示。

圖 3、選取 Ransomware Readiness Assessment



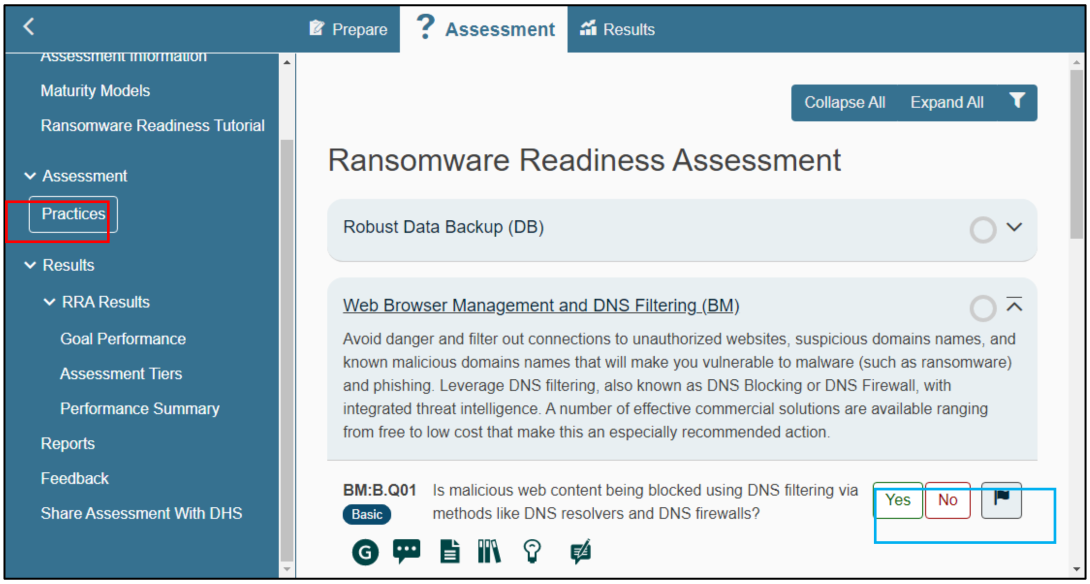
● Ransomware Readiness Assessment

Ransomware poses an increasing threat and continues to rise as a top cyber threat impacting both businesses and government agencies. Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. In some instances, attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. Ransomware disrupts or halts an organization's operations and poses a dilemma for management: pay the ransom and hope that the attackers keep their word about restoring access and not disclosing data, or do not pay the ransom and restore operations themselves. The methods used to gain access to an organization's information and systems are common to cyberattacks more broadly, but they are aimed at forcing a ransom to be paid. Ransomware attacks target the organization's data.

To understand your cybersecurity posture and assess how well your organization is equipped to defend and recover from a ransomware incident, take the Ransomware Readiness Assessment (RRA).

6.　　從左邊選單點選 ‘Assessment’ 的 ‘Practices’ 子項目後，可根據 RRA 之十大項目(表一的 DB、BM、PP、NM、AM、PM、AI、UM、IR、RM)的細節問題進行自評 (藍框處): ‘符合’ 點選 ‘YES’、 ‘不符合’點選 ‘NO’、或是不確定則點擊 ‘旗幟’，完成後點擊 ‘Next’ 按鈕，如圖 4 所示。

圖 4、自評畫面



Ransomware Readiness Assessment

Robust Data Backup (DB)

Web Browser Management and DNS Filtering (BM)

Avoid danger and filter out connections to unauthorized websites, suspicious domains names, and known malicious domains names that will make you vulnerable to malware (such as ransomware) and phishing. Leverage DNS filtering, also known as DNS Blocking or DNS Firewall, with integrated threat intelligence. A number of effective commercial solutions are available ranging from free to low cost that make this an especially recommended action.

BM:B.Q01 Basic　Is malicious web content being blocked using DNS filtering via methods like DNS resolvers and DNS firewalls?

7.　　評估結果畫面，包含各大項防護措施的達成度 (長條圖與表格)，點擊 ‘Next’ 按鈕，如圖 5、圖 6 所示。

圖 5、各項評估結果 1，(長條圖) (示意圖)

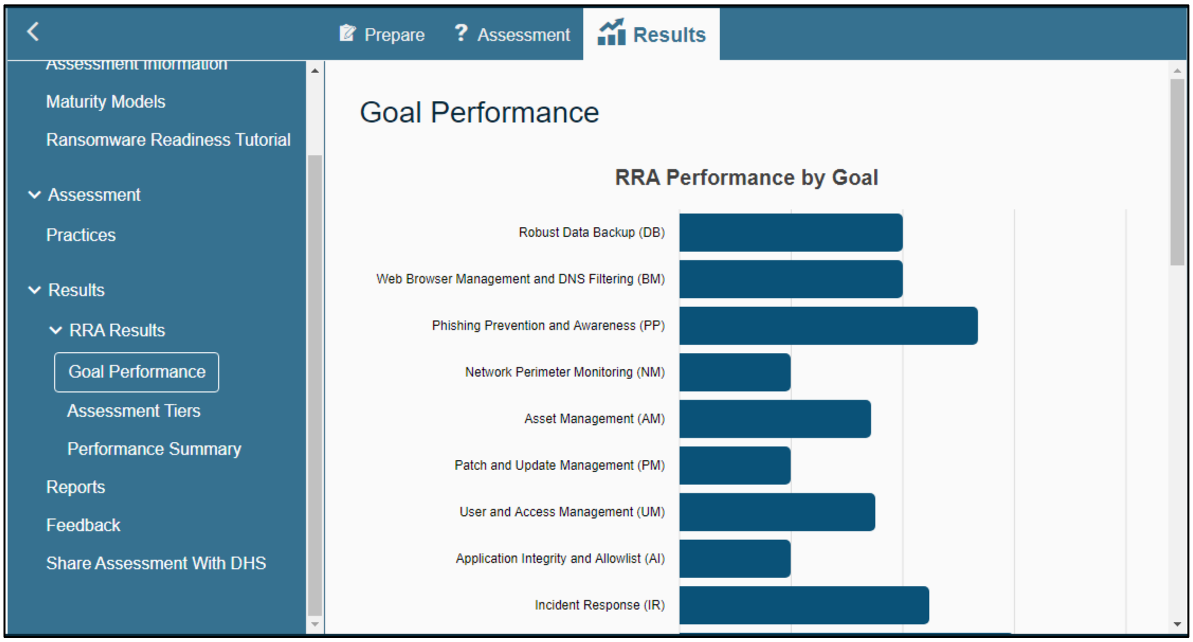
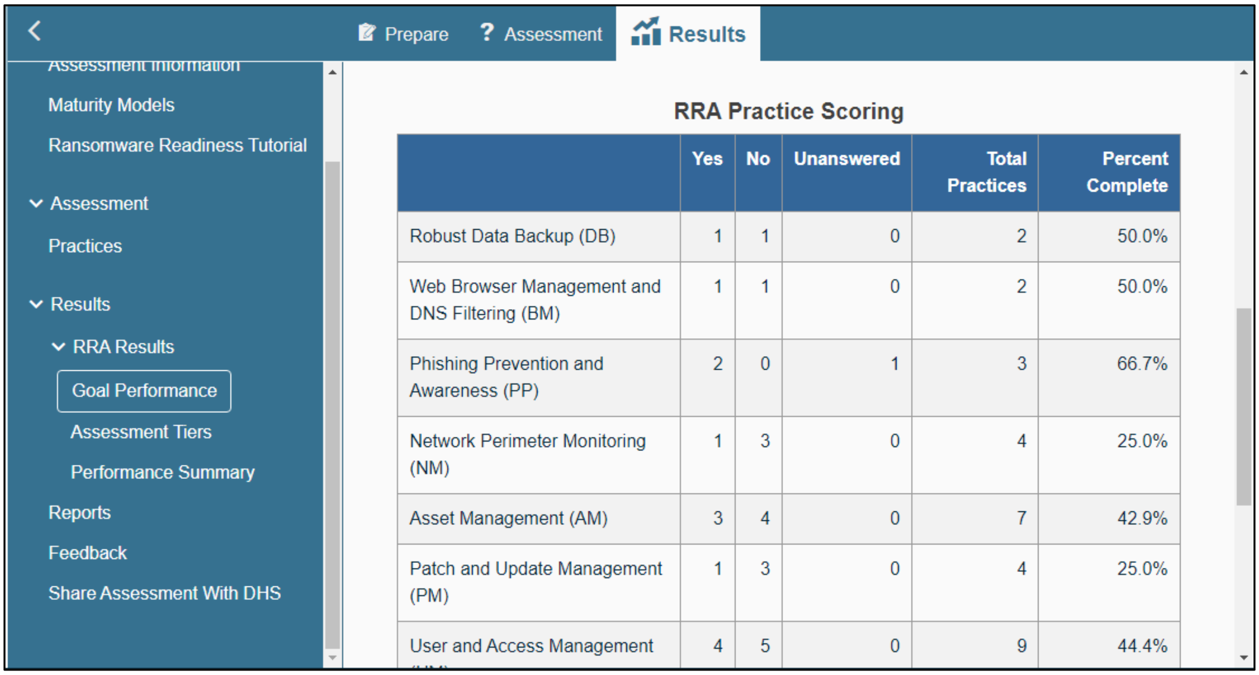

