CHICAGO ZOOLOGICAL SOCIETY
REQUEST FOR PROPOSAL (RFP) FOR
PCI GAP ANALYSIS

The Chicago Zoological Society is soliciting proposals for payment card industry ("PCI") compliance and security audit services. The Society is seeking consulting and advisory services to analyze, audit, validate and verify, and assist with documenting the current state of information security, as well as provide any necessary remediation support to fill in any identified gaps in order to meet PCI Compliance Standards.

This document outlines the Society's guidelines for your responses. The Proposal must be submitted no later than close of business on August 20, 2018. All questions and responses to the RFP must be addressed to:

B. Todd Oakley
Sr. Manager, Information Technology
Chicago Zoological Society
3300 S. Golf Road
Brookfield, Illinois 60513

708-688-8306
Todd.Oakley@czs.org

Organizational Overview

The Chicago Zoological Society ("CZS" or "the Society") is a private nonprofit organization that operates Brookfield Zoo on land owned by the Forest Preserves of Cook County. Opened to the public in 1934, Brookfield Zoo has been a Chicago-area treasure and family destination for more than 75 years. Brookfield Zoo is the largest suburban attraction in Cook County, both in size and visitation. The 216-acre Zoo annually serves over two million visitors from the diverse Chicago metropolitan area. The zoo is open 365 days a year. On an average day, more than 11,000 people visit during the Zoo's peak attendance season in the summer months.

The Society's mission is to inspire conservation leadership by connecting people with wildlife and nature. We strive to provide people of all ages and backgrounds with opportunities to learn about and care for the natural world. When it first opened, Brookfield Zoo was considered "cutting edge" for its bar-less enclosures. One of the first zoos to employ nutritionists, pathologists, veterinarians, geneticists, endocrinologists, and behavioral specialists, we continue in a tradition of innovation.

Project Description

Goals and Objectives

The Society has been engaged in establishing and maintaining payment card industry data security standards ("PCI DSS") compliance since 2010. It has been determined that the appropriate next step is to perform a current and future state gap analysis, including physical, logical and technical security, as well as documentation surrounding said security.

The purpose of this Request for Proposal is to invite qualified service providers to prepare and submit a proposal to provide the following professional consulting services related to PCI DSS and payment application data security standards ("PA DSS"): PCI compliance services performed by a qualified security assessor ("QSA"), ("QSA Compliance Services") and internal vulnerability and penetration testing services, to the Society, in accordance with the requirements defined throughout this RFP.

CZS RFP FOR PCI GAP ANALYSIS

In Scope

1. *Provide a PCI DSS gap analysis for the Society; An accurate and thorough assessment of
    a. the potential risks and vulnerabilities to the confidentiality, integrity, and availability of cardholder data (CHD).
    b. the current network architecture.
    c. the documentation and change management processes.
2. Provide PCI DSS onsite audit resulting in a Report on Compliance for the Society; validate that vulnerabilities and risks identified have been mapped to appropriate areas of the current version of the PCI DSS.
3. *Provide PCI DSS remediation advisory services for the Society.
4. *Provide security policy review and advisory services as it relates to PCI DSS Compliance.
5. Provide the Society risk assessment advisory services.
6. Provide point-to-point encryption (P2PE) gap analysis.
7. Provide P2PE implementation advisory services.
8. Provide consulting and advisory services for the development, implementation and isolation of PCI environments, applications, and services.
9. *Provide onsite and remote PCI training for the Society.
10. Provide baseline penetration testing, results and recommendations, both internally and externally.
11. Provide advisory services and guidance regarding internal vulnerability testing.
12. *Provide advisory services to identify, document policies, procedures and assist with implementation of any recommended compensating controls.
13. *Review the structure of the Society's PCI overview-bodies (i.e. steering committee and subgroups) to determine if the structure is appropriate.
14. Review the steering committee's project lists and provide guidance on the appropriate prioritization.
15. *Provide any other QSA services necessary to establish and/or maintain conformity to PCI standards and approved by the Society that are not specifically mentioned in this RFP.
16. Provide a proposed project timeline.

Respondents should clearly identify in their submittal which services are to be performed onsite and which are or can be accomplished remotely, as well as which services will be provided by a sub-contractor. Also, if sampling is part of the preferred methodology, define when and how sampling will be used.

The requirements of this engagement are to:

- Assist with defining the scope of PCI compliance for the organization as well as consulting on how to reduce scope.
- Determine how effectively the organization is maintaining security, integrity, confidentiality and availability of cardholder data according to the current version of the PCI DSS.
- Determine how effectively the organization is protecting against anticipated threats or hazards according to the current version of the PCI DSS.
- Determine how effectively the organization is protecting against unauthorized access to information according to the current version of the PCI DSS.
- Provide guidance for policy and procedure creation and assist with the drafting and iteration of the same.
- Provide written recommendations and/or a remediation plan to the organization to meet or exceed the current version of the PCI DSS.
- Propose a plan to monitor compliance, provide guidance on updates related to laws and regulations, and review compliance status within timeframes stipulated under the various laws and regulations.
- Provide samples of deliverables (with confidential information removed) typically provided in Respondent's prior PCI engagements.

