RANSOMWARE READINESS ASSESSMENT

MT-ISAC

December 15, 2021

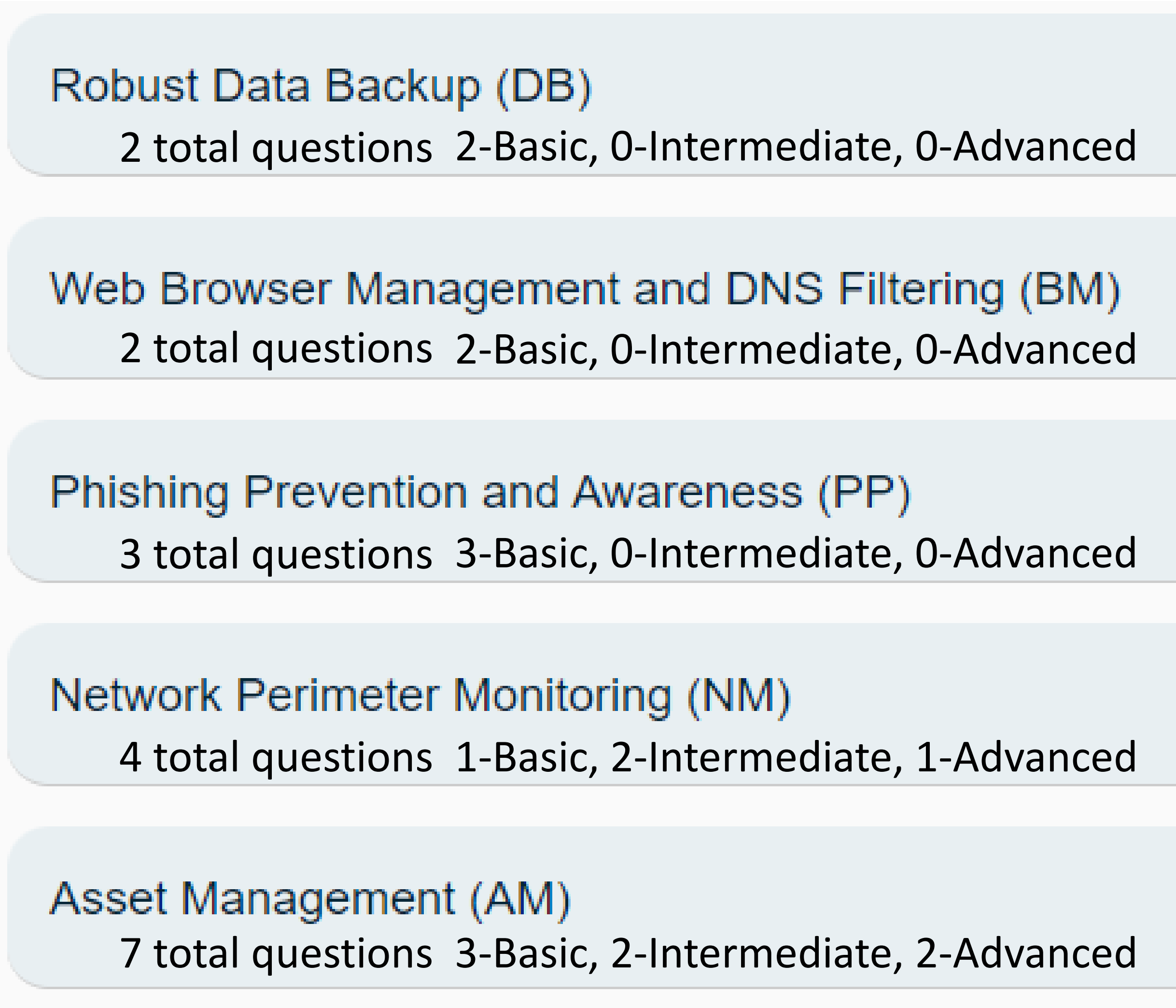
Joe Frohlich
Cybersecurity Advisor - Montana, Region 8

Ransomware Readiness Assessment (RRA)

- Ransomware Readiness Assessment
  - Self-assessment module in Cybersecurity Evaluation Tool (CSET) v10.3
  - 10 Goals with 48 tiered practices (questions); 18 Basic, 16 Intermediate, 14 Advanced
    - Based off CISA Cyber Essentials, Ransomware Guide and leverages the MITRE ATT&CK Framework
    - Structured to give organizations a clear path for improvement
    - Complete with supplemental resources for each practice
  - Several types of reports and charts depicting results
    - Ransomware Assessment Goal Report
    - Deficiency report highlighting weakest goals

