Q1: Number of key controls – We saw in the RFP it specifies the number of control objectives; however, the biggest cost driver is really more dictated based upon the number of controls tested. This is typically the factor on which most firms base their budget on. Are you able to provide the specific number of key controls?

If possible, please provide a control count breakdown of IT and non-IT controls.

A: There are 16 total control objectives and 104 key controls. In addition, there are 5 IT control objectives with 34 key controls and 11 non-IT controls with 70 key controls.

Q2: Number of in-scope systems – Similar to #1, the number of systems which are necessary for review as part of IT General Control is a critical factor in assessing the amount of effort necessary for review. Can you please specify the number of in-scope applications?

A: There are 6 in-scope applications managed by RISLA and 2 additional applications used that are managed by carved-out subservice organizations. Please see the attached "Subservice Organization Control Considerations" from the prior audit that relates to the two subservice organizations.

Q3: Are any of the applications internally developed?

A: Yes, RISLA developed and maintains a loan origination system (LOS). This application supports a web portal providing a self-service module for potential borrowers. Online loan application and borrower information is automatically imported from the portal in the LOS to create an account for the borrower. The primary functions of the LOS are maintaining and viewing loan applications, maintaining borrower accounts, logging and processing loan change requests, and disbursing funds and generating notification letters.

Q4: If multiple systems/applications are in-scope, do IT controls (e.g. user provisioning, change management) follow a standardized/homogenous process across all systems?

A: Similar but not exact across all applications.

Q5: Are any subservice organizations in-scope? If so, how many?

A: See question 2.

Q6: Will the subservice organizations be evaluated using the carve-out or inclusive method?

A: See question 2.

Q7: What is the preferred method for sharing evidence? Will RISLA use its own document-sharing platform, or would you be open to using the service auditor's platform? Our internally developed evidence-sharing platform undergoes an annual SOC 2 examination.

A: Open to using service auditor's platform.

Q8: Will resources be required on site, or can the engagement be performed remotely by U.S.-based staff? If on-site is required, what are the expectations regarding timing and duration?

A: There are some elements that require your personnel to be on-site, mainly IT related testing. The timing and duration will depend upon the efficiency and experience of your staff to audit the required control objectives.

Q9: Will there be a single point of contact at RISLA to coordinate evidence collection, or should we expect to work directly with multiple control owners?

A: There will be multiple control owners depending on the control objective being tested.

Q10: Is there a budget range for this engagement that we should consider?

A: RISLA does not prepare a budget for this project.

Q11: Can RISLA provide the previously issued SOC1 report?

A: This cannot be shared as part of this RFP process.

Q12: If the SOC report can't be provided, below are specific questions we are hoping to be addressed:

Was PY report opinion modified for qualification, emphasis or a matter, or inclusive of a subservice organization? If so, will these matters overlap the period in scope for 1/1/25 – 12/31/25 and forward?

A: No.

Q13: Have there been any major changes during the period that would affect systems/applications in scope?

A: No.

Q14: Does RISLA allow the use of our Firm's offshore resources to assist in the SOC 1 report?

A: No.

Q15: Does RISLA have an Internal Audit Department that would assist in testing in any of the SOC controls for the examination?

A: No.

Q16: Does RISLA require resumes of our staff and seniors that would be assigned to the engagement to be included within our proposal?

A: Yes, see page 3 of the RFP that was posted.

Q17: Are there current contractual obligations from existing clients/lending institutions requiring the SOC report due March 1st?

A: No, this schedule is dictated by RISLA Management.

Q18: Historically, when has your service auditor performed the majority of the fieldwork and testing?

A: November and December.

Q19: Though an existing SOC report exists, does RISLA require readiness/gap assessment or controls workshop for the current period (RFP under Executive Summary mentions Readiness)?

A: No.

Q20: Control Objective 14 states an onsite server room. Does RISLA require auditors to be onsite for observation?

A: Please see question 8, as there are aspects of the audit that will require auditors to be on-site.

Q21: Control Objective 14, would RISLA consider the 'server room' to be the data center?

A: Yes.

Q22: Does RISLA leverage any cloud environments that are in scope for SOC (e.g. Azure, AWS)?

A: Please see question 2.

Q23: How many locations of RISLA execute loan servicing operations?

A: RISLA has one physical location for loan operations.

Q24: Does RISLA utilize any other major subservice organizations for scope of services such as IT services backup and recovery?

A: Please see question 2.

Q25: Will RISLA grant auditor access to their third-party servicing platform?

A: Yes, on a limited basis.

Q26: Can RISLA share what third-party platform they use for servicing loans?

A: University Accounting Systems.

Q27: Does RISLA use a GRC platform and if so, what is the name of the tool?

A: No.

Q28: Does the contracted software vendor issue a SOC 1 Type 2 or a SOC 2 Type 2 Report? If so, is it reviewed annually by RISLA?

A: The contracted software vendor issues a SOC 1 and SOC 2 that are both reviewed by RISLA annually.

Q29: Is RISLA interested in a consulting engagement to review and refresh the control set for the upcoming reporting periods? Typically recommended when a new auditor is taking over and there has been time that has been passed, and controls have been updated in operations but maybe not yet in the report.

A: All expenses related to a new auditor taking over need to be included in the RFP bid.

Q30: Will RISLA require assistance updating their system description (Section 3)?

A: No.

Q31: Should the pricing component be included as a proposal section, an appendix, or separately submitted file?

A: Per the RFP, Pricing shall include:

The bid is for a three-year contract, and the price should indicate the overall fixed price for the engagement as well as hourly rates and an estimated total number of hours for each category of assigned personnel (e.g. partner, manager, senior staff, etc.). Please include all travel and non-personnel costs in your price and if travel and other non-personnel costs are included, please list these separately so RISLA can differentiate the audit fees from travel costs. **Since the bid is for three successive reports (December 31, 2025, 2026, 2027) please list costs and hourly estimates per year separately.**

If all the above is submitted, RISLA does not have a preference for an appendix, separate section, or file.

Q32: Regarding pricing, the RFP mentions FFP and hourly rates. Can the agency please confirm what format they want for the pricing?

A: Please include a fixed price for the engagement and in addition, an estimate of the number of hours and rate for each category of assigned personnel that was used to determine the fixed price. This is only an estimate but is required so when we compare fixed prices, we can determine the approximate number of hours a bidder is dedicating to the project.