SDCERS

San Diego City Employees' Retirement System

San Diego City Employees' Retirement System
Request for Proposals for Execution of One to Five Information Technology Audits over a Three Year Period

The San Diego City Employees' Retirement System ("SDCERS") invites proposals from experienced internal auditing firms in response to this Request for Proposals ("RFP") to provide internal audit services in conducting one to five information technology audits over a three year period.

I. BACKGROUND

A. <u>General Background Information:</u>

SDCERS is a tax-qualified, charter-created public retirement system for the employees of the City of San Diego ("City"), the San Diego Unified Port District ("Port"), and the San Diego County Regional Airport Authority ("Airport"). Since 1927, SDCERS has provided retirement, disability, and death benefits to its roughly 20,000 participants, which include general, safety, and elected officer members. Employees of the Port became members of SDCERS in 1963, and employees of the Airport became members in 2003. It is a contributory system; the contributions to fund the System are paid by the City, Port and Airport, and their respective employees. SDCERS' Board of Administration ("Board") is currently responsible for managing $7 billion in trust fund assets. The Board administers the defined benefit plans of public employees and their survivors under the City, Port and Airport plans. For more information, see SDCERS' Comprehensive Annual Financial Report and other documents at www.sdcers.org.

SDCERS has 50 full-time employees across eight Divisions. The Information Technology Division is under the supervision of the Chief Information Officer/Chief Information Security Officer. Also included within the Information Technology Division is an Application Services Program Manager, an Information Systems Administration Manager and outside Information Technology contractors that assist SDCERS with its operations.

B. <u>IT-Specific Background Information:</u>

SDCERS has a single location in downtown San Diego with a dedicated datacenter hosting network equipment, servers, applications and data. The datacenter has dedicated HVAC and humidity controls as well as a dedicated argon fire suppression system and uninterruptable power supply battery backup power. SDCERS' network is operated as a semi-autonomous, trusted subnetwork of the City of San Diego's overall network. SDCERS physically connects to the City's network using Active Directory authentication over an Opt-e-man circuit linked to the City's core network. SDCERS' network is partitioned off of the City's wide area network by firewalls. SDCERS utilizes spam firewalls to protect its email system. SDCERS' backs up its systems from disk to tape. Tape backups are rotated weekly to Iron Mountain offsite storage. SDCERS has two internal VLANs: one for operations and one for our Board of Administration system. SDCERS uses extensive virtualization to run our systems.

SDCERS contracts with CGI for application support, Zensar for voice and data services, and Atos Solutions server, desktop and email support. Primary applications include pension administration software, accounting software and document management software.

SDCERS has banking relationships that require separate authentication onto the bank's respective websites.

SDCERS' Internal Audit Division

SDCERS employs one, full-time Chief Internal Auditor who develops an Audit Plan based on a risk assessment. That Audit Plan is designed to cover high-risk activities or areas where the Chief Internal Auditor could have the greatest impact, while limiting the scope of work to what can realistically be accomplished during the fiscal year. SDCERS hired an IT Internal Audit consultant to aid in the IT risk assessment and IT audit planning process for FY2020, FY2021 and FY2022. As a result of this collaboration, the FY2020 Risk Assessment identified 23 IT Key Work Activities, three of which were ranked as a top 15 risk out of approximately 125 Key Work Activities.

External Audit Work

In conjunction with the external auditor's annual financial statement audit, SDCERS IT Division completes an IT Risk Assessment Tool and an IT Environment General Computer Controls Form. The IT Division also provides the external auditors with user access rights, system audit logs, policy and procedure documentation and SDCERS' Business Continuity Plan. The NIST based IT Risk Assessment Tool contains nine separate categories with over 40 questions relating to: security program governance, systems certifications, physical access monitoring and disaster recovery planning. SDCERS' external auditors validate a random sample of system access rights for proper controls. External auditors provide written findings for any IT deficiencies. <u>However, the external auditors do not provide SDCERS any assurances on IT.</u>

IT Risk Assessment

SDCERS issued a request for proposal and selected a vendor to conduct an IT Security and Privacy Risk Assessment ("IT Risk Assessment") which was completed in June of 2017. The IT Risk Assessment was completed by the vendor based on a set of standards or guidelines (NIST 800-53) and resulted in 35 security and privacy related recommendations. The majority of the recommendations have been implemented, but other than one, confidential USB Access internal audit completed in August of 2017, no independent findings or assurances have been provided since.