10 Goals of the Ransomware Readiness Assessment

48 tiered practices (questions); 18 Basic, 16 Intermediate, 14 Advanced



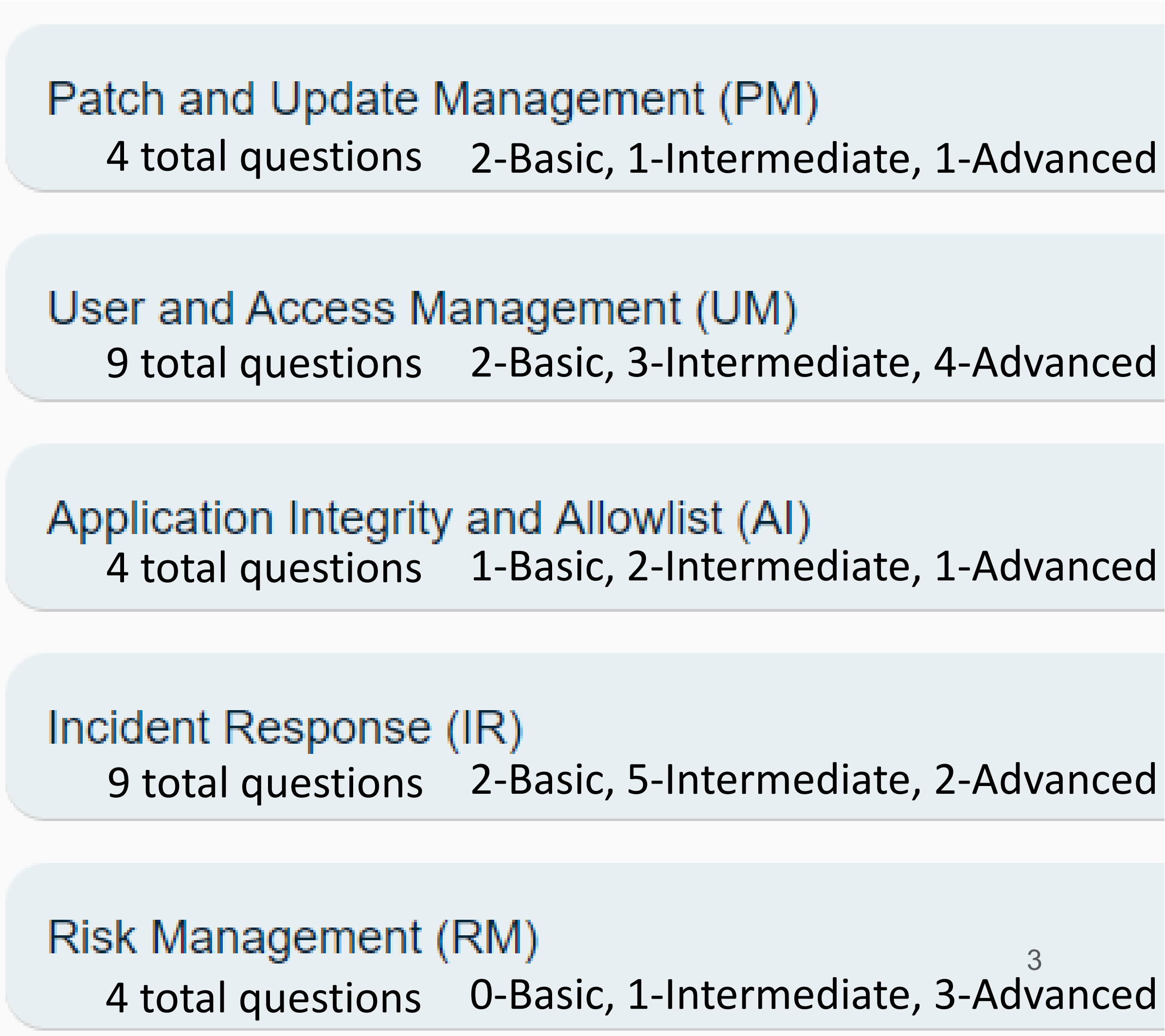
Robust Data Backup (DB)
2 total questions 2-Basic, 0-Intermediate, 0-Advanced

Web Browser Management and DNS Filtering (BM)
2 total questions 2-Basic, 0-Intermediate, 0-Advanced

Phishing Prevention and Awareness (PP)
3 total questions 3-Basic, 0-Intermediate, 0-Advanced

Network Perimeter Monitoring (NM)
4 total questions 1-Basic, 2-Intermediate, 1-Advanced

Asset Management (AM)
7 total questions 3-Basic, 2-Intermediate, 2-Advanced



Patch and Update Management (PM)
4 total questions 2-Basic, 1-Intermediate, 1-Advanced

User and Access Management (UM)
9 total questions 2-Basic, 3-Intermediate, 4-Advanced

Application Integrity and Allowlist (AI)
4 total questions 1-Basic, 2-Intermediate, 1-Advanced

