Risk Assessment Question Mapping

1.0 Inventory and Control of Assets

RA Q1 = Does the organization inventory all company owned devices? (i.e., Laptops, desktops, tablets, smartphones)
RA Q1 Impact Rating = 3

RA Q2 = Does the organization have a way to address any unauthorized assets from the network?
RA Q2 Impact Rating = 5

RA Q3 = Does the organization maintain an inventory of all licensed software installed across the organization?
RA Q3 Impact Rating = 3

RA Q4 = Has the organization adopted and implemented plans to protect and segregate end-of-life software?
RA Q4 Impact Rating = 5

2.0 Account Management

RA Q5 = Does the organization have an inventory of all user accounts including users/admins/service accounts?
RA Q5 Impact Rating = 5

RA Q6 = Does the organization utilize best practices for their password policy?
RA Q6 Impact Rating = 5

RA Q7 = Has the organization adopted MFA for all employees and all remote access connections?
RA Q7 Impact Rating = 5

RA Q8 = Is MFA protecting all organizational data and systems?
RA Q8 Impact Rating = 5

RA Q9 = Does the organization disable dormant accounts?
RA Q9 Impact Rating = 5

RA Q10 = Does the organization have a policy and standard operating procedures outlined for onboarding or change in position?
RA Q10 Impact Rating = 3

RA Q11 = Does the organization have a policy and standard operating procedures outlined for offboarding?
RA Q11 Impact Rating = 5

3.0 Data Protection

RA Q12 = Does the organization have an inventory of critical data?
RA Q12 Impact Rating = 1

RA Q13 = Do administrators have dedicated admin accounts for conducting high privilege tasks?
RA Q13 Impact Rating = 5

RA Q14 = Does the organization encrypt hard drives on endpoints, servers, and on-premises backups?
RA Q14 Impact Rating = 3

4.0 Secure Configuration of Enterprise Assets

RA Q15 = Does the organization have a secure configuration process for endpoint devices?
RA Q15 Impact Rating = 1

RA Q16 = Does the organization have a Patch Management Process to install all software patches within 30 or fewer days and critical and high-severity patches within 7 days?
RA Q16 Impact Rating = 3

RA Q17 = Does the organization's Patch Management Process address both operating systems and installed applications?
RA Q17 Impact Rating = 3

RA Q18 = Does the organization have a secure configuration process for networking devices?
RA Q18 Impact Rating = 3

RA Q19 = Does the organization have a process to ensure that the networking infrastructure such as routers, switches, firewalls, and other network appliances are kept up to date?
RA Q19 Impact Rating = 3

RA Q20 = Does the organization perform quarterly external vulnerability scans?
RA Q20 Impact Rating = 5

RA Q21 = Has the organization configured session lockout times for endpoints?
RA Q21 Impact Rating = 3

RA Q22 = Does the organization have different networks or subnets for staff and students?
RA Q22 Impact Rating = 3

RA Q23 = Does the organization use WPA2 or better for their wireless network(s)?
RA Q23 Impact Rating = 3

RA Q24 = Are the wireless networks segmented from each other?
RA Q24 Impact Rating = 3

RA Q25 = Does the organization protect access via 802.1X or similar?
RA Q25 Impact Rating = 3

RA Q26 = Does the organization change any wireless PSKs annually?
RA Q26 Impact Rating = 3

5.0 Malware Defense

RA Q27 = Does the organization use a DNS filtering service?
RA Q27 Impact Rating = 5

RA Q28 = Has the organization adopted and implemented endpoint detection and response (EDR) software services?
RA Q28 Impact Rating = 3

RA Q29 = Does the organization utilize an Anti-Malware service?
RA Q29 Impact Rating = 5

6.0 Data Recovery

RA Q30 = Does the organization Perform Automated backups?
RA Q30 Impact Rating = 5

RA Q31 = Does the organization have an air gap backup?
RA Q31 Impact Rating = 5

RA Q32 = Does the organization perform bi-annual checks of the backups including testing and validation of recovery capability?
RA Q32 Impact Rating = 5

7.0 Security Awareness

RA Q33 = Does the organization have a security awareness program?
RA Q33 Impact Rating = 3

RA Q34 = Does the organization conduct phishing simulation tests and training at least quarterly?
RA Q34 Impact Rating = 3

RA Q35 = Does the organization offer follow-up security training?
RA Q35 Impact Rating = 3

8.0 Service Provider Management

RA Q36 = Does the organization have a process for vetting their service providers?
RA Q36 Impact Rating = 1

RA Q37 = Does the organization keep an inventory of their service providers?
RA Q37 Impact Rating = 1

9.0 Incident Response Management

RA Q38 = Does the organization have an Incident response plan?
RA Q38 Impact Rating = 3

RA Q39 = Does the organization outline clear responsibilities in the CIRP (CYBER INCIDENT RESPONSE PLAN)?
RA Q39 Impact Rating = 1

RA Q40 = Does the organization have a communication plan and contact information in the CIRP?
RA Q40 Impact Rating = 1

RA Q41 = Does the organization perform periodic exercises such as tabletops to test the plan with the CIRP team members?
RA Q41 Impact Rating = 1

Risk Calculation Formula

Risk Score = RA Q# Score × Impact Rating

Where RA Q# Score is:

- Fully Implemented (1)
- Partially Implemented (3)
- Not Implemented (5)

Risk Rating Categories

- **Low (0-9)** = Overall risk is low to organization
- **Moderate (10-15)** = Overall risk is moderate to organization
- **High (16-25)** = Overall risk is high to organization