Prepare
? Assessment
Results
Assessment Information
Maturity Models
Ransomware Readiness Tutorial
Assessment
Practices
Results
RRA Results
Goal Performance
Assessment Tiers
Performance Summary
Reports
Feedback
Share Assessment With DHS
Goal Performance
RRA Performance by Goal
Robust Data Backup (DB)
Web Browser Management and DNS Filtering (BM)
Phishing Prevention and Awareness (PP)
Network Perimeter Monitoring (NM)
Asset Management (AM)
Patch and Update Management (PM)
User and Access Management (UM)
Application Integrity and Allowlist (AI)
Incident Response (IR)

圖 6、各項評估結果 2、(表格) (示意圖)

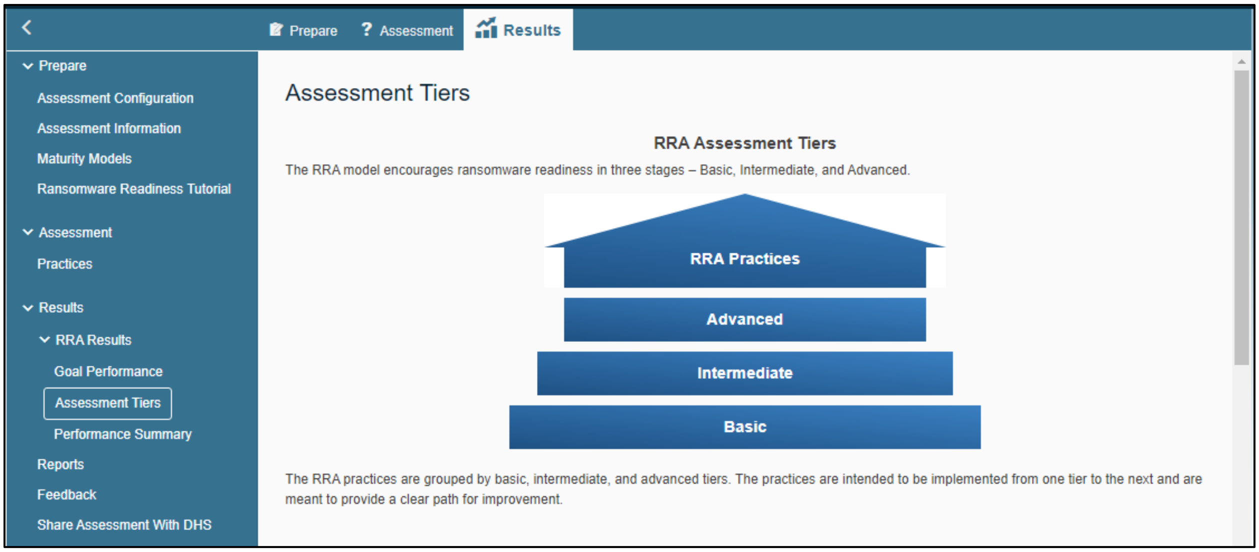


RRA Practice Scoring

| | Yes | No | Unanswered | Total Practices | Percent Complete |
|---|---|---|---|---|---|
| Robust Data Backup (DB) | 1 | 1 | 0 | 2 | 50.0% |
| Web Browser Management and DNS Filtering (BM) | 1 | 1 | 0 | 2 | 50.0% |
| Phishing Prevention and Awareness (PP) | 2 | 0 | 1 | 3 | 66.7% |
| Network Perimeter Monitoring (NM) | 1 | 3 | 0 | 4 | 25.0% |
| Asset Management (AM) | 3 | 4 | 0 | 7 | 42.9% |
| Patch and Update Management (PM) | 1 | 3 | 0 | 4 | 25.0% |
| User and Access Management | 4 | 5 | 0 | 9 | 44.4% |

8. RRA 成熟度等級(圖 7)，以及各級防護成熟度評估結果(圖 8、圖 9)。點擊 'Next'。

圖 7、RRA 成熟度分級圖



Assessment Tiers

RRA Assessment Tiers

The RRA model encourages ransomware readiness in three stages – Basic, Intermediate, and Advanced.