Incident Response (IR)
9 total questions 2-Basic, 5-Intermediate, 2-Advanced

Risk Management (RM)
4 total questions 0-Basic, 1-Intermediate, 3-Advanced

RRA – Download CSET / Access RRA

Step 1

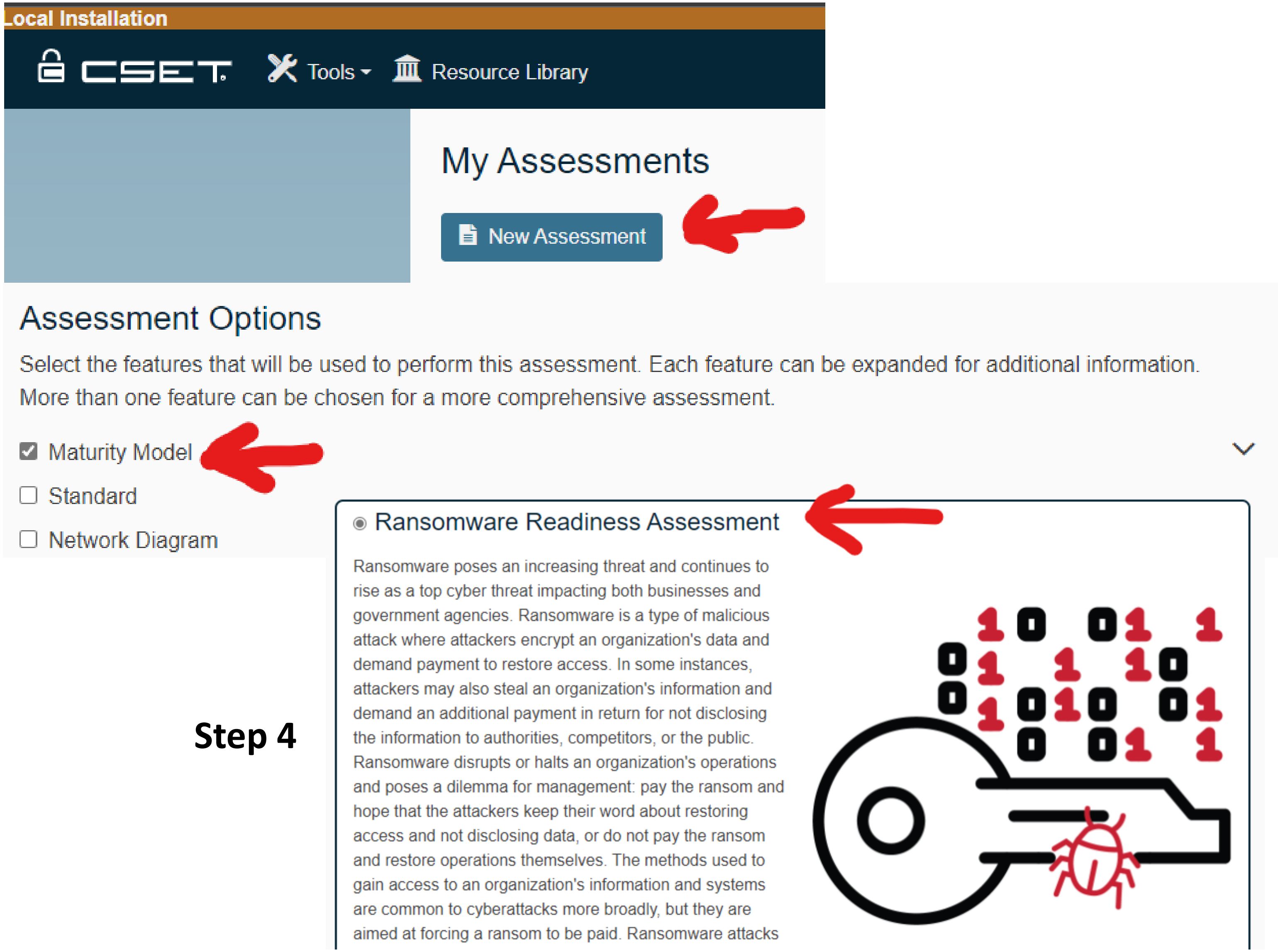
Download CSET latest version via GitHub

- [Releases · cisagov/cset · GitHubCyber]()

Step 2

Step 3

Step 4



My Assessments

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

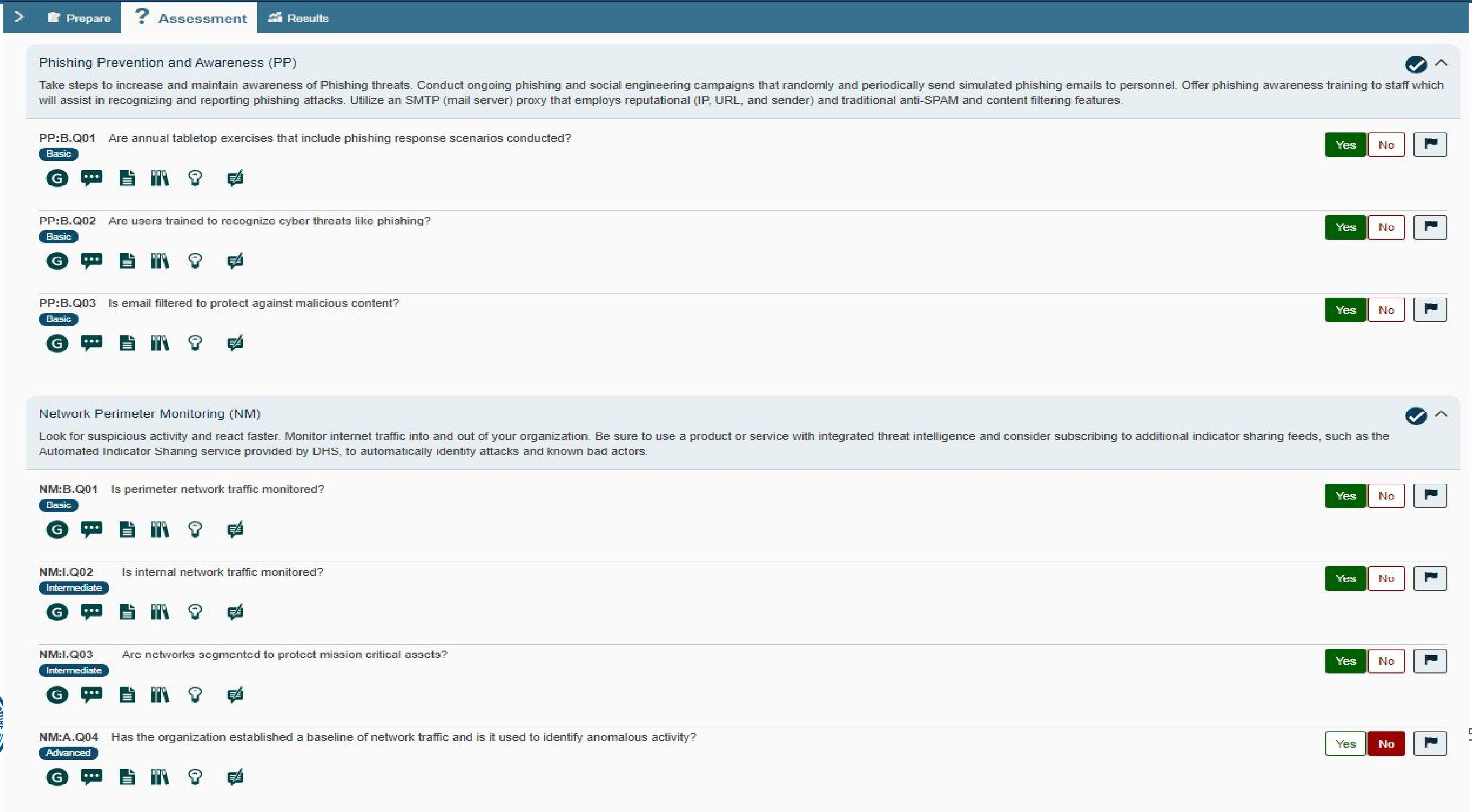
☐ Standard

☐ Network Diagram

● 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

RRA - Practices/Questions



Phishing Prevention and Awareness (PP)

Take steps to increase and maintain awareness of Phishing threats. Conduct ongoing phishing and social engineering campaigns that randomly and periodically send simulated phishing emails to personnel. Offer phishing awareness training to staff which will assist in recognizing and reporting phishing attacks. Utilize an SMTP (mail server) proxy that employs reputational (IP, URL, and sender) and traditional anti-SPAM and content filtering features.

PP:B.Q01 Are annual tabletop exercises that include phishing response scenarios conducted?
Basic
[✓ Yes] No

PP:B.Q02 Are users trained to recognize cyber threats like phishing?
Basic
[✓ Yes] No

PP:B.Q03 Is email filtered to protect against malicious content?
Basic
[✓ Yes] No

Network Perimeter Monitoring (NM)

Look for suspicious activity and react faster. Monitor internet traffic into and out of your organization. Be sure to use a product or service with integrated threat intelligence and consider subscribing to additional indicator sharing feeds, such as the Automated Indicator Sharing service provided by DHS, to automatically identify attacks and known bad actors.

