A logo for a health company

Description automatically generated

## **Public Notices**

## **RFP Information Systems Security Audit**

## **RFP #IT 202301**

## **Responses to Questions**

Q1. How many locations are in scope for the assessment?

*A1.* *There is one location in scope for the audit, however SWMBH relies on a Managed Services Provider for housing equipment and SWMBH employees are governed by a hybrid work policy allowing them to work in the office or at home.*

Q2. The RFP references the statement “proposed audit will meet the requirements of ISO 27001/27002 Cybersecurity Framework or NIST Cybersecurity Framework V1.1”.  Is there a preference for either framework?

*A2. There is no preference.  Either framework is acceptable.*

Q3. Will network penetration testing be included with the scope of work?

*A3. Network penetration testing and vulnerability scanning are not in scope for this audit.  SWMBH has a contract for annual penetration testing and monthly vulnerability scanning.*

Q4. What devices are in scope under “Device Security” (Section 1.1)?

*A4. Network attached devices are in scope.  Examples include but are not limited to servers, printers, laptops, access points and firewalls.*

Q5. What is the proposed budget for the project?

*A5. SWMBH prefers not to disclose our budget information.*

Q6. Has SWMBH conducted either a risk assessment or IS audit in the past?   How many findings/recommendations were issued as a result of the last audit/assessment?

*A6. SWMBH was affiliated with an organization until December 2022 who conducted a comprehensive annual security risk assessment.  All findings were corrected and resolved but one.*

Q7. How many IT employees do you have in the department?

*A7. IT currently has six employed staff members.*

Q8. Is there a deadline to complete the risk assessment?

*A8. The preferred deadline is September 30, 2023 which can be negotiated if necessary.*

Q9. What cloud services does SWMBH utilize? (e.g. SaaS, storage)

*A9. Cloud services include storage and backup, Microsoft 365 tenant services, Microsoft Azure, a remote hosted website and cloud-based work management platforms.*

Q10. Is it expected that “Personnel Security” (Section 1.1) will include the HR department under the assessment (e.g. background check, security training, policies, etc)?

*A10. No, the HR Department will not be involved in the audit.*

Q11. Is there any preference for onsite vs offsite for the performance of the assessment.

*A11. An off-site assessment is acceptable.*

Q12. Is this one risk assessment for Southwest Michigan Behavioral Health whose security posture is under its own control or do the participant Community Mental Health Services Programs get evaluated as part of this assessment?

*A12. This risk assessment only applies to Southwest Michigan Behavioral Health and not the participant Community Mental Health Services Programs.*

Q13. Is the assessment expected to be completed solely through an interview Q&A format or should the assessment include verification of answers through auditing of settings and the capture of screenshots for verification? e.g. For the control "PR.DS-1: Data-at-rest is protected", should the auditor be asking for screenshots of database and file system settings that prove data is protected?

*A13. It is expected that the majority of the assessment will be conducted via a Q&A format, however if the auditor thinks a screenshot is needed for verification, that can be arranged.*