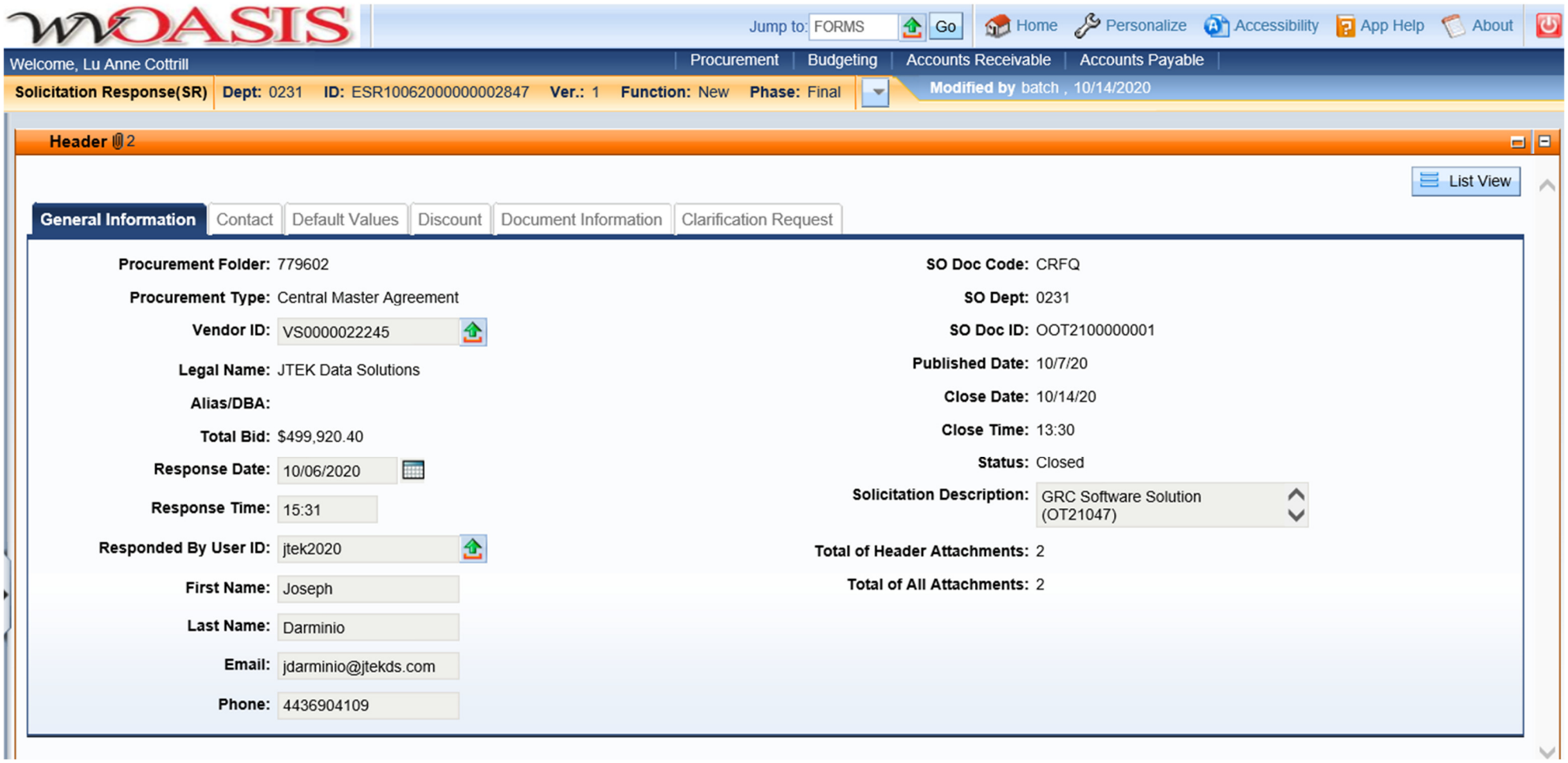
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.


wvOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Lu Anne Cottrill
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0231 ID: ESR10062000000002847 Ver.: 1 Function: New Phase: Final
Modified by batch , 10/14/2020
Header 2
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 779602
Procurement Type: Central Master Agreement
Vendor ID: VS0000022245
Legal Name: JTEK Data Solutions
Alias/DBA:
Total Bid: $499,920.40
Response Date: 10/06/2020
Response Time: 15:31
Responded By User ID: jtek2020
First Name: Joseph
Last Name: Darminio
Email: jdarminio@jtekds.com
Phone: 4436904109
SO Doc Code: CRFQ
SO Dept: 0231
SO Doc ID: OOT2100000001
Published Date: 10/7/20
Close Date: 10/14/20
Close Time: 13:30
Status: Closed
Solicitation Description: GRC Software Solution (OT21047)
Total of Header Attachments: 2
Total of All Attachments: 2

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder:	779602
Solicitation Description:	GRC Software Solution (OT21047)
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2020-10-14 13:30	SR 0231 ESR10062000000002847	1

VENDOR

VS0000022245
JTEK Data Solutions

Solicitation Number: CRFQ 0231 OOT2100000001

Total Bid: 499920.4000000000232830643653 **Response Date:** 2020-10-06 **Response Time:** 15:31:36

Comments:

FOR INFORMATION CONTACT THE BUYER
Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Vendor
Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	GRC Software Solution				499920.40

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

See attached Pricing Page

JTek

JTEK'S RESPONSE TO THE

State of West Virginia

Request for Quote

GRC Software Solution

SOLICITATION NO. CRFQ OOT2100000001

Wednesday,
Oct 7, 2020

SOLUTION PROVIDED BY

RSA

JTek Data Solutions
10411 Motor City Drive
Bethesda, MD 20817

301.469.1900 | WWW.JTEKDS.COM

Oct 7, 2020

Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

*Re: Carahsoft's Response to the State of West Virginia's Request for Quote for GRC Software Solution, Solicitation # CRFQ OOT2***100000001**

Dear Jessica Chambers,

JTEK Data Solutions is pleased to offer RSA to State of West Virginia as a solution to the Request for Quote for a GRC Software Solution. RSA is a pioneer in cybersecurity, and coupled with JTEK's experience as an industry leading government contractor, we believe we have assembled the best solution to fulfill the State of West Virginia's needs.

