PROPOSAL FROM THE CONSULTING COMPANY

The Entertainment Company Compliance and Remediation

JULY 11, 2020

The Entertainment Company

NOTICE TO THE RECIPIENT OF THIS PROPOSAL

The information contained herein, as well as any information shared by The Consultant Company in furtherance of this proposal or relating to this subject matter, are the proprietary and confidential information ("Confidential Information") of The Consultant Company America, Inc., and their release would offer substantial benefit to competitors offering similar services. The Confidential Information includes descriptions of methodologies and concepts derived through substantial research and development efforts undertaken by The Consultant Company. It is the position of The Consultant Company that this proposal and/or Confidential Information are not considered subject to release under the Freedom of Information Act, if applicable. Recipient shall use this proposal and/or any Confidential Information solely for the purpose of evaluation for contract award. In the event that The Consultant Company and Recipient are not otherwise parties to a non-disclosure agreement which protects The Consultant Company's Confidential Information herein, Recipient agrees to maintain in confidence and not to disclose the Confidential Information except to its employees or agents on a "need to know basis." Your acceptance of the submissions of this proposal and evaluation thereof indicates your agreement to these terms.

Neither submission by The Consultant Company nor your acceptance of this proposal, in whole or in part, constitutes acceptance by The Consultant Company of any contractual terms contained in your Request for Proposal, if any, and shall not form a binding agreement between the parties, other than with respect to confidentiality as set forth herein. Such an agreement shall only exist upon the execution of a mutually acceptable contract by both parties. Except as otherwise set forth in such a contract, The Consultant Company makes no representations or warranties to you.

The term "The Consultant Company" appearing in this proposal may refer to The Consultant Company America, Inc., or to one or more of its global affiliates; however, this proposal is being submitted by only The Consultant Company America, Inc., which is solely responsible for its contents and The Consultant Company America, Inc. shall be the contracting entity if this proposal is selected.

The Consultant Company

Table of Contents

Executive Summary and Key Differentiators

The Consultant Company ("The Consultant Company") is pleased to respond to Entertainment Company ("Entertainment Company") Technology's Compliance and Remediation RFP. The Consultant Company has been and would continue to be a trusted service provider of a Managed Services Model that effectively and efficiently provides Compliance and Remediation Services to Entertainment Company. Our focus will be on consistent performance, cost savings and continuous improvements. We are pleased to provide a detailed overview of our Approach and Engagement Model, and we thank you for the opportunity to present this proposal for your consideration.

Since 1999, The Consultant Company has been building a history of successful collaboration with the Entertainment Company. As a result of providing services to multiple areas of Entertainment Company's business, (as depicted in Figure 1 below) The Consultant Company has come to keenly understand the overall business and to appreciate the compliance requirements to safeguard the data of guests and cast members. Currently we have a team of over 100 onsite and 350 offshore staff dedicated to the needs of the Entertainment Company.

Cybersecurity Global Service Line

The Consultant Company launched its Cybersecurity Global Service Line in February of 2015. Our 2,500 cybersecurity professionals are 100% focused on protecting the business of customers like the Entertainment Company. We have built an end-to-end cybersecurity services portfolio.

Safeguarding today's digital business with end-to-end advisory, protection and monitoring security services across critical areas of Identity & Access Management, Applications, End-points and Infrastructure.

We advise and control. We protect. We monitor.

Advise and Control - making sure your cybersecurity strategy is fit for purpose and in line with both your appetite for risk and your budget. From cybersecurity maturity and health assessments, to roadmaps, risk assessments and information asset inventories, including security controls such as pentests and audits, our consulting services are designed to help you make the right choices about what to prioritize and where to invest;

Protect - our cybersecurity protection services design and build the defenses you need to safeguard your data, IT systems, industrial systems and enterprise, throughout your applications, end-points, data-centers and Identity & Access Management;

Monitor - gain situational awareness of how your security controls are operating and the threats you face with our security supervision services. You will detect and react efficiently to cyber-attacks and transform securely. Understand and manage the risks on your digital journey as you exploit the power of the internet while guarding against cyber-attacks.