External Penetration Testing

SDCERS hired an external firm in December of 2017 to perform *website* penetration testing and the contract was renewed in December of 2018. Penetration testing simulates a variety of cyber-attack methods under controlled conditions to identify any vulnerability at SDCERS. Testing by the firm includes use of specific, named test accounts to login to applications to attempt to find vulnerabilities and otherwise compromise systems from within applications.

Vulnerability Scans

SDCERS' IT Division engages the Department of Homeland Security (DHS) to perform weekly vulnerability tests. SDCERS consistently receives at or near DHS' top overall security score. The IT Division provides Status Reports and test results at each Audit Committee meeting.

Network Device Scanning

SDCERS IT performs continuous network device scans on all assets connected to its network using an industry leading product. The scanner identifies a myriad of vulnerabilities including software flaws, missing patches, malware, and misconfigurations across operating systems, devices and applications.

Antivirus Scanning

SDCERS IT performs continuous antivirus scans on all desktops and servers using an industry leading product. The antivirus scanner identifies vulnerabilities including missing patches and identifies and remediates malware.

Patch Management

SDCERS IT performs monthly desktop and server updates to system in conjunction with Microsoft's release cycle.

Inventory Management

SDCERS IT maintains a continuous inventory of software and hardware devices using industry-leading software.

II. SCOPE OF SERVICES

A. General Requirements

SDCERS Internal Audit is seeking the services of qualified and independent firms to lead and assist in conducting one to five audits over the next three fiscal year as summarized within **Section B** below and, more specifically, in **Attachment A**.

The successful respondents will provide specialized skills, industry and subject matter knowledge to perform the engagement(s) and shall apply industry best practices and methodologies (e.g. National Institute of Standards and Technology [NIST 500-83] and American Institute of Certified Public Accountants [AICPA]). The engagement(s) should be planned to incorporate "knowledge transfer" to the SDCERS Internal Audit department.[1] All responding firms must meet the highest standards of professional competence and ethics.

The firms will be expected to plan, conduct fieldwork and report the results of the audit. Services are anticipated to include, but are not limited to the following:

1. Preparation and completion of a robust risk control matrix
2. Preparation and completion of a detailed testing plan ("audit program") and working papers
3. Review of any potential issue(s) resulting from the risk assessment and/or testing procedures
4. Review of applicable SDCERS information technology policy and procedure documentation
5. Written audit report addressed to the Audit Committee describing the results of the engagement(s)
6. Potentially presenting the final report to the Audit Committee

[1] For the FY2020 IT Audit Plan, the Chief Internal Auditor allocated a total of 110 hours to assist on the IT audit, 70 hours for the IT General Controls Audit and 40 hours for the Internal and External Network Penetration Testing. Assistance includes but is not limited to project management, testing or reporting.

Deliverables to be provided to SDCERS Internal Audit will include the final audit documentation comprised of risk control matrices, audit programs, testing working papers, and final reports.

In addition to the foregoing, core skills and expertise of the firms shall include excellent oral and written communication skills, sound judgment, the ability to work well with and maintain the confidence of the Audit Committee and staff, and the ability to deliver services in a timely and cost effective manner.

B. Specific Requirements

The following IT Audits have been planned for the next three years, subject to updated risk assessments:

Audit Name	Fiscal Year	Estimated Hours	Estimated Duration	Target Start Month
IT General Controls Audit	2020	250	6 – 8 Weeks	Nov 2019
Internal & External Network Penetration Testing	2020	120	4 – 6 Weeks	March 2020
Operating Effectiveness of 2017 Security Risk Assessment Remediation	2021	170	6 – 8 Weeks	TBD**
Business Continuity Plan Review	2021	250	6 – 8 Weeks	TBD**
Data Privacy Review	2022	250*	6 – 8 Weeks	TBD**
*This is meant to be an integrated review (IT and Operational). Hours include IT-related hours as well as non-IT related hours. **Target Start Month will be determined at the onset of the fiscal year and will likely be between November and April of the respective fiscal year.				

For additional details, including the audit's objectives and high-level scope, please see Attachment A.

III. CALENDAR OF EVENTS

Issuance of RFP	August 14, 2019
Applicant Questions Due	August 30, 2019
Answers to Questions Published	September 13, 2019
Proposal Due Date	September 27, 2019
Interview/Expected Decision	September 30 - October 4, 2019

IV. PROPOSAL REQUIREMENTS

In setting forth its qualifications, you must provide the information described below. SDCERS may deem a proposal non-responsive and reject the proposal if it does not include all requested information.