The RRA practices are grouped by basic, intermediate, and advanced tiers. The practices are intended to be implemented from one tier to the next and are meant to provide a clear path for improvement.

圖 8、‘Basic’、‘Intermediate’、‘Advanced’各級項目成熟度 (長條圖) (示意圖)

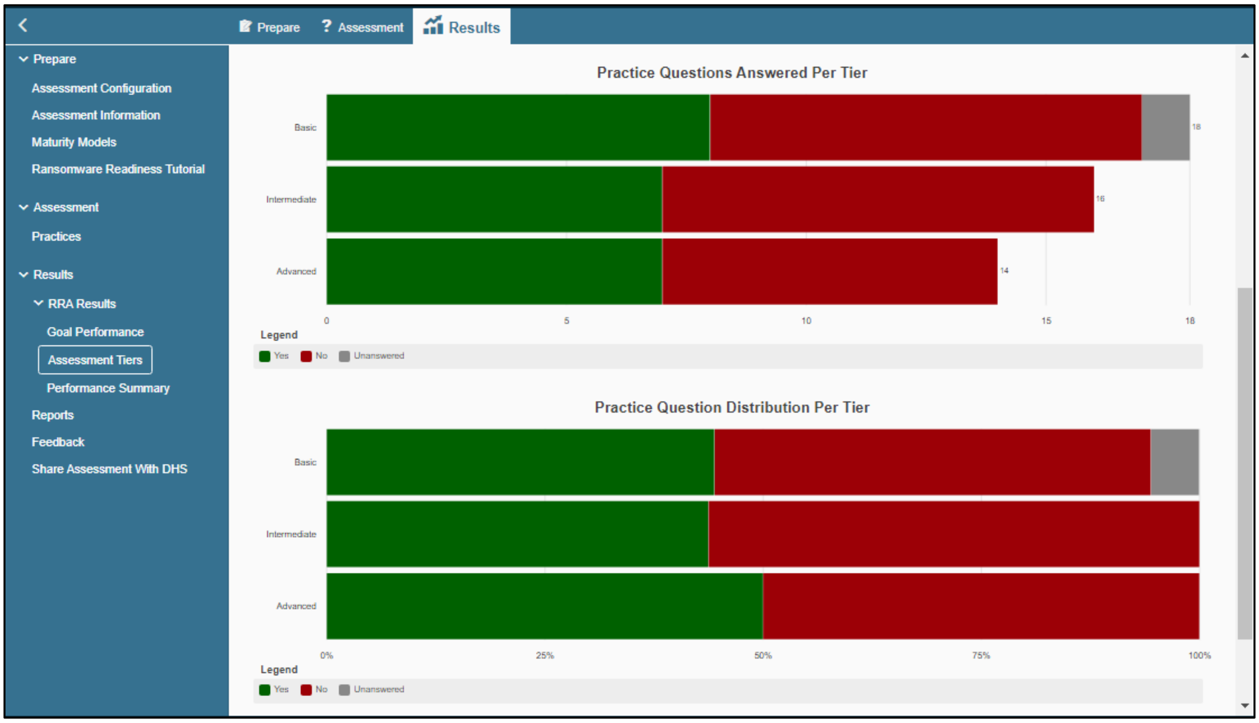
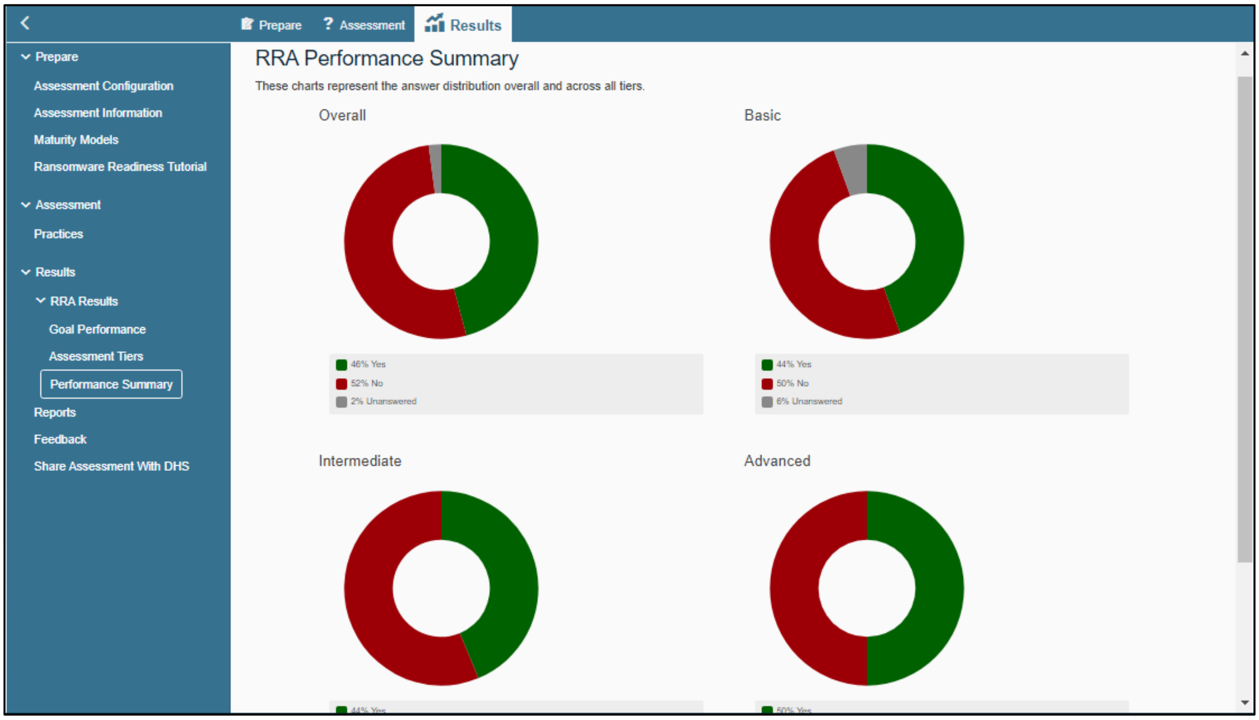


圖 9、‘Basic’、‘Intermediate’、‘Advanced’各級項目成熟度 (圓餅圖) (示意圖)