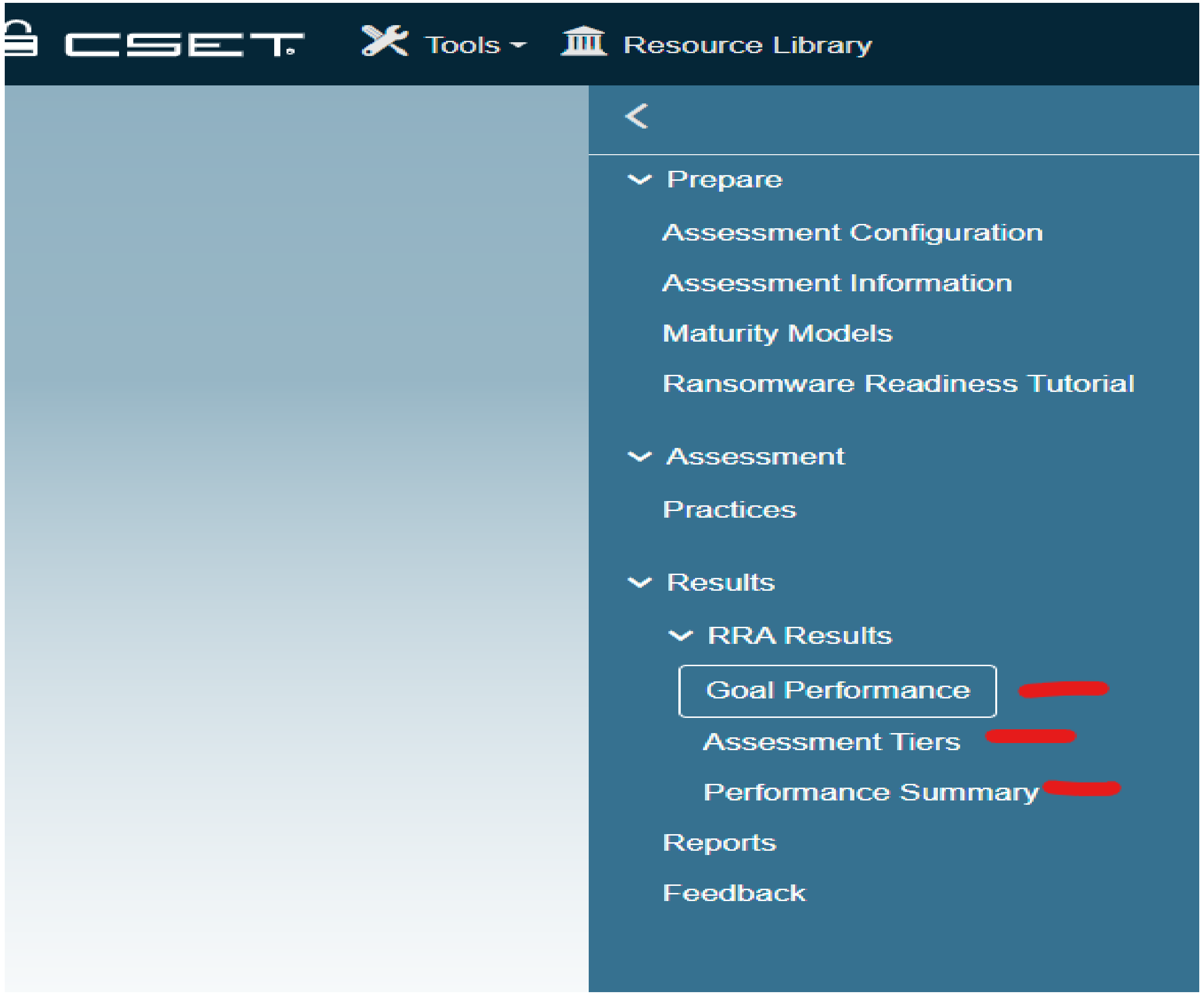
NM:B.Q01 Is perimeter network traffic monitored?
Basic
[✓ Yes] No

NM:I.Q02 Is internal network traffic monitored?
Intermediate
[✓ Yes] No

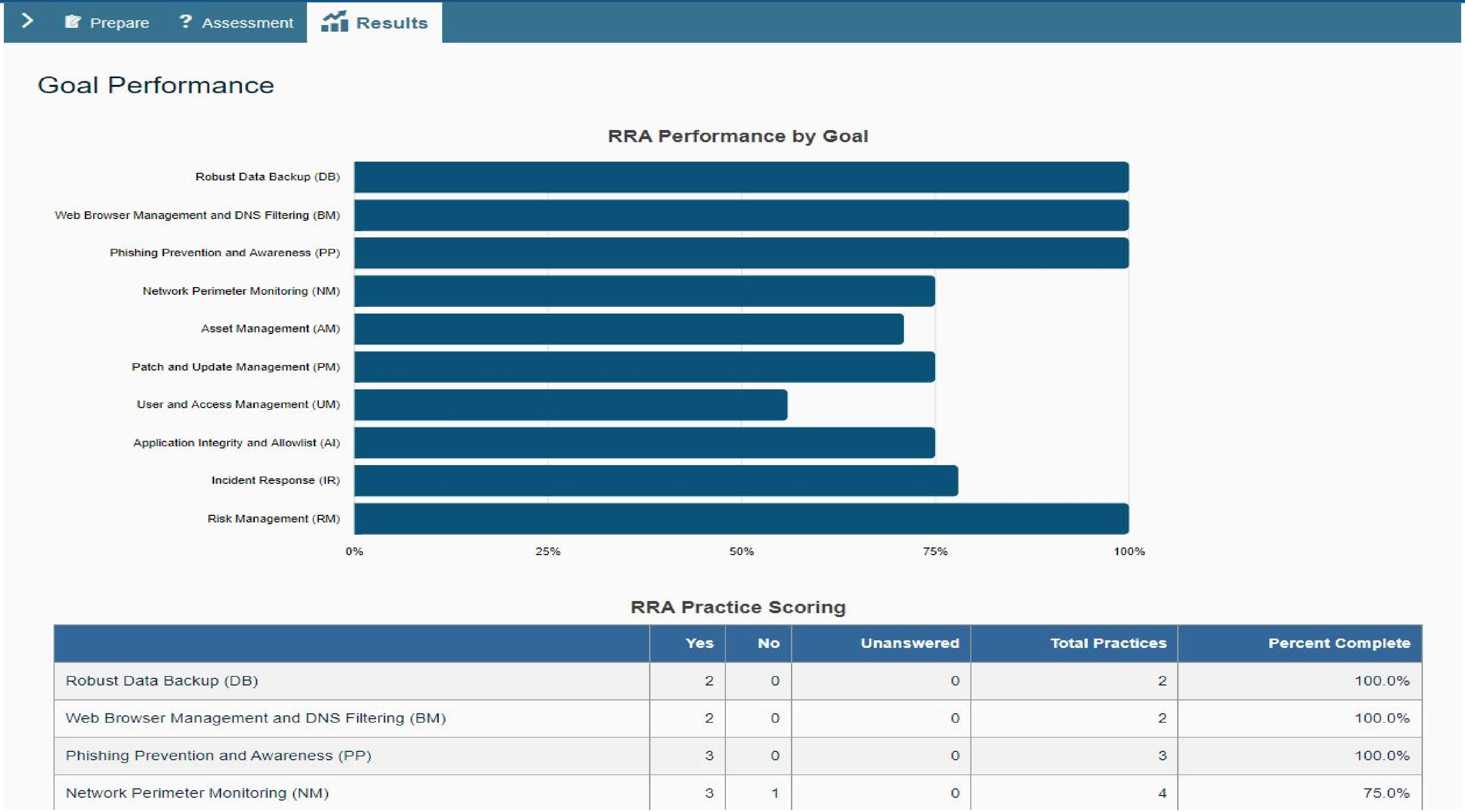
NM:I.Q03 Are networks segmented to protect mission critical assets?
Intermediate
[✓ Yes] No