A. Proposal Submission

Proposals must include a cover letter indicating the mailing address of the office submitting the proposal, the name of the individual who will represent the firm as the primary contact person for the proposal, and the telephone, fax and e-mail information of the primary contact person.

The proposal cover letter must state that the proposal is irrevocable for 180 days and be signed by an authorized person.

Three bound hard copies and one electronic copy (in PDF format on a flash drive or disk) of your proposal are due no later than **5:00 p.m.** PST on the due date listed above. All proposals must be delivered to:

San Diego City Employees' Retirement System
Attention: Sarah Dickson, Chief Internal Auditor
401 West A Street, Suite 400
San Diego, CA 92101

SDCERS reserves the right not to consider proposals received after this deadline, however received.

B. General Minimum Requirements

SDCERS will accept proposals from firms that meet the minimum requirements listed below:

1. The firm must have IT internal auditing experience.

2. The firm must not have, or potentially have, a material conflict of interest, which includes, but not limited to: SDCERS' Trustees, staff, actuary, auditor, or consultants.

3. The firm must carry $15 million in errors and omission insurance coverage.

C. Questions To Be Answered

1. Please provide a brief history of the firm including the year organized, the year the firm began providing internal auditing services to U.S. clients, the total number of professionals, and the other services your firm provides.

2. Please indicate which office would service the account, the names of the team members who would be assigned to this account, their years of IT internal auditing experience, and their contact information.

3. Please indicate whether any portion of the work will be subcontracted, if yes, disclose the name(s) of the subcontractor(s), the service(s) to be subcontracted and how the contractor controls costs, quality, timeliness and confidentiality of these services.

4. Provide two client references relating to engagements similar to the one you are proposing to SDCERS. In providing this information, you consent to and release SDCERS from liability regarding contacting your references and communicating with them about your prior engagements and their opinions regarding your work performed. Please include: Name of firm, address, telephone number, and contact person.

5. List the public pension plans the firm has represented and describe the type of work performed.

6. Identify any potential or actual conflict of interest you have in providing services to SDCERS. Also, state whether you have ever represented SDCERS, the City, the Port, the Airport, or any employee group related to these entities. If so, state the name of each such client, contact information, and the nature and time frame of your representation. In providing this information, you consent to and release SDCERS from liability regarding contacting the client(s) and communicating with them about your current or prior engagement(s) and conflict(s). Also, please describe how you intend to resolve any actual or potential conflict of interest.

7. Identify any past, pending or threatened litigation or administrative or state ethics board or similar body proceedings to which you, your firm or any of the professionals listed above are a party related to performing services.

D. Proposed Fee and Billing

Proposals must contain the following:

1. Fee information in two ways:
    a. By audit, based upon each audit's objectives, estimated hours and high-level scope as documented in **Attachment A**. Include a "not to exceed" price by audit. All anticipated fees for travel should be included in the itemization by audit. Treat the audits as if they are severable.
        1. For the "Data Privacy Review" (last item listed in **Attachment A**), split-out the fees between operational versus IT in the event the SDCERS Internal Audit Division can perform the operational portion of the audit.

    b. By fiscal year, as if you were executing all five audits based upon each audit's objectives, estimated hours and high-level scope as documented in **Attachment A** (only if different than the cumulative price provided in 1a above). Include a "not to exceed" price by fiscal year. All anticipated fees for travel should be included in the proposal.
        1. For the "Data Privacy Review" (last item listed in **Attachment A**), split-out the fees between operational versus IT in the event the SDCERS Internal Audit Division can perform the operational portion of the audit.

Please consider the small size of SDCERS when estimating fees.

2. Professional hourly rates based on staff classification (e.g. partner, principal, manager, staff).

3. If there are services that are NOT described in the Scope of Services in this RFP, but are required for the successful completion of the services, those services should be sufficiently described in your proposal.

4. Applicable billing rates for additional services that may be requested by SDCERS on an as needed basis outside of the RFP. Should additional services be requested by SDCERS, the scope of work and estimated fee must be agreed upon in advance.

5. Special considerations with respect to billing or payment of fees and expenses that you offer and that you believe would differentiate you from other Applicants and make your services more cost effective to SDCERS.

6. Reasons you are not prepared to provide the lowest rate charged for your governmental and non-profit clients.

V. EVALUATION AND SELECTION

A. Evaluation Criteria

The Board or Staff will evaluate the proposals based upon the following factors:

1. Overall organization, completeness, and quality of proposal, including cohesiveness, conciseness, and clarity of response.