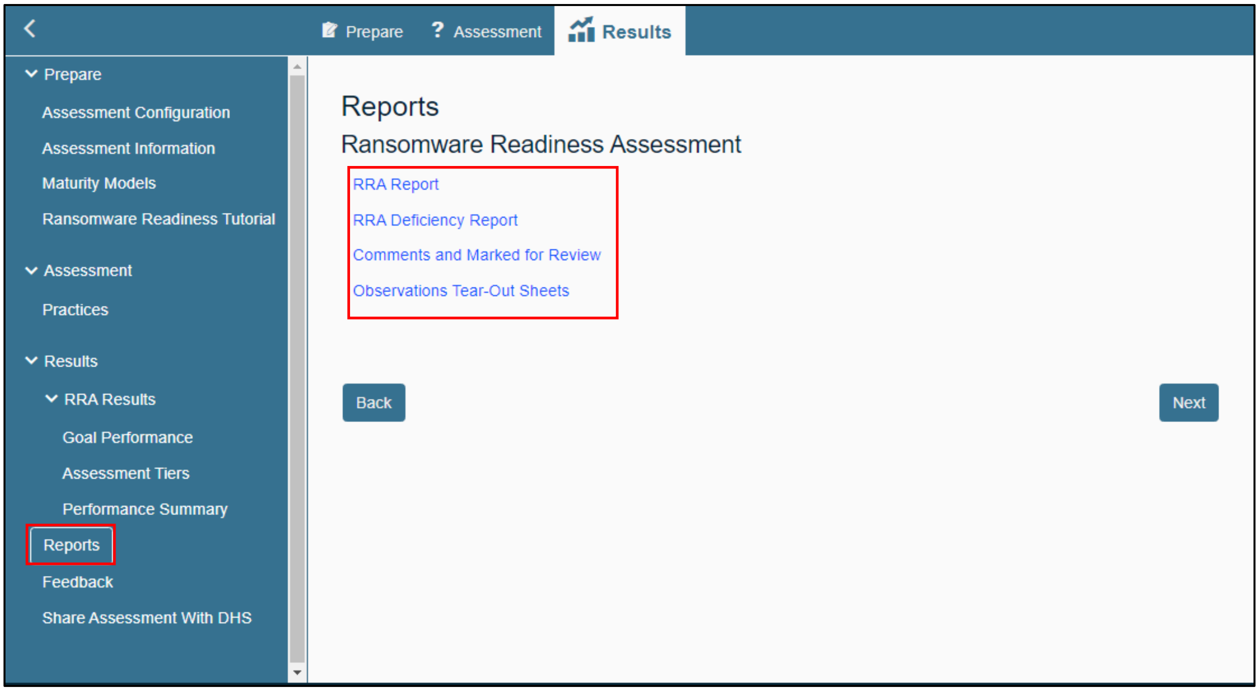


RRA Performance Summary

These charts represent the answer distribution overall and across all tiers.

9. RRA 報告下載，如圖 10 所示。

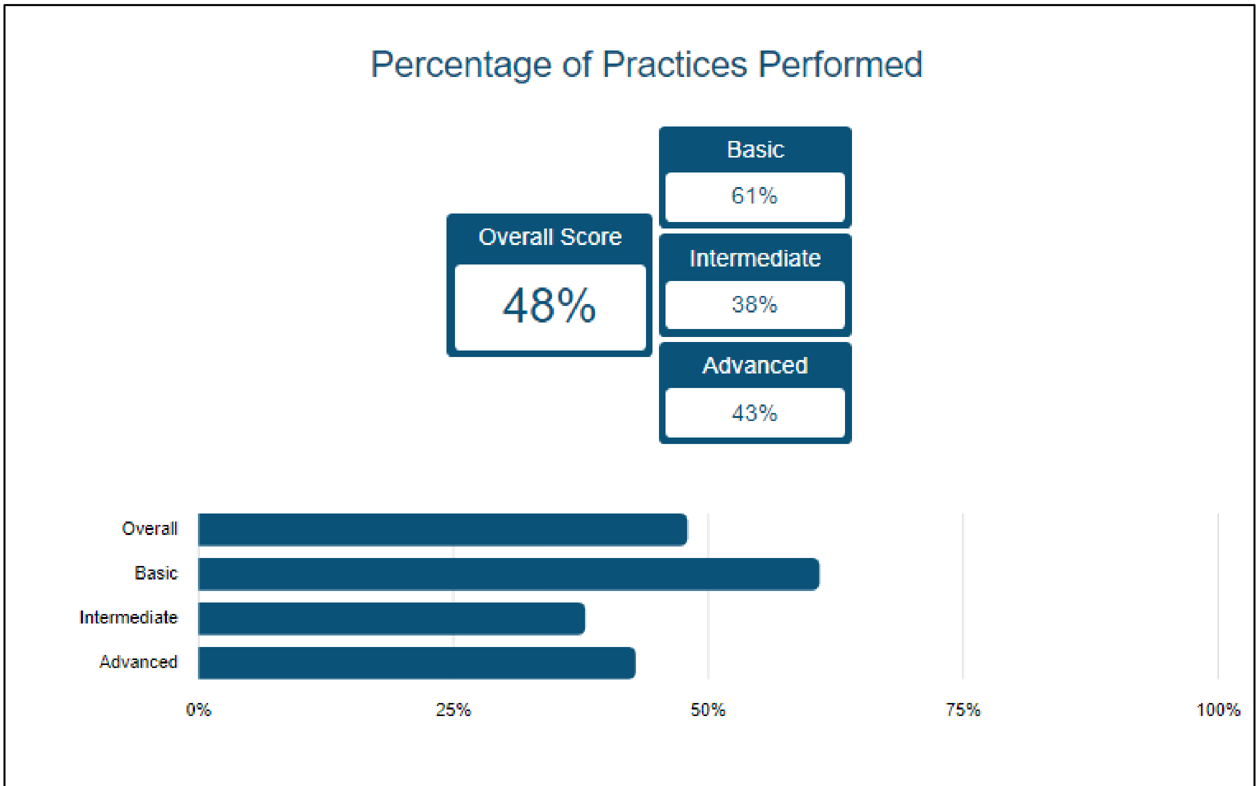
圖 10、RRA 報告下載。



- ‘RRA Report’ 為整體評估報告，包含:
  - 整體評估分數與各等級成熟度(圖 11)
    - 呈現組織於各等級與總體成熟度概觀。
  - 各項評估結果(圖 5、圖 6)
    - 呈現 RRA 十大評估項目的各項成熟度。
  - 建議改善項目(圖 12)
    - 呈現 RRA 十大評估項目最低至最高成熟度排名，提供組織檢視優先改善的項目。
  - 十大項目完成度(圖 13)
    - 呈現 RRA 十大評估項目的各項完成比例。
  - RRA 成熟度分級圖(圖 7)
    - 呈現 RRA 的 ‘Basic’、‘Intermediate’ 與 ‘Advanced’ 三個等級機制，提供組織了解目前各等級防護成熟度與改善措施之優先度。建議會員可依序完成 ‘Basic’ 等級之所有措施之後再持續完善 ‘Intermediate’ 與 ‘Advanced’ 之防護措施。
  - ‘Basic’、‘Intermediate’、‘Advanced’各級項目成熟度 (圖 8、圖 9)
    - 呈現各等級的成熟度。
  - 各問題的細節、建議措施與參考資料。白底為自評‘符合’的項目(圖 14)，紅底為自評‘不符合’的項目(圖 15)
    - 提供組織了解各問題針對的防護措施內容及參考資訊。