NM:A.Q04 Has the organization established a baseline of network traffic and is it used to identify anomalous activity?
Advanced
Yes [✓ No]

RRA – Results with Charts and Graphs



RRA - Goal Performance



>
Prepare
? Assessment
Results

Goal Performance

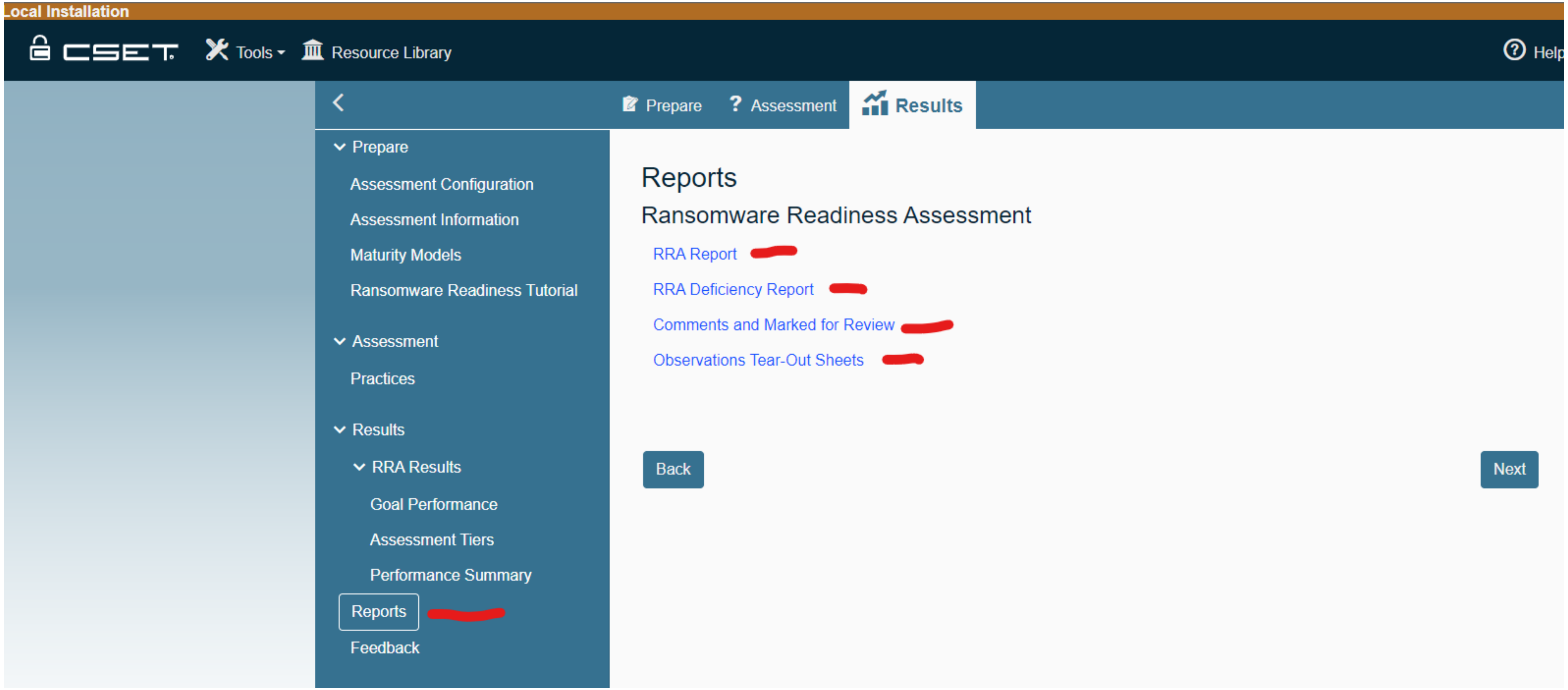
RRA Performance by Goal

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)
Risk Management (RM)
0%
25%
50%
75%
100%

RRA Practice Scoring

	Yes	No	Unanswered	Total Practices	Percent Complete
Robust Data Backup (DB)	2	0	0	2	100.0%
Web Browser Management and DNS Filtering (BM)	2	0	0	2	100.0%
Phishing Prevention and Awareness (PP)	3	0	0	3	100.0%
Network Perimeter Monitoring (NM)	3	1	0	4	75.0%