2. Professional qualifications and experience of the firm and assigned personnel.

3. Accessibility of assigned personnel to SDCERS on an on-going basis.

4. Anticipated cost of services, including hourly rates, discounts and cost-effectiveness.[2]

5. Information provided by references.

B. Selection Process

Staff will review all proposals to determine timeliness and completeness. Any proposal that does not address all requested requirements or is untimely may be rejected, at SDCERS' sole discretion. Staff will evaluate all proposals based on the criteria stated above.

Staff and the Board may interview applicants it believes are qualified to perform the services requested. Applicants selected for interviews will be notified in advance of the proposed interview date.

[2] Although proposed fees will be given weight in the selection process, SDCERS reserves the right to negotiate with any applicant selected lower fees or a different fee structure than proposed.

VI. PROPOSAL LIMITATIONS AND CONDITIONS

A. Limitations

This RFP does not commit SDCERS to award an agreement, pay any costs incurred in the preparation of a response, or procure services of any kind whatsoever. SDCERS reserves the right, in its sole discretion, to negotiate with any or all applicants considered, or to postpone, delay or cancel this RFP in whole or in part. SDCERS may terminate negotiations, at its sole discretion. SDCERS reserves the right to award an agreement or agreements based upon proposals received; you should not rely upon the opportunity to alter your proposal (e.g., services, fees, etc.) during negotiations.

SDCERS may request an applicant to clarify the contents of its proposal. Other than to provide such information requested by SDCERS, no applicant will be allowed to alter its proposal after the RFP due date.

All material submitted in response to this RFP is the sole property of SDCERS. SDCERS reserves the right to use any and all ideas submitted in the proposals received.

SDCERS may waive informalities or irregularities in a proposal, at SDCERS' sole discretion.

B. Errors and Omissions

If you discover an ambiguity, conflict, discrepancy, omission or other error in this RFP, immediately notify Sarah Dickson at Sdickson@sdcers.org and request clarification or modification of the document.

If it deems necessary, SDCERS may modify this RFP. Notice of any modification will be given by written notice to all applicants who have furnished a proposal or notice of intent to propose.

If an applicant fails to notify SDCERS of a known error or an error that reasonably should have been known before the final filing date for submission, the applicant assumes the risk. If awarded an agreement, the applicant will not be entitled to additional compensation or time by reason of the error or its late correction.

VII. AGREEMENT APPROVAL

SDCERS' selection of one or more successful applicants will not be binding until it has been approved by authorized Staff, Committee or the Board. Any direction by SDCERS Staff, Committee or the Board to enter into a contract is not a binding contract unless negotiations result in agreement by all parties.

VIII. GENERAL INFORMATION

A. No Contact

No contact with SDCERS' Board of Administration, staff or consultants relating to the RFP is allowed while this RFP is pending, except as expressly allowed herein. Any contact relating to the RFP with said persons is grounds for disqualification. Notwithstanding, you may submit written questions via e-mail to Sarah Dickson, Chief Internal Auditor, at Sdickson@sdcers.org on or before the date listed above next to "Applicant Questions Due." Staff will publish answers to any questions received on its website (www.sdcers.org) on the date listed above next to "Answers to Questions Published."

B. No Reimbursement For RFP Expenses

SDCERS will not reimburse any expenses incurred in responding to this RFP including the costs of preparing the response, providing any additional information, or attending an interview or interviews.

C. Notice Regarding The California Public Records Act And Open Meetings Laws

The proposal you submit in response to this RFP will be subject to the California Public Records Act (Cal. Gov. Code §6250 *et. seq*., the "Act"). The Act provides that all records relating to a public agency's business are open to public inspection and copying, unless an exception applies. In addition, if SDCERS chooses to hire or recommend you for hiring, your proposal may appear in a publicly posted agenda packet for a public meeting in accordance with the Ralph M. Brown Act (Cal. Gov. Code §54950 *et seq*.). If it is included in the agenda packet, your proposal will not be exempt from public disclosure. If a request is made pursuant to the Act for materials you have submitted, SDCERS will determine, in its sole discretion, whether the materials are subject to public disclosure. If SDCERS determines that the materials requested are not subject to disclosure under the Act, SDCERS will either notify you so you can seek a protective order at your own cost or expense and/or SDCERS will deny disclosure of those materials. If SDCERS denies disclosure, then by submitting your proposal you agree to reimburse SDCERS for, and to indemnify, defend, save and hold harmless SDCERS, its officers, trustees, fiduciaries, employees, and agents from and against any and all claims, damages, losses, liabilities, suits, judgments, fines, penalties, costs, and expenses including, without limitation, attorneys' fees, expenses and court costs of any nature whatsoever (collectively, “Claims”) arising from or relating to SDCERS’ non-disclosure. By submitting your proposal, you also agree to indemnify, save, and hold SDCERS harmless from and against any and all Claims arising from or relating to SDCERS’ public disclosure of any such designated portions of your proposal if SDCERS determines disclosure is required by law, or if disclosure is ordered by a court of competent jurisdiction.