CZS RFP FOR PCI GAP ANALYSIS

Out-of-Scope

- Completion of an Attestation of Compliance
- Ongoing Penetration and/or Vulnerability testing
- Ongoing Society staff training

RFP Deliverable Components

Each responding bidder should be sure to provide the following details in the proposal.

1. Executive Summary: The Executive Summary should include a clear statement of the Consultant's understanding of the RFP including a summary of the Scope of Work. Include, at a minimum, an outline of the contents of the proposal, an identification of the proposed project team, a description of the responsibilities of the project team, and a summary of the proposed services.
2. Organization background
    a. Company history
    b. Briefly introduce your firm, providing a summary of the administration, organization and staffing of your firm, including multiple offices, if applicable. Provide an organizational chart indicating the positions and names of the core management team which will undertake this engagement.
    c. Provide the background on how long your firm and/or individuals in your firm have been an active credentialed and certified PCI DSS QSA.
    d. Respondent is to provide a narrative description of a minimum of three (3) previous projects the Respondent has completed in the past five (5) years to demonstrate the Respondent's capability and qualifications to successfully complete the anticipated work. If experience levels of respondents accommodate, particular emphasis will be placed on firms that have performed PCI DSS QSA services for not-for-profits.
    e. Proposed team profiles and roles.
        i. Identify the project manager and each individual who will work as part of this engagement. Include resumes for each person to be assigned. Include any professional designations and affiliations, certifications and licenses, etc., including PCI DSS QSA credentials.
        ii. Describe the organization of the proposed team, detailing the level of involvement, field of expertise, and estimated hours for each member of the team.
    f. Describe your customer service and quality control programs.
3. Scope
    a. Describe how you will provide the aforementioned deliverables from the scope of services.
    b. Describe what Society staff support you anticipate for the project.
    c. What tools (i.e., technical devices, software, questionnaires, etc.) do you use when making assessments? Do you provide these tools to the Client for future use?
4. Cost estimates.
        a. Provide a proposed fee schedule. Express your administrative fee in lump sum not-to-exceed maximum amount and a separate price for travel and related expenses.
        b. Indicate your specific expectations concerning reimbursement for travel, per diem expenses, printing, video conferences, and other incidental expenses for the firm.
        c. Respondent shall incur no travel or related expenses chargeable to the Society without prior approval by an authorized Society representative.
        d. Related expenses chargeable to the Society, such as supplies, printing, binders, etc. shall be passed through at Respondent's cost. Related expenses shall not include postage, copies, telephone toll charges, or other charges incurred in the normal course of business and shall not be charged.

5. References
    a. Provide three references and contact information to verify consultant's direct experience in servicing accounts of a similar size, complexity, and business volume to the Chicago Zoological Society, based on the options specified in this RFP. Ensure that contact information includes name, title, address, e-mail address, and phone number of each reference and that you have verified that this is current information for these individuals/companies

Timeline

This RFP is being distributed starting the week of July 22, 2018. Responses are due no later than 5 pm August 20, 2018. Partner selection is expected to be completed by mid-September with a project kick off starting in October.

Depending on responses and queries, we may choose to conduct a bidder conference call in August or September.

Required Proposal Response Format

You may upload one (1) electronic proposal in the format pre scribed herein on our website at http://www.czs.org/RFP/. However, if you choose to respond in writing, one (1) original, three (3) copies and one (1) electronic version (Flash drive, etc.) of the proposal should be returned in a sealed envelope bearing the RFP name, and name and address of the respondent on the outside of the delivery package.

Basis for Award of Contract

The Society will award the contract to the proposal which demonstrates the best combination of price, experience and creativity.

Evaluation of the Proposals will be conducted by an evaluation team. The evaluation criteria are as follows:

- Overall cost effectiveness of the Proposal.
- Feedback based on responses provided by Proponent's customer references
- Demonstration of a clear understanding of the project, the scope of work, its objectives and the purpose for conducting the work.
- Demonstration of the financial and technical capabilities of the Proponent to complete the project satisfactorily and on time.
- Provision of a detailed account of recently completed projects of a similar scope and nature, including the methodology which was used to achieve objectives, and, if applicable, explain any methodology changes being brought to the proposed approach.
- How the Proponent intends to keep the Society informed of project progress and any evolving issues throughout the course of the project.

All Proponents will be advised in writing of the success or failure of their respective Proposals.

CZS Reservation of Rights

CZS reserves the right to reject any or all proposals, without explanation, to waive irregularities and to accept a proposal which, in CZS' sole judgment, is in the best interest of CZS.

MBE/WBE/DBE/8(a)

The Chicago Zoological Society is committed to ensuring that certified minority-owned business enterprises (MBE), women-owned business enterprises (WBE), disadvantaged business enterprises (DBE), and U.S. Small Business Administration 8(a)-certified (8(a)) firms are afforded opportunities to compete for and participate in the Chicago

Zoological Society's purchasing activities. If your company is certified as an MBE, WBE, DBE or 8(a) company, please send your current certification with your response to this RFP.

Vendor References

No less than three (3) partner or client references should be provided.