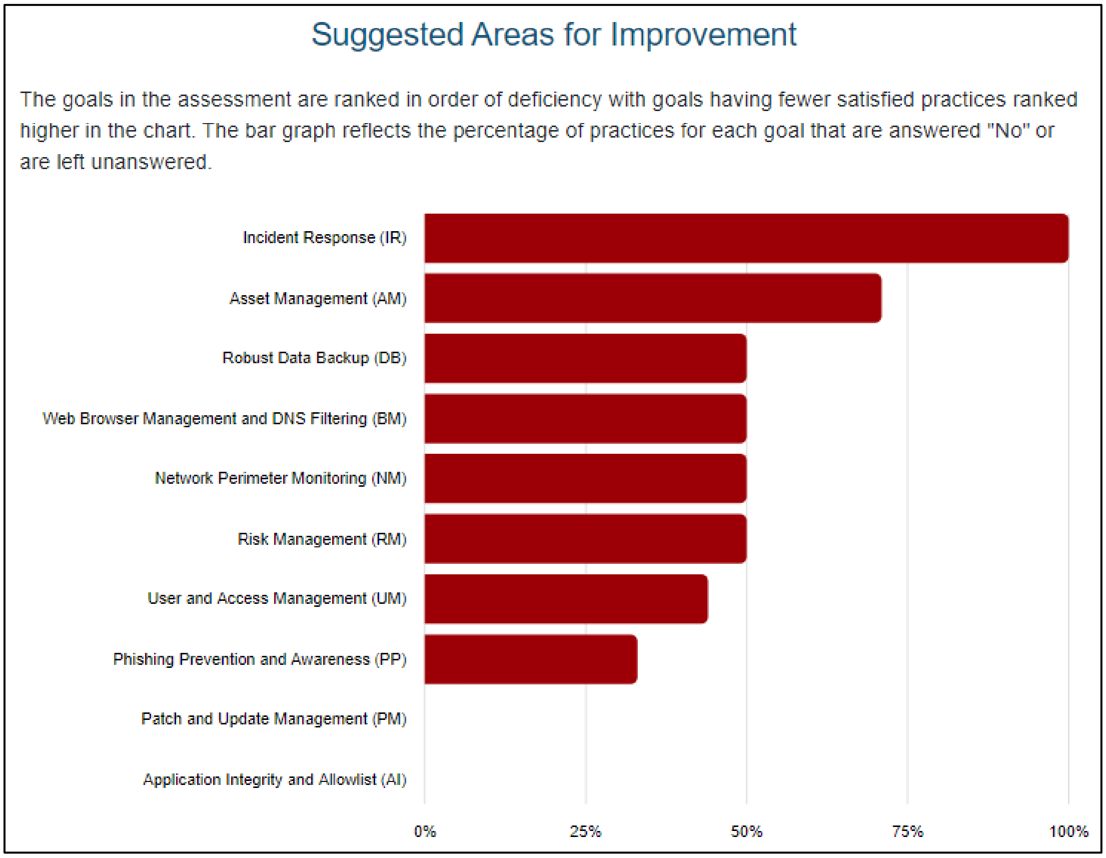
- ‘RRA Deficiency Report’為未達成之防護項目，包含:
    - 建議改善項目(圖 12)
        - 呈現 RAA 十大評估項目最低至最高成熟度排名，提供組織檢視優先改善的項目。
    - 回答‘不符合’的各個問題清單(依照等級分類) (圖 16)
- ‘Comments and Marked for Review’為自評階段選取‘不確定’的項目清單 (圖 17)
- ‘Observations Tear-out Sheet’為含有自評組織的基本資訊頁(圖 18)

圖 11、整體評估分數與各等級成熟度(示意圖)



Scores are calculated as the percentage of "Yes" answers.

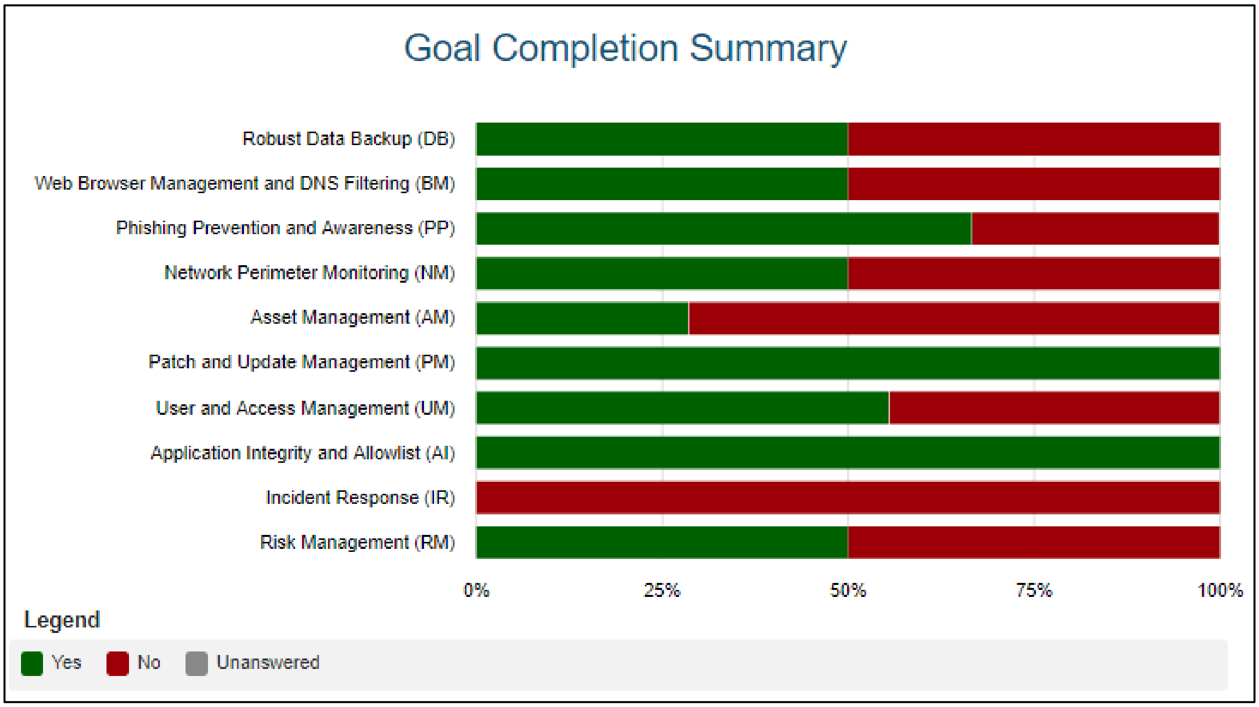
圖 12、建議改善項目(示意圖)