IX. AGREEMENT PERIOD

Either Party may, in its sole discretion, terminate the agreement at any time, subject to California law, including ethical obligations to protect SDCERS’ interests in the process of withdrawing.

Attachment A

FY2020-FY2022 IT AUDIT PLAN

Audit Name	Objective	Target Time Period	Key Work Activities	Est. Hours	Est. Duration	Notes
IT General Controls Audit	Evaluate the design and operating effectiveness of IT general controls, focusing on logical and physical security, IT operations, and software development and change management.	FY 2020	Project Management, Change Management, Application and Systems Security, Identity Management, Backup and Recovery Management, IT Operations	250	6-8 weeks	Assess the operating effectiveness of IT general controls. Four systems will be in scope. Areas covered will be: 1. Logical and Physical Security 2. Software Development and Change Management 3. IT Operations 4. Project Management (PM)
Internal and External Network Penetration Testing	Evaluate network security risks by identifying critical vulnerabilities on the organization's external and internal presence and conducting network penetration testing.	FY 2020	Network Security	120	4-6 weeks	Attempt to: 1. Breach the organization by acting as an unauthorized user, with the ultimate goal of compromising your networks and data. The tests seek to exploit weaknesses in systems. Obtain access to sensitive data and systems. 2. Gain administrative access over the network. 3. Determine the ability of an attacker to exfiltrate data undetected outside of the network. 4. Identify critical application vulnerabilities on externally facing applications.** **Application testing included as part of the external penetration testing is not a substitute for a dedicated application penetration test.
Operating Effectiveness of 2017 Information Security Risk Assessment Remediation	Evaluate the operating effectiveness of security and cybersecurity related remediation efforts implemented by management as a result of the 2017 Information Security and Privacy Risk Assessment, and assess whether remediation efforts have been integrated into the IT division's internal processes.	FY 2021	Infrastructure and Asset Management, Event, Incident, and Problem Management, Data Privacy and Protection	170	6-8 weeks	Focus will be on Security findings and recommendations (count of 19).

Attachment A

Audit Name	Objective	Target Time Period	Key Work Activities	Est. Hours	Est. Duration	Notes
Business Continuity Plan Review	Evaluate the overall effectiveness of the organization's Business Continuity Plan (BCP) by assessing the general approach, appraising the recovery planning roles and responsibilities, reviewing the established program and materials, assessing the business impact analysis, evaluating the assessment of disaster risks and related mitigation measures, evaluating selected recovery strategies, assessing documentation and recovery procedures, evaluating the testing program, and assessing overall BCP awareness and knowledge.	FY 2021	Business Continuity Planning	250	6-8 weeks	The primary objectives are to: 1. Assess the general approach to business continuity planning for completeness and inclusion of appropriate program policies and elements. 2. Appraise the recovery planning roles and responsibilities for relevance and effectiveness in directing and managing the business continuity planning program. 3. Review the established program for maintaining the BCP documentation and related materials and provisions. 4. Assess the business impact analysis (BIA), including the identified critical functions and their associated resource requirements. 5. Evaluate the assessment of disaster risks and the analysis of the organization's mitigation measures. 6. Evaluate the selected recovery strategies for correlation to the defined requirements and thoroughness of implementation. 7. Assess the BCP documentation, including the procedures for restoring critical resources and resuming business operations. 8. Evaluate the testing program that has been implemented to periodically validate the business continuity planning provisions. 9. Assess the organization's efforts to promote awareness and knowledge of the BCP.
Data Privacy Review	Evaluate the privacy program and controls against the AICPA's trust services criteria for privacy. The review will focus on providing recommendations to better align the organization with the generally accepted privacy principles.	FY 2022	Data Privacy and Protection	250	6-8 weeks	Evaluate the privacy program against the privacy criteria organized as follows: 1. Notice and communication of objectives 2. Choice and consent 3. Collection 4. User, retention, and disposal 5. Access 6. Disclosure and notification 7. Quality 8. Monitoring and enforcement