RRA - Reports

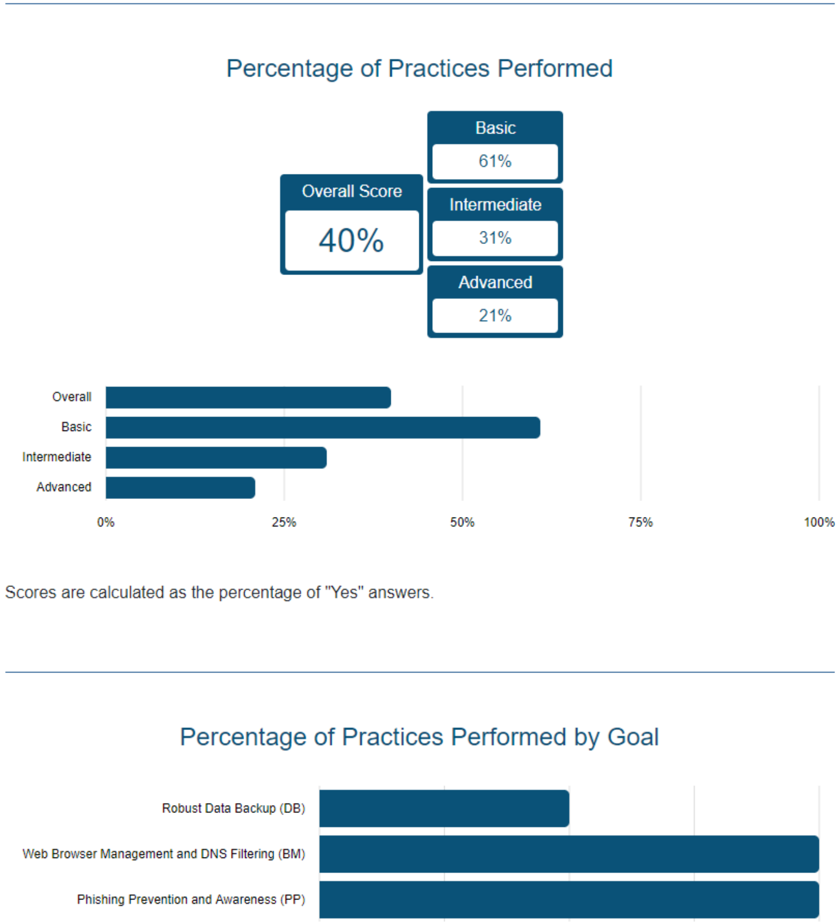


Reports

Ransomware Readiness Assessment

- RRA Report
- RRA Deficiency Report
- Comments and Marked for Review
- Observations Tear-Out Sheets

The RRA Report



Percentage of Practices Performed

Overall Score
40%

Basic
61%

Intermediate
31%

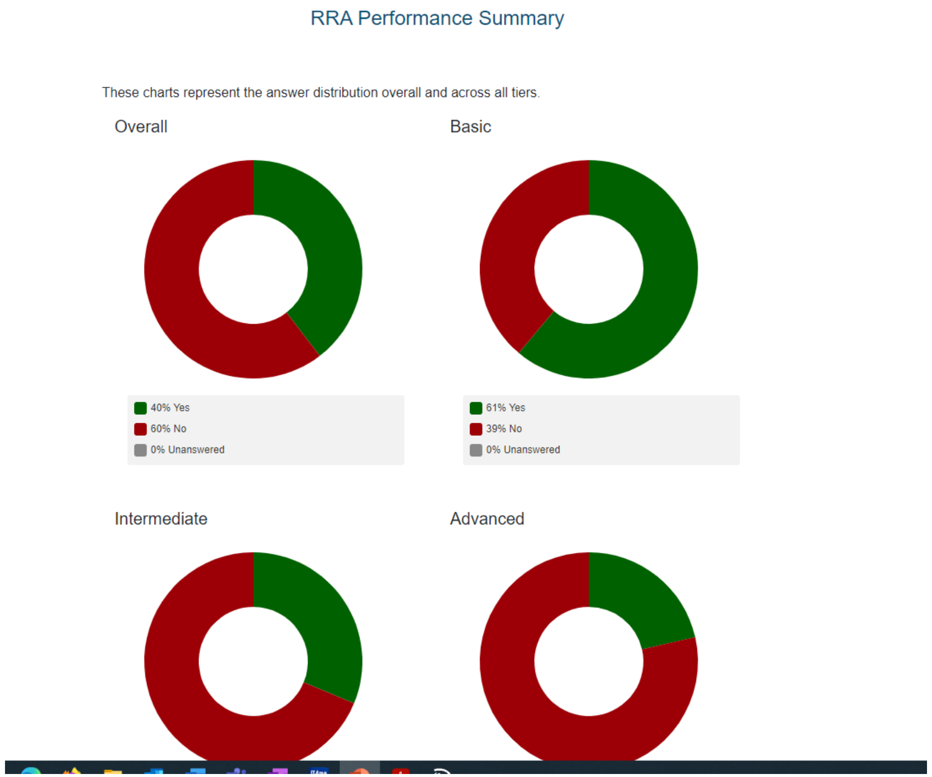
Advanced
21%

Overall
Basic
Intermediate
Advanced
0%
25%
50%
75%
100%

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

Percentage of Practices Performed by Goal

Robust Data Backup (DB)
Web Browser Management and DNS Filtering (BM)
Phishing Prevention and Awareness (PP)