Suggested Areas for Improvement

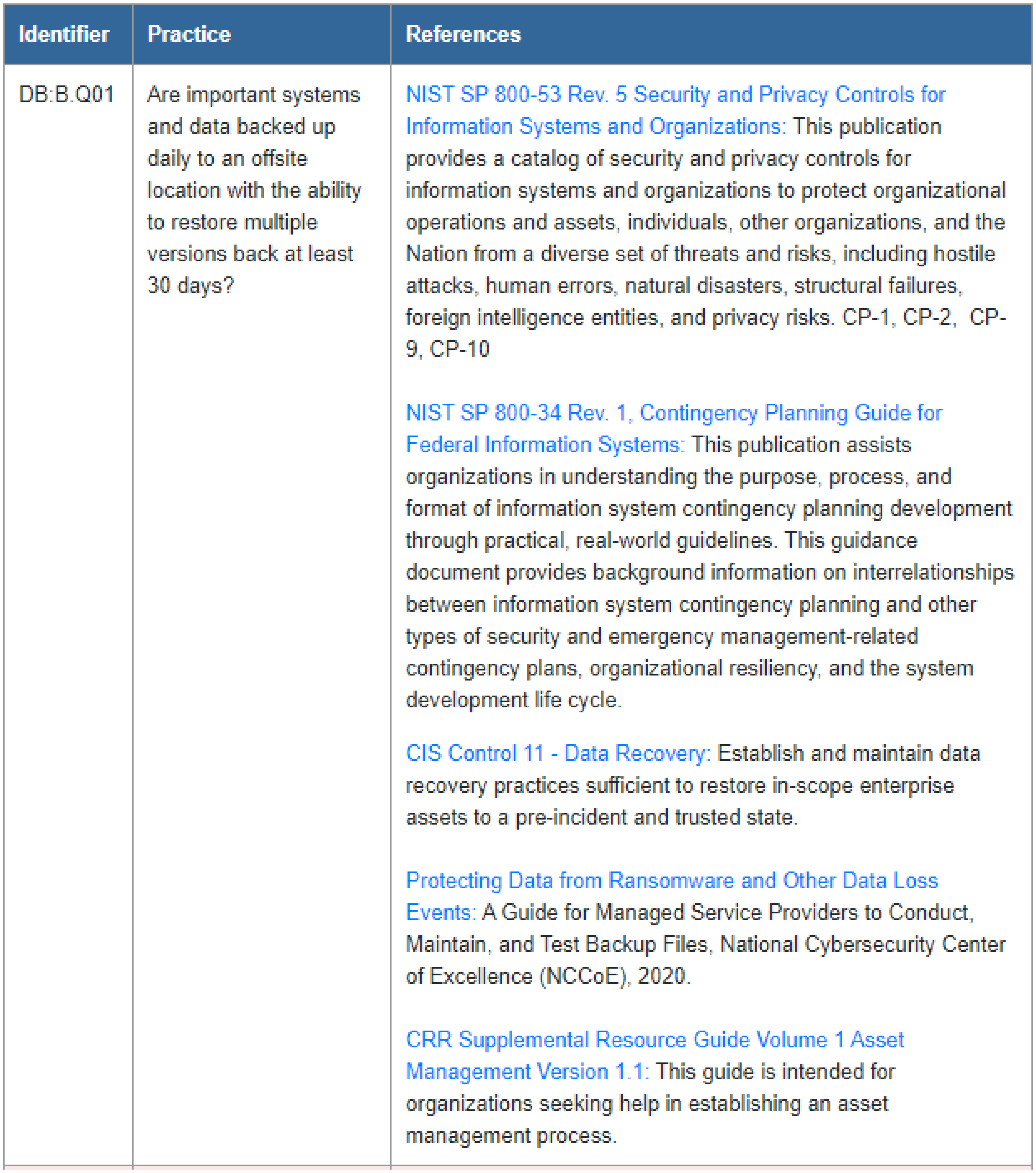
The goals in the assessment are ranked in order of deficiency with goals having fewer satisfied practices ranked higher in the chart. The bar graph reflects the percentage of practices for each goal that are answered "No" or are left unanswered.

圖 13、十大項目完成度(示意圖)



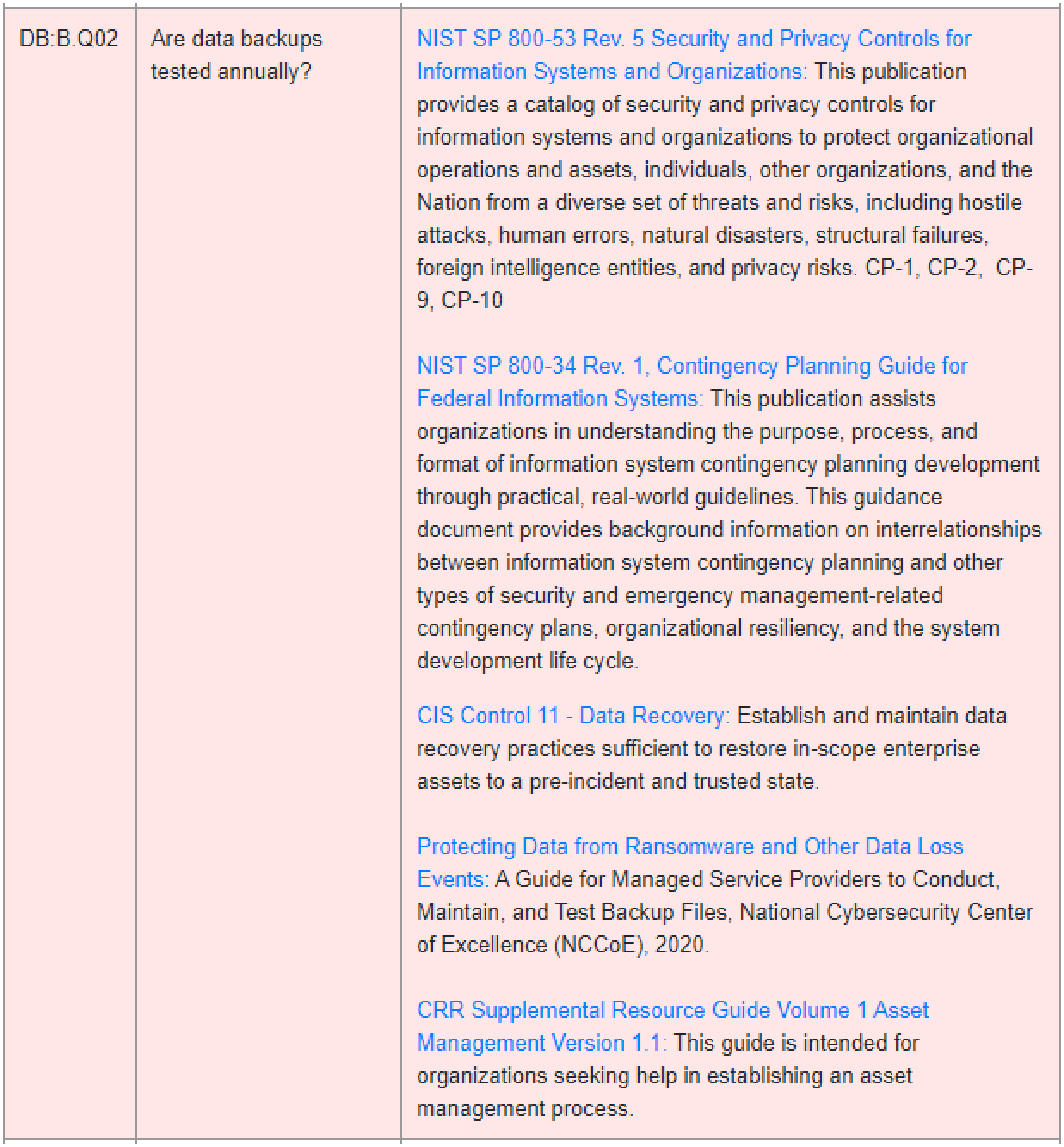
Goal Completion Summary

圖 14、自評為‘符合’的項目與細節說明



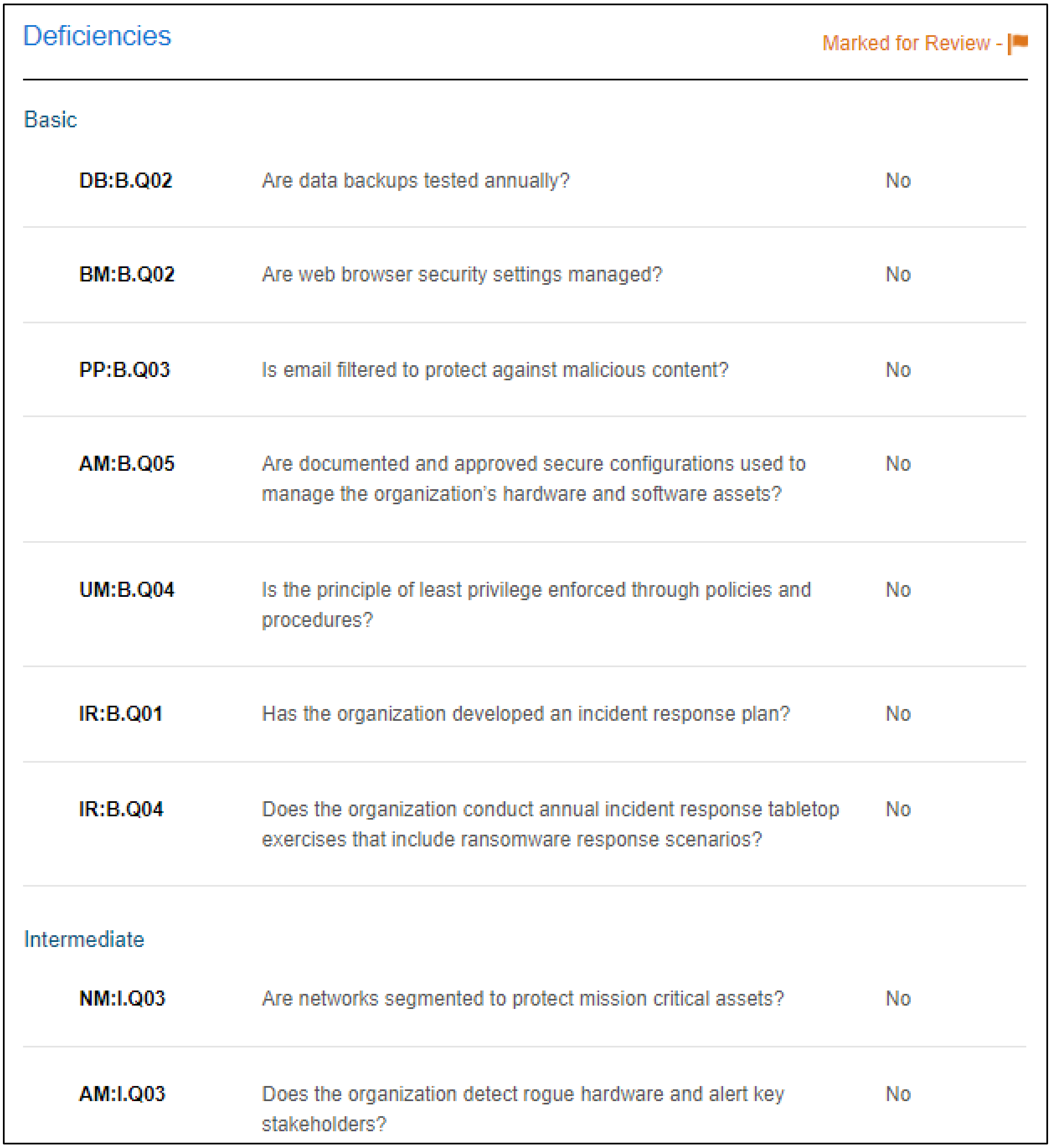
| Identifier | Practice | References |
|---|---|---|
| DB:B.Q01 | Are important systems and data backed up daily to an offsite location with the ability to restore multiple versions back at least 30 days? | NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-1, CP-2, CP-9, CP-10<br>NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: This publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle.<br>CIS Control 11 - Data Recovery: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.<br>Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain, and Test Backup Files, National Cybersecurity Center of Excellence (NCCoE), 2020.<br>CRR Supplemental Resource Guide Volume 1 Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process. |

圖 15、自評為‘不符合’的項目與細節說明



| | | |
|---|---|---|
| DB:B.Q02 | Are data backups tested annually? | NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-1, CP-2,  CP-9, CP-10<br>NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: This publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle.<br>CIS Control 11 - Data Recovery: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.<br>Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain, and Test Backup Files, National Cybersecurity Center of Excellence (NCCoE), 2020.<br>CRR Supplemental Resource Guide Volume 1 Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process. |

圖 16、自評為‘不符合’的項目清單 (依照等級分類) (示意圖)