Our Compliance Journey with the Entertainment Company

The Consultant Company appreciates the trust the Entertainment Company placed in our Compliance team 20 months ago as we began working together delivering compliance and remediation support. Our extended team of compliance professionals are deeply committed to continuing this journey with The Entertainment Company. This proposal includes enhancements to our existing delivery model resulting from our experience working side-by-side with The Entertainment Company strategists and leadership. We are proud of our joint accomplishments and the business value we have created, including:

- Establishing the requisite governance structure and team of compliance professionals (CISA's)
- Managing the Knowledge Transfer activities leading up to "Go-live" in January of 2015
- Formalizing the work activities in each of the compliance programs
- Ensuring value creation, using the most cost effective resource mix
- Maturing our joint onshore and offshore delivery model

We are also acutely aware of the lessons we have learned, and the additional enhancements needed as we continue our journey and grow value.

- Deepening our pool of compliance professionals to support The Entertainment Company
- Expanding onshore support to meet periods of peak demand
- Regularly bringing process innovation and industry insights to the table

Understanding Your Objectives

Entertainment Company's business objectives and value expectations set forth in the RFP are very clear. The Consultant Company is uniquely positioned with insights to the Entertainment Company Security and Compliance teams. Having the context of a larger relationship supports and strengthens the delivery of our Compliance and Remediation Support Services. Our compliance professionals will

leverage the existing The Consultant Company account governance structure. We have benefited from strong leadership relationships based on highly compatible corporate values.

Our tailored Compliance and Remediation Support solution is designed to meet the objectives and expectations of The Entertainment Company Compliance:

- ☑ Third-Party Provider with Experience
- ☑ Certified Compliance Professional
- ☑ PCI – Understanding and Experience
- ☑ XOX – Understanding and Experience
- ☑ EU Data Privacy – Understanding and Experience
- ☑ Compliance Education Tailored for Technical Teams
- ☑ Equipped to Expand into Growing Areas of Compliance
- ☑ Flexible to Meet Peak Periods of Activity
- ☑ Support Across Time Zones

We also understand the broader objectives and drivers within our relationship:

- ☑ Delivering Sustained Economic Value
- ☑ Focusing "Cast Members" on the Strategic Business Initiatives
- ☑ Reducing "Risk" and Increase "Accountability and Quality"
- ☑ Operating Effectively in The Entertainment Company's Multi-Vendor Environment
- ☑ Working Together - Collaborative / Consultative / Innovative

Our Operating Model

We are proposing enhancements to our existing solution; however, our "One Team" operating model remains unchanged. The Consultant Company compliance professionals will continue working as an extension of the Entertainment Company Compliance team. The Entertainment Company Strategist will set the direction and manage the overall program while the Consultant Company compliance professionals focus on efficient, effective program execution, with metrics-driven transparency.

Team Structure and Staffing

Key enhancements have been made to our team structure and staffing approach. We have matured from our original structure, a team of full-time dedicated resources, to a hybrid structure with a combination of full-time dedicated program leads and "pools" of leveraged compliance professionals.

Several points of consideration were explored in developing this more robust and flexible staffing structure.

- Alignment with our existing engagement governance structure and global Governance, Risk and Compliance (GRC) functions
- Staffing levels based on our understanding of The Entertainment Company's program scope and schedules
- TheShore ratios to provide the requisite skills, proximity to business, and support coverage
- Extended coverage across time zones
- Flexibility to meet peak periods of activity

In addition to the leveraged GRC Leaders and four dedicated Primary Leads, our fixed monthly pricing includes 3.0 FTE's (full-time equivalents) of leveraged compliance professionals from our offshore pool. This combination of Primary Leads and leveraged resources maintains the current staffing levels The Consultant Company provides today.

The proposed hybrid structure with a combination of full-time primary leads and "pools" of leveraged compliance professionals will provide:

- Flexibility to engage additional resources during peak periods of activity
- Team depth and resilience to support: coverage, people training/development, leaves of absence, and attrition
- Extended offshore support hours when needed until 4 PM Eastern
- Building on a Strong Foundation

The Entertainment Company Strategist and the Consultant Company team of CISA professionals have successfully managed and matured execution in each of the programs over the last 20 months. With this strong working foundation in place, we would like to expand and deepen our cybersecurity and compliance discussions.