RRA Performance Summary

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

Overall

🟩 40% Yes
🟥 60% No
▨ 0% Unanswered

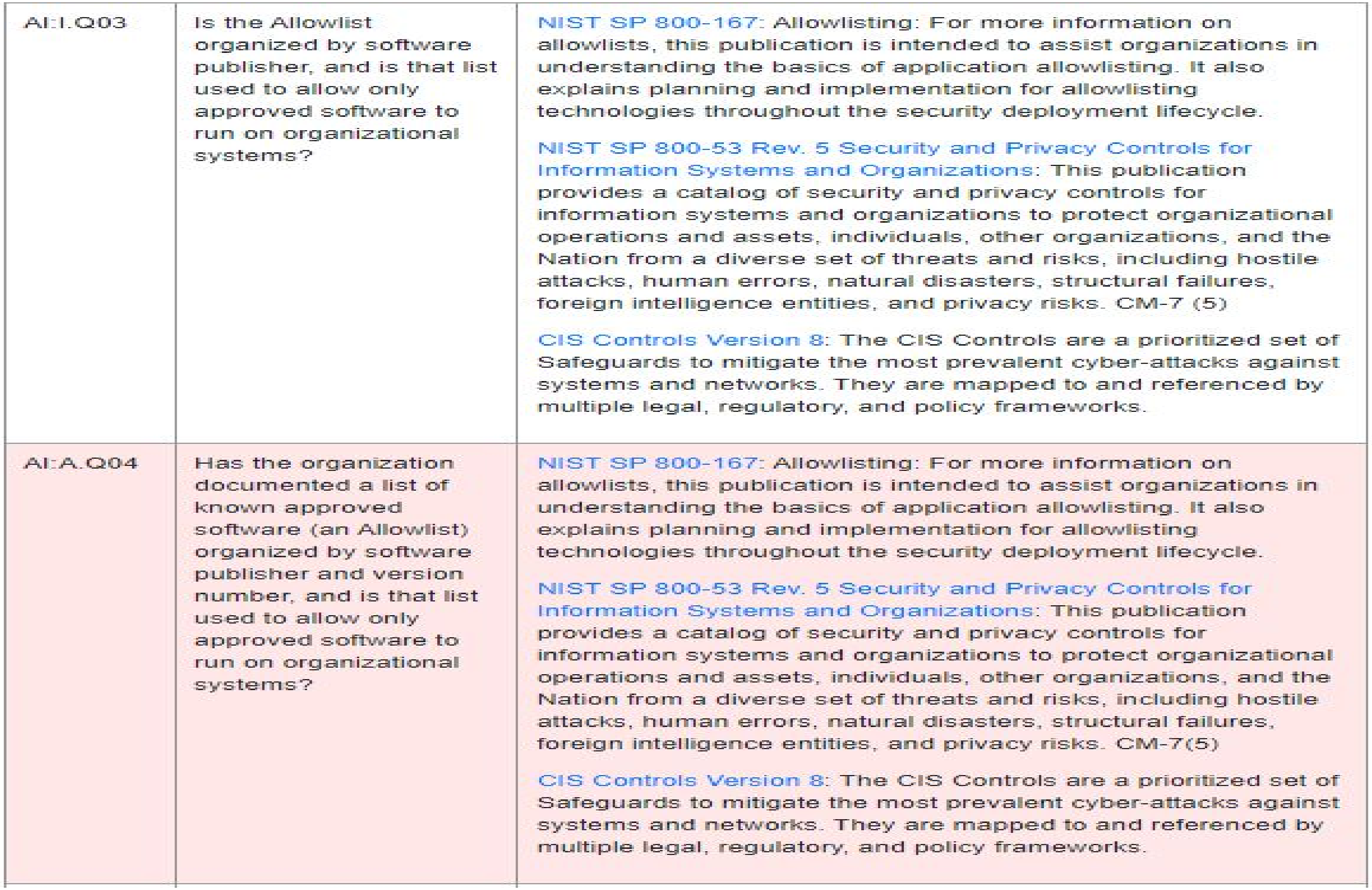
Basic

🟩 61% Yes
🟥 39% No
▨ 0% Unanswered

Intermediate

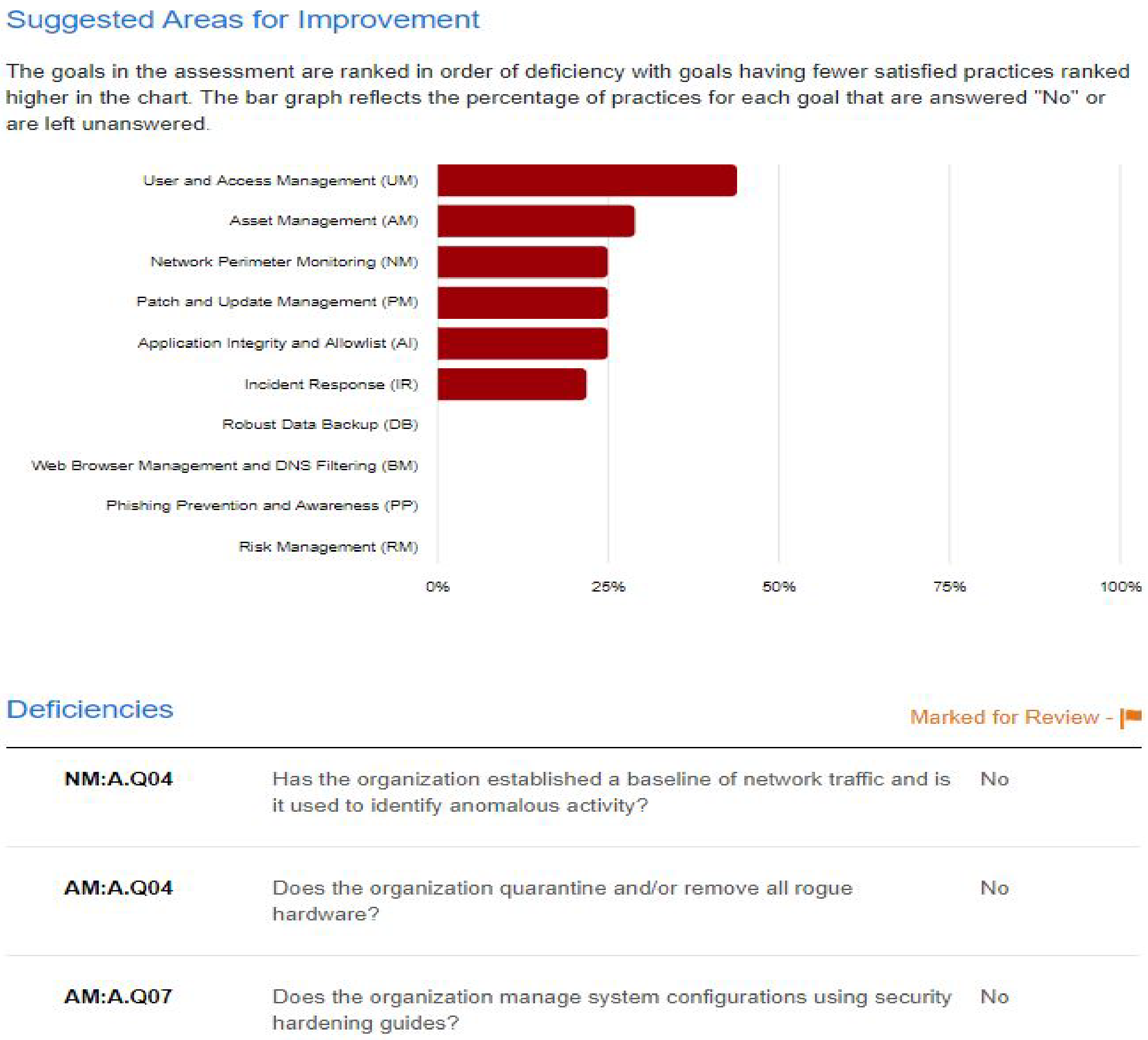
Advanced

RRA Report - References



AI:I.Q03	Is the Allowlist organized by software publisher, and is that list used to allow only approved software to run on organizational systems?	NIST SP 800-167: Allowlisting: For more information on allowlists, this publication is intended to assist organizations in understanding the basics of application allowlisting. It also explains planning and implementation for allowlisting technologies throughout the security deployment lifecycle. 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. CM-7 (5) CIS Controls Version 8: The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.
AI:A.Q04	Has the organization documented a list of known approved software (an Allowlist) organized by software publisher and version number, and is that list used to allow only approved software to run on organizational systems?	NIST SP 800-167: Allowlisting: For more information on allowlists, this publication is intended to assist organizations in understanding the basics of application allowlisting. It also explains planning and implementation for allowlisting technologies throughout the security deployment lifecycle. 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. CM-7(5) CIS Controls Version 8: The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.

RRA Deficiency Report



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.

User and Access Management (UM)