## Deficiencies

Marked for Review - ⚑

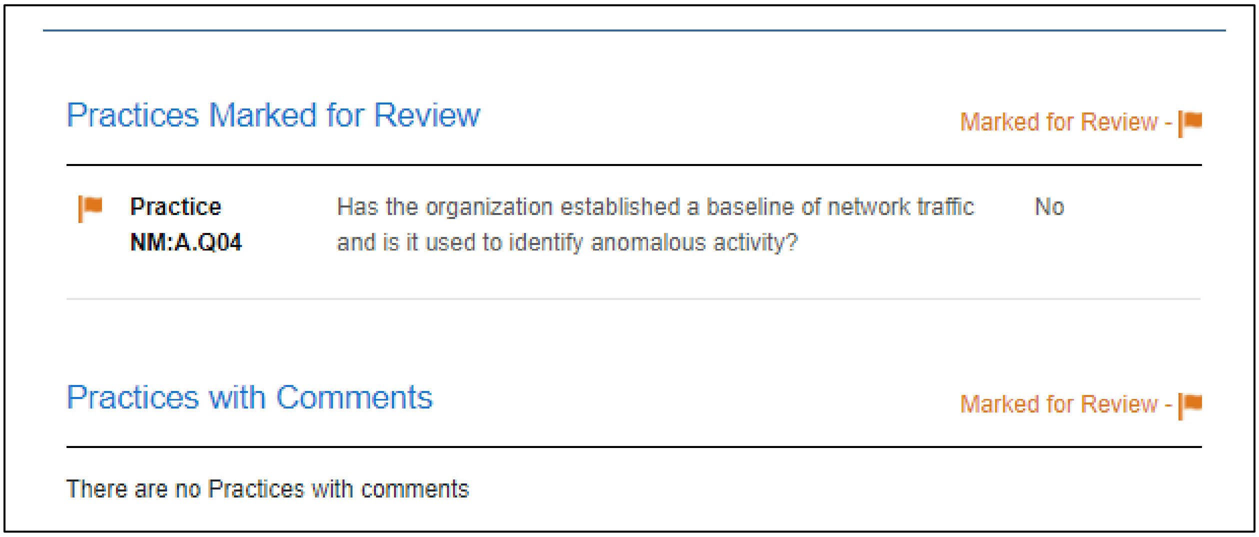
### Basic

| | | |
|---|---|---|
| **DB:B.Q02** | Are data backups tested annually? | No |
| **BM:B.Q02** | Are web browser security settings managed? | No |
| **PP:B.Q03** | Is email filtered to protect against malicious content? | No |
| **AM:B.Q05** | Are documented and approved secure configurations used to manage the organization's hardware and software assets? | No |
| **UM:B.Q04** | Is the principle of least privilege enforced through policies and procedures? | No |
| **IR:B.Q01** | Has the organization developed an incident response plan? | No |
| **IR:B.Q04** | Does the organization conduct annual incident response tabletop exercises that include ransomware response scenarios? | No |

### Intermediate

| | | |
|---|---|---|
| **NM:I.Q03** | Are networks segmented to protect mission critical assets? | No |
| **AM:I.Q03** | Does the organization detect rogue hardware and alert key stakeholders? | No |

圖 17、自評階段選取‘不確定’的項目清單(示意圖)



## Practices Marked for Review

Marked for Review - 🚩

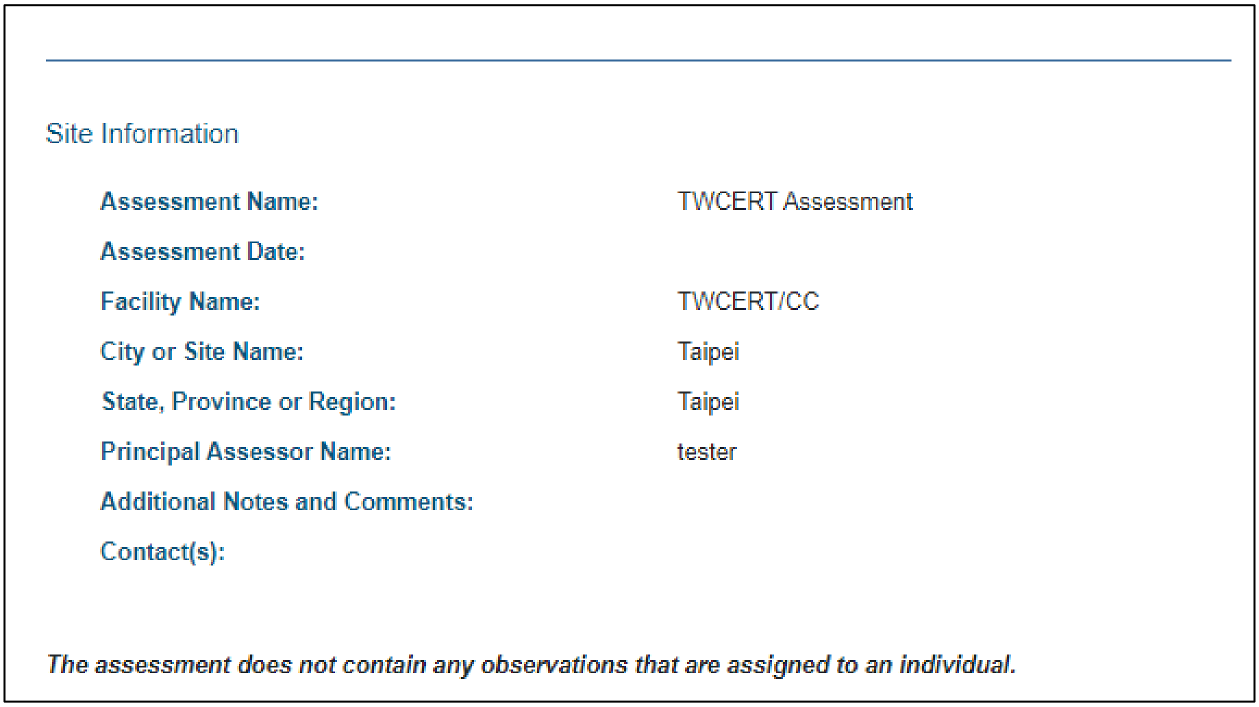
| | | | |
|---|---|---|---|
| 🚩 | **Practice NM:A.Q04** | Has the organization established a baseline of network traffic and is it used to identify anomalous activity? | No |

## Practices with Comments

Marked for Review - 🚩

There are no Practices with comments

圖 18、自評組織的基本資訊(示意圖)



### Site Information

| | |
|---|---|
| **Assessment Name:** | TWCERT Assessment |
| **Assessment Date:** | |
| **Facility Name:** | TWCERT/CC |
| **City or Site Name:** | Taipei |
| **State, Province or Region:** | Taipei |
| **Principal Assessor Name:** | tester |
| **Additional Notes and Comments:** | |
| **Contact(s):** | |

***The assessment does not contain any observations that are assigned to an individual.***