Each the Consultant Company team member maintains a mindset of continuous improvement and bringing forward ideas for process innovation. For example, our log monitoring team is actively working with application specialists on opportunities to automate portions of the manual activities. We will incorporate innovations and improvements within our status reporting and raise these opportunities in our joint discussions. We will also engage our larger team of The Consultant Company Group experts at no additional cost to The Entertainment Company, for example:

- Aaron Fort, North America Data Privacy Officer, sharing insights on the EU General Data Protection Regulation (GDPR) and hosting a discussion session with The Entertainment Company Security and Compliance specialists.
- Puneet Paremel, North America Assurance Audit Leader, working with our engagement team to assess practices and provide recommendations for improvement.
- Anne Hathaway, Global Security Operations Center Lead, presenting how our Log Monitoring service is only a small portion of our Managed Security Operation Center (SOC).

Why the Consultant Company?

Our team strongly desires to continue on the compliance journey *as The Entertainment Company's trusted partner.* We believe that The Consultant Company is the right choice.

Partnership – The Consultant Company is proud to have built a strong history of collaboration with the Entertainment Company Company since 1999 and with the Entertainment Company Compliance team since 2014.

Flexibility – The Consultant Company is ready and able to expand to meet The Entertainment Company's compliance needs. Whether expansion means meeting a period of peak demand within an existing compliance program or meeting the requirements of new regulations or new geographies, we are ready to deliver.

Continuity – The Consultant Company has 20 months of The Entertainment Company Compliance program experience. The Entertainment Company and The Consultant Company have worked as One Team to set the wheels in motion.

Cost Saving – The Consultant Company brings a mix of onshore and offshore certified compliance professionals to the team. Our expanding investment in cybersecurity and compliance professionals within our TheShore centers is a strategic direction for The Consultant Company.

The Consultant Company is committed to providing The Entertainment Company with the right balance of best talent from the right locations and working collaboratively as "One Team" to create and deliver optimal Compliance and Remediation Services.

Milestone Date Proposal

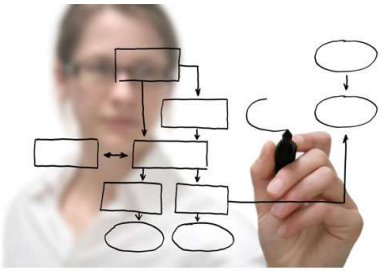
During our initial transition prior to the take-on of Compliance Services, we jointly achieved many milestones. Given our status as incumbent, we are currently executing Compliance and Remediation activities in each of the program areas. Given this, our teams will not be required to perform additional Transition related activities.

Our deliverables for these Compliance and Remediation activities are detailed below.

The Consultant Company will continue to deliver daily/weekly/monthly status reports that support the work effort expended to complete the Milestones within your current Compliance Program.

Work Breakdown Structure and Responsibilities

PCI Program Execution



A. Update PCI handbooks and distribute to application teams

B. Gather and QA assessment documents

C. Support fieldwork

D. Coordinate PCI penetration testing
   1) Conduct kickoff
   2) Gather information from application teams
   3) Schedule penetration testing
   4) Track approvals
   5) Upload testing details
   6) Coordinate credentialed penetration testing
   7) Review findings
   8) Communicate status

XOX Program Execution

A. Prepare and submit interim testing XOX work papers
   1) Update XOX narratives
   2) Conduct internal walkthroughs
   3) Determine populations and select samples as per the sampling guidelines
   4) Evaluate the chosen samples against the attributes as outlined in the XOX template
   5) Collect evidence for each of the attribute and embed sufficient documentation within work paper in order to justify the testing of the attributes.
   6) Submit work paper in Archer for Strategist's review
   7) Address any return comments, as necessary. The testing is complete once the work paper is approved.

B. Prepare and submit update (or remediation) testing XOX work papers
   1) Determine populations and select samples as per the sampling guidelines

2) Evaluate the chosen samples against the attributes as outlined in the XOX template
3) Collect evidence for each of the attribute and embed sufficient documentation within work paper in order to justify the testing of the attributes.
4) Submit work paper in Archer for Strategist's review
5) Address any return comments, as necessary. The testing is complete once the work paper is approved.

C. Monitor and review XOX artifacts

Privacy Program Execution

A. Identify Privacy in-scope applications and servers

B. Identifying any issues with the in-scope servers and following up with application team to get those corrected

QUID Program Execution

A. Pre-validate Access Central server list to confirm that all in-scope servers are included in the server list baseline file.

B. Extract the user list.

C. Collect all manual data required for the review.

D. Validating the reviewer assignments in Access Central. It includes the manual re-assignment of servers to respective reviewers.