Asset Management (AM)
Network Perimeter Monitoring (NM)
Patch and Update Management (PM)
Application Integrity and Allowlist (AI)
Incident Response (IR)
Robust Data Backup (DB)
Web Browser Management and DNS Filtering (BM)
Phishing Prevention and Awareness (PP)
Risk Management (RM)
0%
25%
50%
75%
100%

Deficiencies

Marked for Review - ⚑

NM:A.Q04	Has the organization established a baseline of network traffic and is it used to identify anomalous activity?	No
AM:A.Q04	Does the organization quarantine and/or remove all rogue hardware?	No
AM:A.Q07	Does the organization manage system configurations using security hardening guides?	No

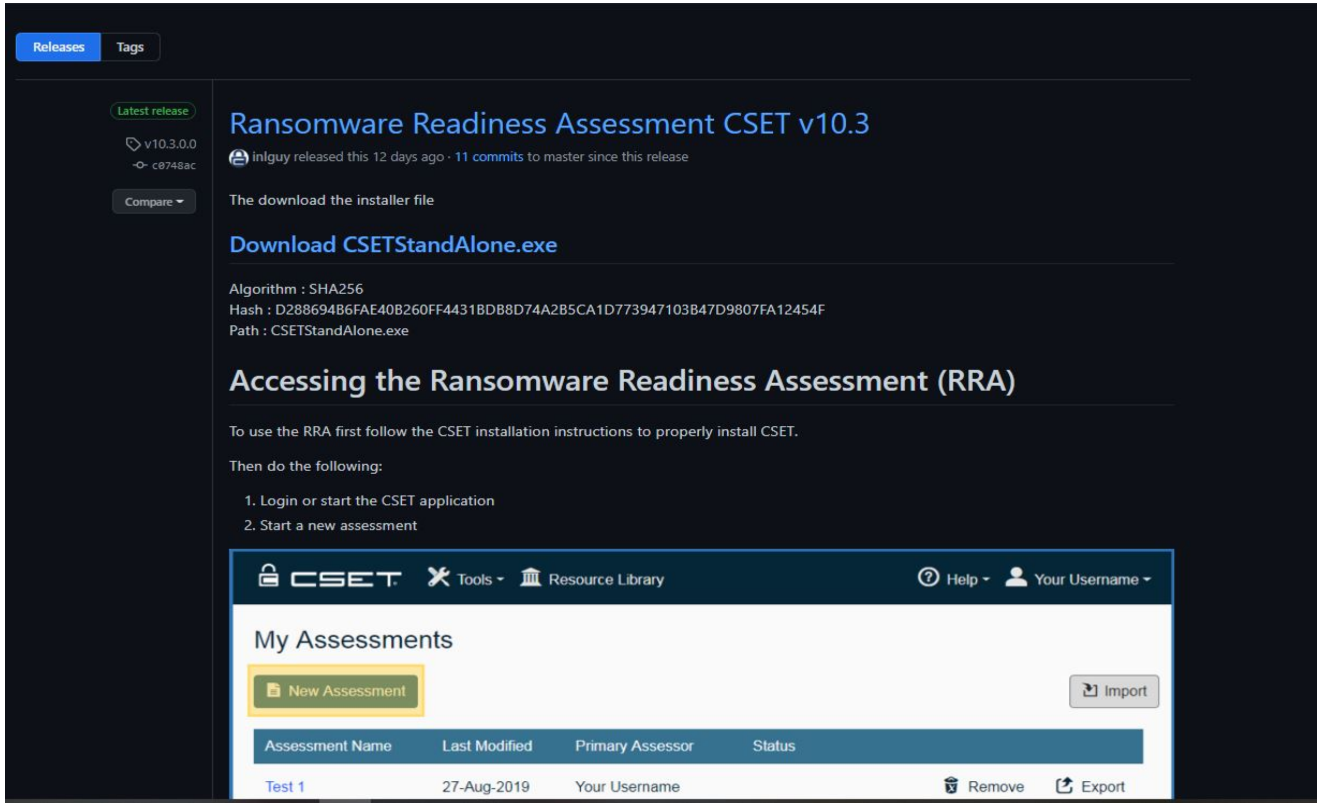
Download CSET / RRA on GitHub and take RRA

Download via GitHub

- Releases · cisagov/cset · GitHubCyber
- Security Evaluation Tool (CSET®) | CISA

Questions?

- **Contact Joe Frohlich joseph.frohlich@cisa.dhs.gov**
- **Contact Cyberadvisor@cisa.dhs.gov or Vulnerability@cisa.dhs.gov**



Ransomware Readiness Assessment CSET v10.3

inlguy released this 12 days ago · 11 commits to master since this release

The download the installer file

Download CSETStandAlone.exe

Algorithm : SHA256
Hash : D288694B6FAE40B260FF4431BDB8D74A2B5CA1D773947103B47D9807FA12454F
Path : CSETStandAlone.exe

Accessing the Ransomware Readiness Assessment (RRA)

To use the RRA first follow the CSET installation instructions to properly install CSET.

Then do the following:

1. Login or start the CSET application
2. Start a new assessment

Assessment Name	Last Modified	Primary Assessor	Status		
Test 1	27-Aug-2019	Your Username		Remove	Export

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA