RFP Addendum – Responses to Vendor Questions

This addendum provides consolidated responses to questions received from prospective proposers and supplements the Request for Proposals (RFP) for IT Audit Services. The RFP is being issued to comply with applicable procurement requirements and does not reflect dissatisfaction with prior audit services. Many questions are addressed in the RFP itself; the responses below are intended to clarify MMBB's intent and apply to all proposers.

Some questions overlap or request detailed technical, architectural, or execution-level information. Where questions are repetitive, a single consolidated response has been provided. Questions requesting detailed technical, architectural, security control implementation, or execution-level information will be addressed during post-award planning with the selected firm and are not required as part of the proposal submission.

1. Engagement Scope and In-Scope Entities

MMBB's IT department supports MMBB, the Maine Health and Higher Educational Facilities Authority, and the Maine Governmental Facilities Authority within a shared IT environment. As such, IT audits are conducted across the shared environment rather than as separate or selectively reviewed systems for each authority.

MMBB has not identified specific systems or services as explicitly out of scope beyond what is defined in the RFP. Audit scope will be confirmed annually based on the selected audit areas and MMBB's risk considerations.

2. Audit Approach and Objectives

The intent of the engagement is a controls effectiveness audit conducted in an audit-style format, with testing of relevant controls and the inclusion of management recommendations. The engagement is not intended to be a standalone security maturity assessment.

3. Audit Cadence and Rotational Coverage

MMBB's intent is to achieve coverage of the listed rotational audit areas over a three-year cycle. Rotational areas are selected annually based on risk considerations and organizational priorities, with the objective of reviewing each area at least once during the cycle and higher-risk areas more frequently as appropriate. MMBB retains responsibility for determining audit priorities and rotational coverage, informed by management input and risk considerations.

4. Internally Developed Applications

MMBB utilizes approximately a dozen internally developed applications that are primarily client-server in nature. These applications support internal IT administration, accounting functions, and program management activities for MMBB and its related authorities.

Internally developed applications and other business applications supporting MMBB operations may be included in audit scope when relevant to the selected audit areas.

5. Cloud Services (High-Level)

MMBB utilizes a limited cloud footprint consisting of a primary cloud platform supporting collaboration, identity, and business services, along with a small number of additional software-as-a-service (SaaS) applications used to support specific business functions. MMBB does not operate a multi-cloud environment or independently manage cloud-hosted infrastructure beyond this scope.

6. Standards and Frameworks

MMBB does not require strict alignment to a single framework for reporting purposes. While MMBB is familiar with NIST-based concepts, the primary expectation is that reporting be clear, consistent, and appropriate to the scope of the audit. Proposers may recommend the framework they believe is most suitable for the engagement.

7. Remediation and Follow-Up

The selected firm is expected to provide recommendations within the audit report. Formal remediation or corrective action plans are not required; however, the firm should be available to respond to management questions and share general best practices related to its recommendations.

The annual review of prior year findings is intended to be a status-oriented discussion of remediation progress rather than a full re-testing or validation exercise, and may include general guidance or feedback from the auditor.

8. Reporting Format Expectations

Audit observations should be presented in a clear, audit-style format appropriate for management and oversight audiences. Reports should clearly describe observations, associated risks, and recommendations in a manner that is understandable to both technical and non-technical stakeholders.

Primary audiences for audit reporting include IT management and executive leadership, with distribution to the Board or other affected functional areas as appropriate.

9. Pricing Structure

MMBB prefers that proposers submit pricing on a per-audit-area (a la carte) basis. Pricing will be used to support annual audit planning and to allow MMBB to evaluate anticipated costs over a multi-year audit cycle, while retaining flexibility to determine specific audit areas on a year-by-year basis.

MMBB has not designated a specific budget or grant amount for individual audit areas. Proposers should submit pricing in accordance with the RFP requirements.

10. Travel and On-Site Work

Remote audit procedures are preferred where feasible, with limited on-site presence for physical control reviews as needed.

Proposers may include estimated travel-related costs for any audit procedures that would require on-site presence, such as review of physical building or facility controls. MMBB has conducted both on-site and virtual reviews in the past, and on-site work is expected to be limited. Any travel costs should be clearly identified and itemized.

Any on-site travel, if required, will be coordinated in advance with MMBB and approved prior to incurring travel-related expenses.

11. Contracting Approach

MMBB does not currently require use of a standard professional services agreement for IT audit services. Historically, MMBB has executed an engagement letter with the selected firm that defines the audit scope, pricing, and applicable terms prior to commencement of audit activities.

12. Evaluation Criteria

MMBB does not apply fixed weighting to individual evaluation criteria. Proposals will be evaluated holistically based on experience, methodology, cost, and references to determine the best overall value to MMBB. While cost is a consideration, MMBB will not select a proposer based on cost alone.

13. Fieldwork Timing

IT audit fieldwork has typically been conducted in the spring. Timing is coordinated annually and planned to avoid peak periods for financial audits, IT operations, and other MMBB staff, with specific dates mutually agreed upon during annual planning.

14. Assumptions for Planning and Sampling

Assumptions related to interviews, sampling sizes, and systems in scope will be determined during post-award planning based on the specific audit areas selected and MMBB's risk considerations.

15. Public Records and Confidentiality

MMBB recognizes that proposals may be subject to disclosure under Maine's Freedom of Access Act (FOAA). Proposers are encouraged to avoid including sensitive technical or security-specific details in their proposals and reserve such information for post-award discussions, as appropriate.

The IT audit report is intended primarily for internal management and oversight purposes. Any disclosure or redaction considerations would be handled in accordance with applicable laws and MMBB policies.