E. Support application teams review.

F. Perform QA review of QUID evidence and approve them in Archer.

Log Monitoring Program Execution

A. Perform application log auditing, log analysis and anomaly detection for applications on boarded through CLS, Splunk or done manually

B. Perform database log auditing, log analysis and anomaly detection for associated databases in Oracle, Imperva and Informix

C. Perform daily follow up on fixing of the anomalies

D. Monitor mailbox

E. Prepare weekly reports and share with client and stakeholders

F. Hold weekly update call with client and stakeholders.

G. Prepare monthly report and share with stakeholders.

H. Perform quarterly base lining activity for all applications and databases

I. Onboard new application or database logs as added to scope

J. Perform base lining for new on boarded applications or databases

K. Perform off boarding of applications or databases as removed from scope

Expectations of The Entertainment Company Team Members

The Entertainment Company has designated a Project Manager to whom all The Consultant Company communications will be addressed with respect to the services and who has authority to act for The Entertainment Company in all aspects of the Compliance Services. Responsibilities of the Entertainment Company Project Manager include resolving issues, escalating them within the organization, and assisting in the issuance of project scope and project timelines and work plans.

Project Deliverables

Stream	Related Activities and Deliverables
Project Governance Monthly Status	Resource management - Forming the project team throughout the course of the project depending on constraints and needs. This is achieved by selecting, acquiring, training, coaching, motivating, reviewing and releasing project team members. Client Relationship Management - Establishing and maintaining the relationship with the client. It also consists of understanding, formalizing and monitoring client requirements. Communication Management - Establishing and achieving communication on project-related information. Issue Management - Preparing for, identifying and capturing project related issues, launching the relevant actions to resolve them, and tracking and monitoring the issues.
PCI Compliance and Penetration Testing	Update the PCI Handbook for quality / completeness and distribute to application teams. Create PCI tasks for in-scope applications and create and assign questionnaires and tasks to application and IT security compliance teams. Without this, the application teams would not be able to post evidence to assess. Simultaneously a CiRT Task is created by the Archer team with compliance team guidance. After artifacts have been submitted by application teams, our team performs a review/assessment of the quality of the evidence/documents. Responses given by application teams should equal the spirit and context of requirements. Seek clarification and additional supporting evidence. Coordinate with application teams for closure in a timely manner. If an artifact is returned by assessors, we coordinate with application teams to gather additional information/evidence requested by assessors. Work closely with application teams as they may need assistance to understand the requirement. Lead application holds walkthroughs by planning and scheduling meetings with all stake holders and collect information during observation meetings to submit to Strategists / assessors. It is important to follow-up with stake holders to expedite the submission of artifacts. Report on progress made by our team on assigned tasks. Bring up challenges or hindrances proactively in daily calls so these can be addressed or escalated by the Strategists. For Penetration Testing, conduct a kick off call with the application teams on the activity. Send out the Information Gathering Forms (IGF) to application teams requesting the server/ IP addresses and application details for in scope testing. Schedule the Penetration Tests based on the test window provided by the application teams. Open change tickets in Service Now and track the approvals to closure once test is complete. Coordinate with the Penetration testers by updating the SharePoint calendar and uploading finalized IGFs to SharePoint with the test window and test details. Coordinate Penetration tester's access requests to perform credentialed application testing. Schedule findings meetings with application teams, remediation team and penetration testers. Distribute reports to the application team and coordinate with the remediation team. Post reports to Archer tasks with PCI Penetration testing artifacts. Update the penetration test tracking sheet and send completion status to Strategists.
XOX	Prepare and submit Interim testing XOX work papers.

<table>
<tr><th>Stream</th><th>Related Activities and Deliverables</th></tr>
<tr><td></td><td>During the course of testing, the population for the entire control is determined. From the population, samples are selected as per the sampling guideline. The chosen samples are evaluated against the attributes as outlined in the XOX template.

For each of the attributes, evidence is collected and embedded in the work paper. Sufficient documentation is added to the work paper in order to justify the testing of the attributes.

Once the testing is complete, the work paper has to be submitted in Archer and has to be reviewed by the Entertainment Company Strategist.

If a work paper is returned respond to the return comments. This may require coordination with the application team to address the returns.

The testing is complete once the work paper is approved.

Update testing XOX work papers are prepared and submitted in Archer following a similar process as above during the latter part of the Fiscal year.

Apart from preparing XOX work papers, also monitor the timely submission of XOX artifacts in Archer by application teams and review artifacts after submitted. Coordinate with teams if issues are found prior to approving the artifacts in Archer.</td></tr>
<tr><td>Privacy</td><td>Identify the Privacy in-scope servers by checking all of the in-scope applications within Service Now. Identify issues with the in-scope servers and follow up with the application teams to make corrections.

The in-scope servers are validated using the Server Information card tool which looks for various updates like AV status, HIDS status, Tripwire status, and Qualys status. Coordinate with the application team for issues found during the validation and drive to closure. This activity is currently performed twice a year.</td></tr>
<tr><td>QUID</td><td>Pre-validate the access central server list before extracting the user list to confirm that all in-scope servers are included in the server list baseline file.

Post-validate the access central server list after extracting the user list to confirm that data for all in-scope servers is available in the tool. If not, follow-up with the access central team to receive it.

Collect all manual data required for the review by raising ServiceNow requests to respective teams (or) contacting them through email. This includes:
Approved user list
User list of iMOD servers
AS400 Server
All in-scope Database instances (SQL, Oracle, Informix).
Validate the assignment of reviews in access central. This includes the manual reassignment of servers to respective reviewers.

Address queries, if any, from application teams to pave the way for them to complete the review.

Perform QA review of QUID evidence submitted by application teams and approve them in Archer. This includes follow-up with applications teams for additional evidence as needed.</td></tr>
<tr><td>Log Monitoring</td><td>Perform application log auditing, log analysis and anomaly detection for the below applications.<table><tr><th>Application Name</th><th>No. of Applications</th></tr><tr><td>CLS</td><td>34</td></tr><tr><td>Splunk</td><td>8</td></tr><tr><td>Manual</td><td>2</td></tr></table>Perform database log auditing, log analysis and anomaly detection for below databases.<table><tr><th>Database Name</th><th>No. of Databases</th></tr><tr><td>Oracle</td><td>5</td></tr><tr><td>Imperva</td><td>16</td></tr><tr><td>Informix</td><td>1</td></tr></table></td></tr>
</table>

Project Organization

Key enhancements have been made to our team structure and staffing approach. We have matured from our original structure, a team of full-time dedicated resources, to a hybrid structure with a combination of full-time dedicated primary leads and "pools" of leveraged compliance professionals.

Developing this more robust and flexible staffing structure many options for improvement were considered.

- Alignment with our existing engagement governance structure and global Governance, Risk and Compliance (GRC) functions
- Staffing levels based on our understanding of The Entertainment Company's program scope and schedules
- The Shore ratios to provide the requisite skills, proximity to business, and support coverage
- Extended coverage across time zones.
- Flexibility to meet peak periods of activity

The proposed hybrid structure with a combination of full-time primary leads and "pools" of leveraged compliance professionals will provide:

- Flexibility to engage additional resources during peak periods of activity
- Team depth and resilience to support coverage, people training/development, leaves of absence, and attrition
- Extended offshore support hours when needed until 4 PM eastern

In addition to the leveraged GRC Leaders and four dedicated Primary Leads, our fixed monthly pricing includes 3.0 FTE's (full-time equivalents) of leveraged compliance professionals from our offshore pool. This combination of Primary Leads and leveraged resources maintains the current staffing levels The Consultant Company provides today.

Team CV's (removed for company privacy)

Respondent Requirements

Respondent assumes The Entertainment Company will continue to retain these services

- Governance
- Strategy and Program Management
- Management Escalations
- Tool Admin / Configuration
- Projects

Respondent's solution is based upon the following requirements

- Use of The Entertainment Company PCs and / or build of Compliance Virtual Desktops for offshore resources
- The Entertainment Company email to be used by The Consultant Company team
- The Consultant Company offshore Compliance resources may be located in facility work area without the need for isolated /segmented office areas and security cameras
- Log monitoring resources staffed from within The Consultant Company Security Operations Center (not CISA)

- The Entertainment Company will assist The Consultant Company to obtain consent where The Entertainment Company signature is required

Pricing Response

The Consultant Company's enhanced solution provides approximately 10% additional cost savings to The Entertainment Company over the next three years. We anticipate the realization of further efficiencies as we continue to mature and innovate. Please see attachment: The Consultant Company - Compliance RFP Pricing – XXXXXXX.

Sample Agreement Response

The Consultant Company proposes the use of our existing Master IT Outsourcing Services Agreement.