JTEK is a Certified Small Business located in Bethesda, Maryland. We have been delivering IT solutions and services to government entities since 2012 and hold various government purchasing contracts, including GSA IT Schedule 70, DHS CDM, ITES-3S, SMARTbuy, DoD ESI, and SEWP V. JTEK is supported by our government distributor, Carahsoft Technology Corporation located in Reston, Virginia, enabling our ability to provide state and federal government agency industry best pricing on a wide selection of IT solutions. Our CAGE Code is 6PXL8; our DUNS Number is 78386767.

For any questions or clarifications regarding the contents of our proposal, please contact me directly at 443.690.4109/jdarminio@jtekds.com. This proposal is valid for 90 days from the closing date.

Thank you for your time and consideration.

Sincerely,

Joseph Darminio

Joseph Darminio
Account Manager, JTEK Data Solutions

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Solution Overview

JTek understands that the State of West Virginia is seeking an IT Security Professional Services. As the Prime Contractor, JTek has assembled a team for the initiative that includes our Solution Provider, RSA as the best solution to meet WV's requirements.

Prime Contractor: JTek Data Solutions

JTEK Data Solutions: HubZone, 8a Small business, VAR, focused on Federal IT Transformation

JTEK provides world-class technology solutions that allow organizations to maximize agility, efficiency, efficacy, and scalability. By using our proven expertise in modern infrastructure and digital transformation, we are able to build a secure foundation, break down the walls between your IT departments, and posture your organization for a cloud-native future.

Data Center Virtualization
Imagine the cost savings associated with a dramatically reduced datacenter footprint. Whether it's server, desktop, network or storage virtualization, JTEK's designed solutions will reduce capital expenses while improving flexibility, security and scalability.

Converged Infrastructure
Reduce Cost and Improve flexibility. JTEK's CI systems enable significant O&M cost reduction by integrating the compute, network and storage. Converged Infrastructure is designed for maximum elasticity – in terms of performance and scalability - for internal growth or into the Cloud.

Private and Hybrid Cloud Design
Designed for flexibility, private and hybrid clouds give you the power to choose the technology in your solution stack while removing the complexity and risk that typically comes with designing, integrating, and deploying best-of-breed solutions.

Security
Manage risk and threats throughout the enterprise. Secure access for increased mobility and collaboration. Secure virtualization and cloud computing workloads. Detect anomalies by comparing users' activities against their known, "good" behavior as well as the behavior of their peers. JTEK can analyze, assess, and develop a threat and incident management strategy.

Hadoop/Big Data Analytics Design
JTEK makes Hadoop easy to use, cost-effective and with a short time to production. JTEK helps customers bridge the gap from a current EDW into a Hadoop or MPP solution without an overhaul of current staff technical capabilities, while reducing TCO and improving performance dramatically.

Data Protection
Protect your most critical asset - data – whether it's virtualized or still in a Mainframe, and accelerate transformation with JTEK's industry-leading solutions. Integration with VMware, Oracle, and other Tier 1 applications, as well as the existing infrastructure, is unparalleled.

Solution Provider: RSA

RSA is part of a broader security transformation strategy as one of Dell Technologies' strategically aligned businesses.

Dell Technologies provides essential infrastructure for digital business and IT transformation through our family of strategically aligned businesses that see the world the same way – yet offer customers choice. Built on the combined capabilities of Dell, Dell EMC, VMware, Pivotal, SecureWorks, RSA and VirtuStream in one company, Dell Technologies is best positioned to address our customers' critical IT needs and RSA plays a leading role in developing and supporting Dell's security transformation solutions in each of these critical functions:

- Unified Business Risk Management: RSA Archer Suite
- Adaptable Advanced Security Operations: RSA NetWitness Suite & RSA Archer Suite
- Resilient Secure Modern Infrastructure: RSA SecurID Suite
- Trusted Expert Advisory Services: RSA Risk & Cyber Security Practice

Together with our strategically aligned business partners in Dell Technologies, we offer unmatched solutions to enable security transformation from the endpoint to the boardroom.

Quarterly financial reports for Dell Technologies can be retrieved in the following link: http://investors.delltechnologies.com/.

QUALIFICATIONS

Vendor, or Vendor's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

Vendor must have implemented a GRC software solution with a Federal or State, or Local Government entity.

JTEK Data Solutions has worked with numerous customers within the Federal, State and Local Government entities. References can be included upon final request.

RSA has implemented these. RSA Archer has provided similar solutions for other State Governments. We would be pleased to provide more information on specific customer at the appropriate time.

Vendor must hold current certifications and assentation; SOC 2 Type 2 and ISO 27001. It is preferred to be provided with vendors bid, however, it may be requested prior to award.

The RSA Archer SaaS offering is a new (as of November, 2019) offering. As a result, there is not yet a RSA-specific SOC2, Type II audit report for the RSA Archer SaaS offering, as there is not yet a sufficient lookback period for an auditor to audit. RSA plans to include the RSA Archer SaaS offering in its next SOC2, Type II audit after a sufficient amount of time has passed to allow for a proper lookback by auditors.

The Vendor must be compliant with Internal Revenue Service (IRS) 1075, Section 9.3.1.12 – Remote Access requirements.

- IRS 1075, Section 9.3.1.12 states that "*FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore -outside of the United States territories, embassies, or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore.*"

Geo-specific IP blocking is not possible with the current shared, multi-tenant, community cloud offering. However, customers can use IP whitelisting/blacklisting on a per-instance basis to control the IPs from which users can access the instance. With RSA Archer SaaS US, RSA does not transfer Scoped Data across US borders.

MANDATORY REQUIREMENTS

Contract Items and Mandatory Requirements: Vendor shall provide Agency with the Contract Items listed below on an open-end and continuing basis. Contract Items must meet or exceed the mandatory requirements as shown below.

Contract Item #1 Governance, Risk, and Compliance (GRC) Software Solution Mandatory Requirements:

Vendors GRC solution must provide a cost-effective cloud-based Software-as-a-Service (SaaS) risk management solution for the State Cybersecurity Framework. (Including future scalability when new agencies are on-boarded)

With RSA Archer SaaS, customers can stay focused on their business processes, and we will handle the hardware, maintenance and upgrades. RSA Archer SaaS provides performance and scalability in a flexible manner with our “scale up and scale out” infrastructure to support growing Integrated Risk Management needs.

Vendors GRC solution must implement NIST Cybersecurity Framework (NIST CSF), NIST 800-53 control set, and align to PCI DSS, HIPAA, FERPA, CJIS, and other compliance programs. Vendors GRC solution must automatically implement changes or updates in laws or compliance programs and alert users to relevant updates.

RSA Archer features one of the most extensive policy and control libraries in the IRM industry, including a proprietary set of 1,200+ guiding standards organized through a unique custom IRM taxonomy that is aligned with several prevailing best practice frameworks like COBIT, HIPAA, PCI, and NIST 800-53. Together with its companion repositories of external authoritative source requirements, supporting policies, technical control procedures and baseline configuration benchmarks, and assessment questions, RSA Archer's embedded IRM content libraries comprise hundreds of thousands of discreet mapping connections enabling customers to drive a comprehensive IRM program out of the box. Integrations with external content resources like the Unified Compliance Framework have also been established to further extend the breadth and depth of content coverage. An updated listing of available content resources can be found in the RSA Archer content catalog; updates are made to the content on a quarterly basis as new regulations are introduced or existing ones updated.

Vendors GRC solution must maintain the Security Requirements Traceability Matrix (including objectives, risks, controls, ranks, rates, etc.), and allow periodic updates to be made.

RSA Archer IT Controls Assurance provides the ability to assess and report on the performance of controls across all IT assets and automate control assessment and monitoring. You can implement a centralized system to catalog IT assets for compliance reporting and establish a system of record for documenting IT controls. Streamlined processes and workflow for testing of IT controls allow you to deploy standardized assessment processes for manual controls and integrate testing results from automated systems. Issues identified during compliance assessments are centralized, enabling you to track and report on compliance gaps. Remediation efforts for gaps can be documented and monitored to ensure compliance variances are addressed in a timely manner.

For tracking applications through the SDLC, RSA Archer's Risk Project application provides a repository for all risk-related projects. Project records follow a comprehensive, start-to-finish approach and include sections for project staffing and scoping, risk identification, risk analysis and risk treatment. The stages of the Risk Project are based on internationally recognized Risk Management methodologies, including COSO ERM, ISO: 31000, NIST800-30 and others.

Through the Risk Project application, you can:

- Define the scope of the project, the type of risk assessment being performed and the affected company assets.
- Perform risk assessments to identify potential risk areas.
- Analyze findings from risk assessments, documenting threats, vulnerabilities, risk analysis discussions, and overall likelihood and impact.
- Document a risk treatment plan by defining remediation plans or exception requests based on the findings.

Vendors GRC solution must identify and assess strategic risks, opportunities, and mitigating controls.

The Risk Register as a part of the RSA Archer Operational Risk Management solution serves as the corporate controlled library of risks used by the entire organization. It allows you to capture the base data for a given risk statement and link risks to processes, objectives, key risk indicators, financial losses and mitigating control procedures as well as see inherent and residual risk scores.

Vendors GRC solution must monitor and manage strategic risks and opportunities.

Key risk and control indicators can be established and associated with risk and control registers, respectively, and monitored to provide early warning of changes in the organization's risk profile.

Vendors GRC solution must report strategic risks and opportunities.

The RSA Archer Operational Risk Management solution includes dozens of dashboards and reports out of the box to report strategic risk information at both an analyst and executive level.

Vendors GRC solution must include a workflow management component that allows for work to be created and shared (internally or externally), including the ability to record user comments.

The RSA Archer Advanced Workflow engine enables application authors to visually describe business processes as a flowchart. For example, an advanced workflow can: update values in a record, send a notification, display different layouts to users depending on the stage of the workflow, and prompt users to take action or make a decision. Comments can be recorded at any stage of the workflow along with date and timestamps.

Vendors GRC solution must automatically push out control assessments to control owners annually.

RSA Archer's Compliance Engagement application enables the Compliance Team to initiate and manage the life cycle of testing, report the results of testing to executive management, and create engagements that target certain compliance scopes, control sets, or control instances. This functionality includes the automatic creation and assignment of Control Self Assessments, Design Tests, and Operating Tests for each control procedure that has been brought into the scope of the specific Compliance Engagement record from the centralized Control Procedures application.

Vendors GRC solution must send reminders/receive feedback on due tasks and dates to all relevant resources and other stakeholders.

RSA Archer's notification capability allows you to create the necessary notifications and to be sent out based on set criteria. Email notifications can be automatically sent to predefined users/user groups once data conditions are met, such as a change to a data asset occurs or a due date approaches. All notification content is completely configurable by administrators leveraging the Platform Application Builder's code-free interface. Notifications can contain a deep link into the specific task or activity requiring the user's attention. Also, if the responsible user hasn't completed the assignment before the due date, notifications can be configured as reminders to users as well as sending escalation emails to managers, executives, etc.

In addition to email notifications, RSA Archer's Task Management functionality enables the creation and assignment of tasks either manually or via automated processes. You can view detailed status reports of open tasks and a history of completed tasks. The Task Management application is accessible from any application with task management enabled.

When an application includes task management, tasks related to records in that application are tracked and logged in a related records field called Open Tasks/Activities. In addition to viewing tasks in a record, users can use the Task-Driven Landing page to see their assigned tasks. Reports can also be placed on dashboards detailing tasks that have been assigned to them.

Vendors GRC solution must deliver automated escalations if deadline is approaching.

RSA Archer's notification capability can be configured to automatically send notifications, reminders and escalations to stakeholders and managers based on virtually any condition such as workflow progress, due date, escalated priority, etc. The recipients of these notifications can be configured to automatically target managers of individuals or static groups for escalation purposes.

Vendors GRC solution must provide standardized templates for different functions/areas, including reporting templates and a testing result reporting template linked to every control.

All RSA Archer applications and questionnaires come with existing data entry forms which break out fields/questions into columns, sections, and tab set for efficient data capture. Fields can be of multiple types (e.g. Text, Numeric, Values List, Date, Attachment, External Links, Image, IP Address, User/Groups List/Record Permissions, Voting, Sub-form, and Cross-Reference) will be placed on the layout; field and layouts can be configured using a code-free point-and-click, drag-and-drop interface.

RSA Archer serves as the central repository for all your reporting requirements. The RSA Archer Platform includes a built-in reporting engine that is native to the system. In addition to RSA Archer's extensive list of over 1000 canned reports, the RSA Archer Platform provides a user-friendly interface for performing simple keyword searches or complex, multi-application searches.

For more complex templates, RSA Archer has built in Mail Merge template export functionality. Mail Merge templates define how record data is inserted from RSA Archer into a Microsoft Word document or PDF file using the Mail Merge functionality. This functionality is particularly useful for conducting iterative vendor assessments, compliance reviews, and capturing information at a specific point in time. Templates are authored in Microsoft Word and include field codes corresponding to fields to be exported out of an RSA Archer record.

Vendors GRC solution must allow for documentation of risk/control issues/findings/remediation plans.

With RSA Archer Issues Management, business users can create a coordinated and consolidated view into known issues, gaps, and deficiencies. The solution offers an organized, managed process to escalate issues in order to provide visibility into ownership through the established chains of command. Workflow, reporting and email notifications are included for proper sign-off and approval of issues, remediation plans, and exception requests in order to ensure the findings are thoroughly managed.

Vendors GRC solution must track remediation deadlines/timelines. Vendors GRC solution must provide a dashboard to show, at a minimum, which updates are outstanding, the last Security Requirements Traceability Matrix review dates, and when testing is overdue.

The RSA Archer Issues Management solution as described in the requirement above tracks all remediation activities including timelines and notifications. There are dozens of dashboards included out of the box with RSA Archer that display tracking metrics. Any report that is not available out of the box can easily be created and added to a dashboard to show exactly what you need, when you need it.

Vendors GRC solution must provide data visualization tools or allow export of data to other tools such as Microsoft Office

The RSA Archer built-in reporting engine supports statistical reporting that allows the user to grasp the full scope of the data without paging through hundreds or thousands of records through a visual representation. In addition to tabular reporting which can be flat or hierarchical, the following chart types are available:
Vertical Bar
Horizontal Bar
Pie
Donut
Gauge
Funnel
Line
Radar
Bubble
Heat Map
Scatter
Tree Map
Sunburst

Reports within RSA Archer can be exported into Microsoft Word, PDF, Excel, HTML, XML, and CSV formats. RSA Archer Dashboards can be exported into Word, PDF, and PowerPoint formats as well.

Vendor must provide a means to summarize and track data in the system.

Any field within the schema of an RSA Archer application (content repository) or questionnaire can be brought into searches and reports for tracking and summarization. (See the response above regarding reporting.) Additional calculated fields can be configured solely for reporting purposes that can reside off layout and calculated fields can be created utilizing a function library that mirrors that functions present in applications such as Microsoft Excel and Access.

Vendor must provide a means to summarize performance metrics.

RSA Archer Key Indicator Management provides a means for organizations to establish and monitor metrics related to each business unit within the organization. Metrics can be tracked as part of key risk indicators (KRIs), key control indicators (KCIs), key quality indicator (KQI), or key performance indicators (KPIs). Depending on your overall implementation, metrics could also be associated with other elements of your IRM program, including strategies and objectives, products and services, and business processes to monitor quality assurance and performance. The Metrics component allows Risk Managers to establish thresholds, bands, or trends, and manage the regular tracking of values to indicate a pass/fail status for the indicator.

Vendors GRC solution must have user/access management tools to allow for creation/management of user accounts (Active Directory integrated preferred for future use; role-based access required)

The SSO implementation with RSA Archer SaaS allows clients to be signed into Archer using the same credentials as their network. RSA Archer offers both direct SAML 2.0 integration and FIM integration capabilities. FIM solutions that use either SAML v1 or v2 are supported. This includes Microsoft ADFS. No password information is transmitted across the network to the SaaS cloud. Only the authentication information from the client is transmitted, this information is digitally signed and encrypted using standard digital certificate technologies. Direct LDAP synchronization is supported. To enable LDAP sync, customers will simply have to provide a list of outbound whitelist IP addresses to our SaaS operations team. No professional services engagement is required. Groups within AD can be used to map users to appropriate groups within RSA Archer.

Role-based access must be defined at the functional level (i.e. allow user access to data only relevant to their function)

Once a user is authenticated into RSA Archer, the system's Access Control functionality will then determine what data can be accessed and which functions can be performed by the user based on the permissions they are granted by the administrator. In Archer we call these permissions Access Roles. An Access Role is a collection of application-level and page-level rights that can be assigned to any number of users and groups to control their privileges (create, read, update and delete) for individual pages within the system.

Will restrict certain functions to authorized staff only (i.e. certain user group has read-only access, another user group has ability to delete records)

Yes. Please see the response to the requirement above.

Contract Item #1 Governance, Risk, and Compliance (GRC) Vendor Mandatory Requirements:

The vendor must conduct training with a group of power users of the new tool enabling a "train- the- trainer" approach. This training is to be included in the lump sum cost on the Exhibit A Pricing Page Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support.

RSA Archer offers a comprehensive list of training options. An appropriate training curriculum, aimed at long term success of an RSA Archer implementation at Janney will require a detailed discussion between RSA Archer and West Virginia to clearly define priorities and organizational goals. For the purpose of this proposal RSA Archer recommends the following training schedule: Two students should take both the Archer Administration I and Archer Administration II courses.

1. **Staff Training - $10,000**
    1. 2 students trained in Archer Administration I
    2. 2 Student trained in Archer Administration II
2. **Train the Trainer Session - $18,500**
    1. On-site trainer for up to 5 students

The vendor must provide technical support within one (1) business day and make best efforts to resolve problems as quickly as possible.

RSA uses a "follow-the-sun" process to hand off cases among our customer support centers, ensuring that your case is worked on around the clock. Full details of RSA's Support Strategy, case management and escalation procedures are available on RSA Link here: https://community.rsa.com/docs/DOC-40389

The vendor must guarantee application has 99.9% uptime.

The RSA Archer SaaS Production SLA is 99.5% uptime.

The vendor must provide frequent progress reports during any outage.

Platform administrators are notified at least five business days in advance of scheduled maintenance and no less than 24 hours before emergency maintenance. The notice indicates the anticipated impact of such maintenance on availability, including duration. If there are any significant issues with an upgrade that could extend the maintenance window, RSA will immediately let customers know the expected impact.

In case of a Force Majeure Event that RSA reasonably believes will impact the Service Offering or its ability to perform its obligations, RSA shall, to the extent possible, promptly notify Customer of such Force Majeure Event. Such notification shall, as soon as such details are known, contain:
i. a description of the Force Majeure Event in question;
ii. the impact the Force Majeure Event is likely to have on the Service Offering and RSA's obligations;
iii. the operating strategy and the timetable for the utilization of the contingency site;
iv. the timeframe in which RSA expects to return to business as usual; and
v. crisis management escalations affecting Customer Content.

RSA Archer Customer Support and/or Customer's RSA account manager shall coordinate with Customer's representative for the purpose of exchanging information and detailed, up-to-date status and on-going actions on and from the occurrence of a disaster. Customer shall make sure that its representative is at all times known to RSA Archer Customer Support.

The vendor must ensure that State of West Virginia data is not co-mingled with other customer's data.

RSA Archer SaaS entails a shared, multi-tenant, community cloud environment. This means hardware infrastructure components, including but not limited to firewalls, load balancers, web servers, database servers and storage equipment are shared by multiple customers. While shared hardware is used, customer data is segmented on a per-instance basis, which is more granular than a per-customer basis, as each customer can have multiple instances (e.g. DEV, UAT, PROD instances) within the offering. Each application instance is logically separated via use of separate directories and databases so that no customer data is comingled.

The vendor must ensure that State of West Virginia data can be exported and returned to the state.

In the event this Service Offering and/or the Agreement is terminated (other than by reason of Customer's breach), and if Customer so requests at the time of termination, RSA will make available to Customer an industry standard file of most recent Customer Content within RSA's possession within thirty (30) days of termination.

The vendor must ensure State of West Virginia data is destroyed at the end of the contract.

Media storage devices used to store customer data are classified by AWS (RSA's IaaS provider) as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned. See https://aws.amazon.com/compliance/data-center/controls/ for details.

Vendor must support data in transit encryption using TLS 1.2 or higher.

RSA Archer SaaS uses TLS 1.2 for encrypting data in transit. All communication with the RSA Archer GRC Platform software takes place over HTTPS.

Vendor must support encryption at rest using AES-256 or higher.

Yes. Scoped data at rest is encrypted using AES-256 (or better) encryption.

Vendor must use two-factor authentication and or network access control limiting access from an exposed IP or subnet preferred.

Two-factor authentication is required for RSA SaaS Operations personnel to access the back-end production environment. Customers wishing to utilize multi-factor authentication can employ single-sign on to leverage their existing strong authentication mechanisms for network access.

Vendor must provide at least fifteen (15) power user licenses and must be included in the lump sum cost on the Exhibit A Pricing Page Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support.

Please see the attached Exhibit A.

Contract Item #2 Professional Services - Post Implementation Customization

The Post Implementation Customization Rate must be a single hourly rate that will be billed for all staff time and is to be used to consult with vendor staff on unforeseen customization issues that may arise after the GRC solution has been successfully implemented. Requests to use the Implementation Consultant Hours must be outlined in a SOW (Statement of Work) and include both the problem and required number of hours to address the problem, and must be executed by an authorized representatives of both Parties.

The professional services effort required to implement the RSA Archer Use Cases outlined in this proposal can vary significantly based on a number of factors. The level of involvement from customers, staff, volume of configurations, and strategic staging efforts may influence total effort estimated in this proposal. Before engaging in an implementation effort, RSA Archer will work closely with West Virginia to develop a detailed

Scope of Work and project plan. This Statement of Work (SOW) will include a detailed breakdown of tasks and an accurate estimate of effort. The effort estimations in this proposal should be considered initial estimates and carry a +/- factor of 25%.

Archer Implementation Services: In response to West Virginia's understood business need, we propose the following Professional Services estimated effort:

RSA Archer Professional Services to implement the following RSA Archer Use Case licenses - 995 hr. @ $250/hr. = $248,750
RSA Archer Issues Management, Controls Assurance, IT Risk Management, Policy Program Management, Top-Down Assessment, and Key Indicator Management.
T&E Expenses - $5,000
(Estimate 2 On-site visits @ $2,500/visit for project completion)

Software as a Service Addendum

Vendor must sign the attached Software as a Service Addendum prior to award.

Please see signed Software as a Service Addendum attached.

CONTRACT MANAGER

During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager:	Joseph Darminio
Telephone Number:	443-690-4109
Fax Number:	
Email Address:	jdarminio@jtekds.com

IN SUMMARY

JTek Data Solutions and RSA appreciate the opportunity to offer this solution for the WV's initiative.

The JTek Team has proposed a superior and cost-effective solution that fully complies with the WV's requirements set forth in Solicitation # CRFQ OOT2000000003. We understand the importance of your project goals, and we are confident you will benefit from this solution and our expertise.

JTek Data Solutions looks forward to the opportunity to speak with you regarding the details of this proposal, as well as the opportunity to work with State of West Virginia on this project.

Secureworks
One Concourse Pkwy, Ste. 500
Atlanta, GA 30328
www.secureworks.com

RSA Security

174 Middlesex Turnpike

Bedford, MA 01730

March 20, 2020

Re: RSA Archer Web Application Security Assessment – Letter of Attestation

To whom it may concern:

In February of 2020, RSA contracted Secureworks to perform a Web Application Security Assessment of the RSA Archer Application. Testing was conducted remotely, targeting the public-facing web application. The objective of this assessment was to identify security risks and suggest mitigation strategies to reduce risk to critical business data.

The engagement began on February 10, 2020 and was completed on February 28, 2020. The testing process began with an information-gathering phase, during which the Secureworks assessment team conducted steps designed to gather all pertinent information surrounding the target environment. Automated and manual testing techniques were used to assess the target areas to gauge the level-of-business risk of any discovered vulnerabilities.

This assessment represents a point-in-time analysis of the target environment and a point-in-time review of the security controls of a particular application or group of application components. There were five major phases conducted within the assessment: discovery, vulnerability analysis, automated testing, manual testing, and reporting. These phases allowed Secureworks consultants to conduct a security examination of the target systems, while gathering the required information to properly rank and prioritize the threats for the client.

The Web Application Security Assessment of RSA's Archer application encompassed all of the systems and applications that were provided as the targets in scope. The assessment was performed by consultants using a methodology based on industry best practices, such as ISO 27002, NIST 800-115, OWASP, and PTES.

General Findings and Opinion: In our opinion, the accompanying discussion fairly presented, in all material respects, the areas evaluated and their corresponding security status. While Secureworks cannot guarantee that a security breach will never occur, it is our overall opinion that RSA has taken the appropriate steps to reduce their enterprise-risk level and mitigate the probability of such an event.

Limitations: These findings are based on the controls that were evaluated as of February of 2020. Because subsequent changes to the customer's network or environment could impact the security posture of RSA, Secureworks disclaims any projections of these findings to future periods.

Use of this Document: This document has been prepared solely for the use of RSA, and its officers, directors, and employees. No other third party shall be entitled to rely upon this document. The provision of this document or information herein to the parties other than RSA shall not entitle such parties to rely on this report or the contents thereof in any manner or for any purpose whatsoever, and Secureworks specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary or punitive) arising from or related to provision of such report or information to such parties.

If you have questions or comments, do not hesitate to contact us.

Sincerely,

Secureworks

Secureworks
One Concourse Pkwy, Ste. 500
Atlanta, GA 30328
www.secureworks.com

Dell RSA Archer (SaaS)

February 7, 2020

Re: External Penetration Test

To whom it may concern:

In October of 2019, Dell RSA Archer (SaaS) contracted Secureworks to perform an External Penetration Test of the Dell RSA Archer (SaaS) Internet-facing systems. Testing was conducted from Secureworks' offices in Atlanta, GA, targeting the external network environment. The objective of this assessment was to identify security risks and suggest mitigation strategies to reduce risk to critical business data.

The engagement began on October 21, 2019 and was completed on October 30, 2019. The testing process began with an information-gathering phase, during which the Secureworks assessment team conducted steps designed to gather all pertinent information surrounding the target environment. Automated and manual testing techniques were used to assess the target areas to gauge the level-of-business risk of any discovered vulnerabilities.

This assessment represents a point-in-time analysis of the target environment and a point-in-time review of the security controls of a particular application or group of application components. There were five major phases conducted within the assessment: discovery, vulnerability analysis, automated testing, manual testing, and reporting. These phases allowed Secureworks consultants to conduct a security examination of the target systems, while gathering the required information to properly rank and prioritize the threats for the client.

The External Penetration Test of Dell RSA Archer (SaaS)'s external network environment encompassed all of the systems and applications that were provided as the targets in scope. The assessment was performed by consultants using a methodology based on industry best practices, such as ISO 27002, NIST 800-115, OWASP, and PTES.

General Findings and Opinion: In our opinion, the accompanying discussion fairly presented, in all material respects, the areas evaluated and their corresponding security status. While Secureworks cannot guarantee that a security breach will never occur, it is our overall opinion that Dell RSA Archer (SaaS) has taken the appropriate steps to reduce their enterprise-risk level and mitigate the probability of such an event.

Limitations: These findings are based on the controls that were evaluated as of October of 2019. Because subsequent changes to the customer's network or environment could impact the security posture of Dell RSA Archer (SaaS), Secureworks disclaims any projections of these findings to future periods.

Use of this Document: This document has been prepared solely for the use of Dell RSA Archer (SaaS) and its officers, directors, and employees. No other third party shall be entitled to rely upon this document. The provision of this document or information herein to the parties other than Dell RSA Archer (SaaS) shall not entitle such parties to rely on this report or the contents thereof in any manner or for any purpose whatsoever, and Secureworks specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary or punitive) arising from or related to provision of such report or information to such parties.

If you have questions or comments, do not hesitate to contact us.

Sincerely,

Secureworks

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 722642

Doc Description: GRC Software Solution (OT20131)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2020-05-12	2020-05-27 13:30:00	CRFQ 0231 OOT2000000003	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

STEK Data Solutions
10411 Motor City Dr #700
Bethesda, MD 20817
443-690-4109

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Signature X [signature] **FEIN #** 90-0772660 **DATE** 5/26/20

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:

The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Office of Technology to establish an open-end contract for a Governance, Risk, and Compliance (GRC) software solution. This software will be a component of the Cyber Risk Program that was procured under CRFP ISC ISC2000000001. The GRC software solution will enhance the ability of the State of West Virginia to maintain compliance with industry regulatory requirements, federal regulatory requirements, applicable laws, and security expectations. The vendor will provide a GRC technology solution that enables the State and its individual agencies to implement an adaptive and effective internal control system for establishing, maintaining, assessing, and reporting effective internal controls per the terms and conditions and specifications as attached.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - NETWORKING SUPERVISOR DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	GRC Software Solution				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description :

See attached Pricing Page

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

RSA ARCHER SAAS

Infrastructure Overview

March 2020

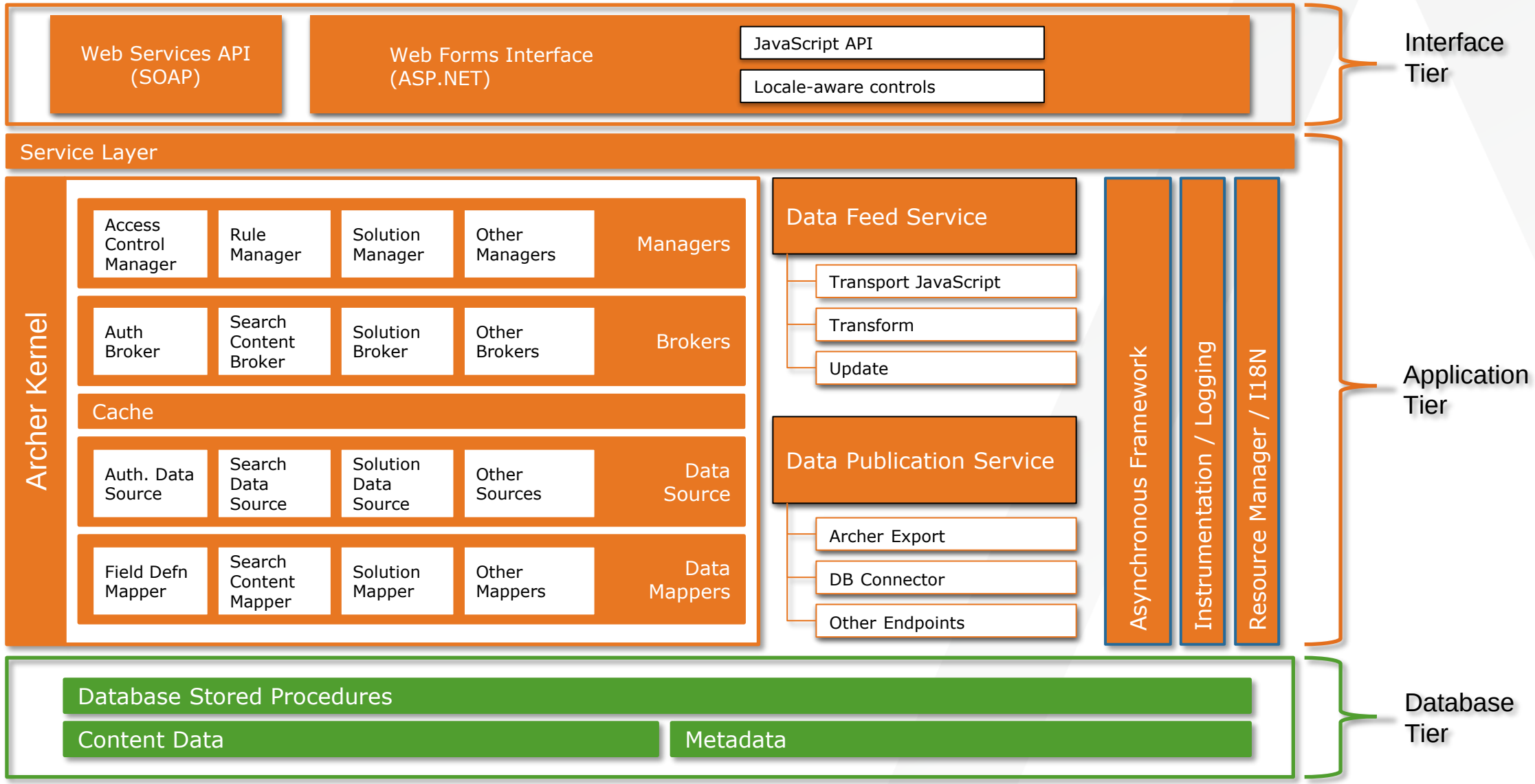
PERSPECTIVES

RSA Archer Platform – Architectural View

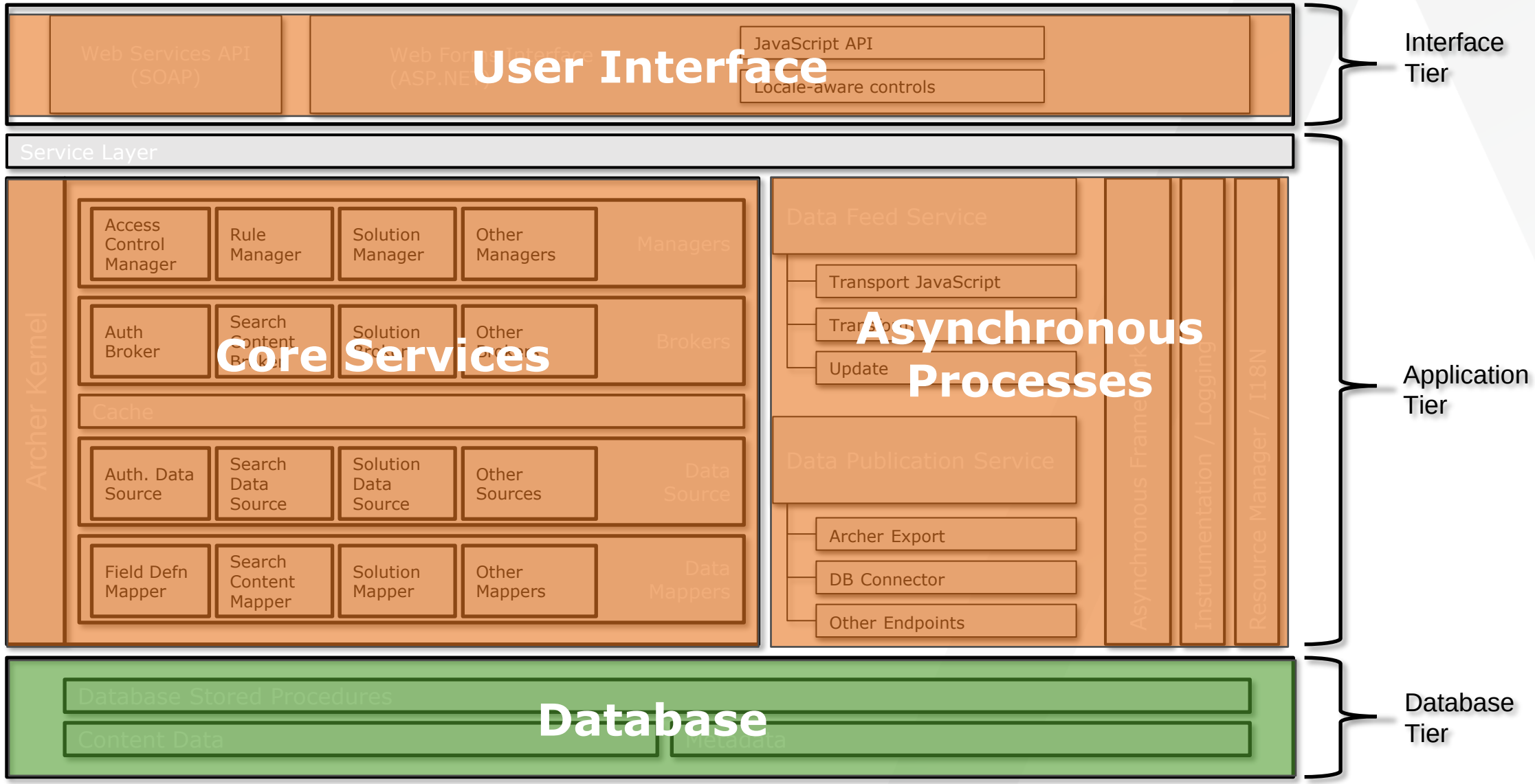
RSA Archer Platform – Operational View

RSA Archer SaaS– Infrastructure View

RSA ARCHER PLATFORM – ARCHITECTURAL VIEW



RSA ARCHER PLATFORM – ARCHITECTURAL VIEW



RSA ARCHER PLATFORM CAPABILITIES

User Interface

- ✓ Web-based architecture
- ✓ Load balanced, horizontally scalable
- ✓ Supports distributed caching

Core Services

- ✓ Archer business logic
- ✓ Load balanced, horizontally scalable
- ✓ Supports distributed caching

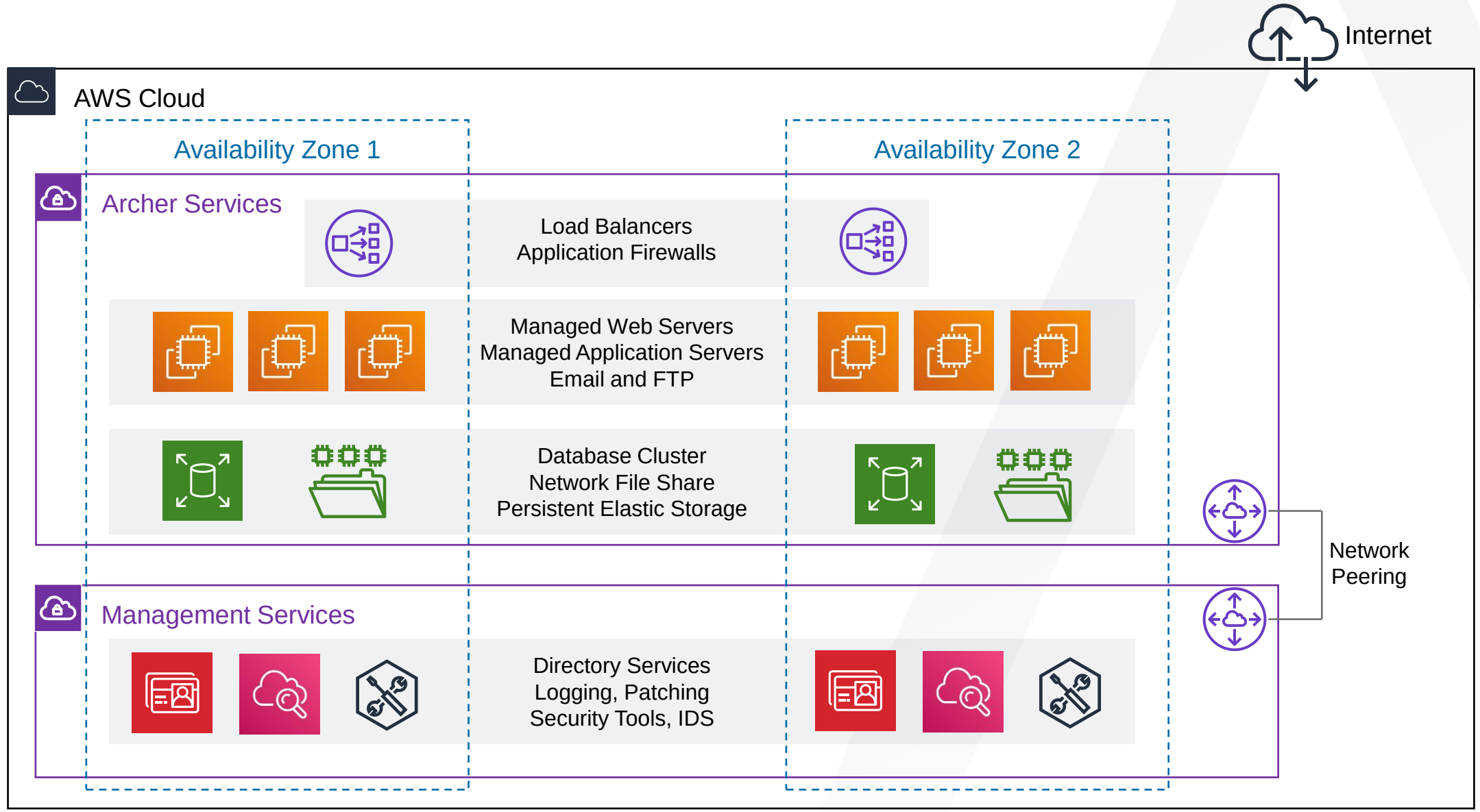
Asynchronous Services

- ✓ Archer Job Engine
- ✓ Workflow Engine
- ✓ Notifications
- ✓ Indexing

Database

- ✓ Clustered Configuration
- ✓ Scalable storage and compute
- ✓ Distributed backups

RSA ARCHER SAAS ENVIRONMENT



RSA ARCHER SAAS ENVIRONMENT

Access Control

- Enterprise grade load balancer
- Least-privileged Security Group model
- Network and application firewall controls
- Public and private subnet isolation
- Identity and access management

Platform Compute

- Service-specific virtual machines
- Scalable compute infrastructure
- Software deployment automation
- Continuous monitoring and logging
- Configuration management controls

Management Services

- User directory and management controls
- Log aggregation
- Security scanning tools
- Intrusion Detection System (IDS)
- Secure server image generation
- Software license reporting

Platform Datastore

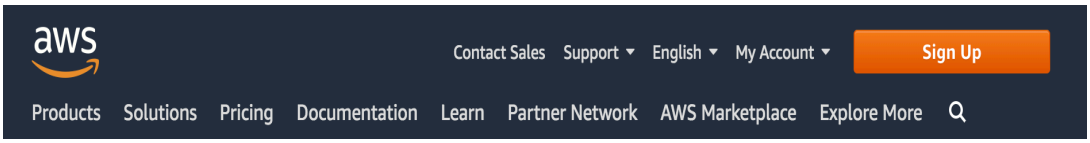
- Highly available database cluster
- Highly available filesystem cluster
- Physically distributed backups
- Scalable compute and storage
- Isolated network subnet
- Continuous monitoring and logging
- Configuration management controls

Download AWS Compliance Reports with AWS Artifact

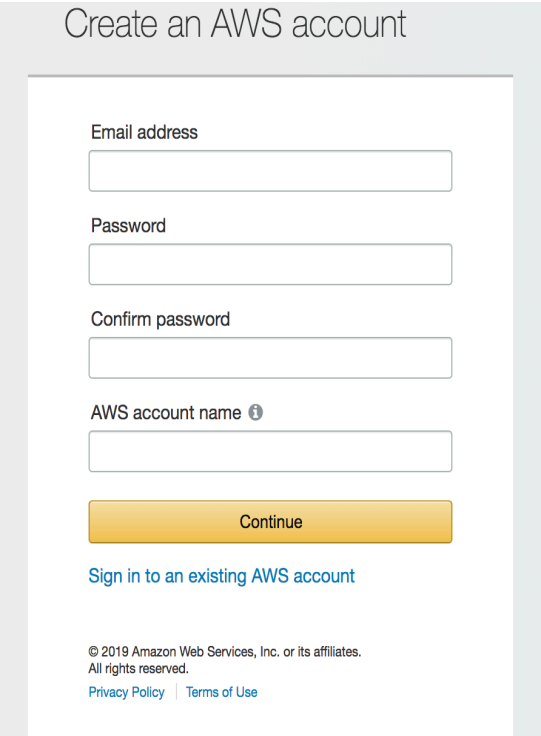
AWS provides self-service access to the latest AWS Compliance Reports directly in the console with AWS Artifact. When new reports are released by AWS, they are immediately made available for you to download in AWS Artifact. For more information, visit the AWS Artifact webpages: AWS Artifact Website, AWS Artifact Video Tutorial, Getting Started Quick Guide, AWS Artifact FAQs.

To get started, sign in to the console and search Artifact. If you do not already have an AWS account, you can create one following the steps below. There is no charge associated with creating an account and using AWS Artifact to download compliance reports.

STEP 1: Go to www.aws.amazon.com and click the Sign Up button in the top right.

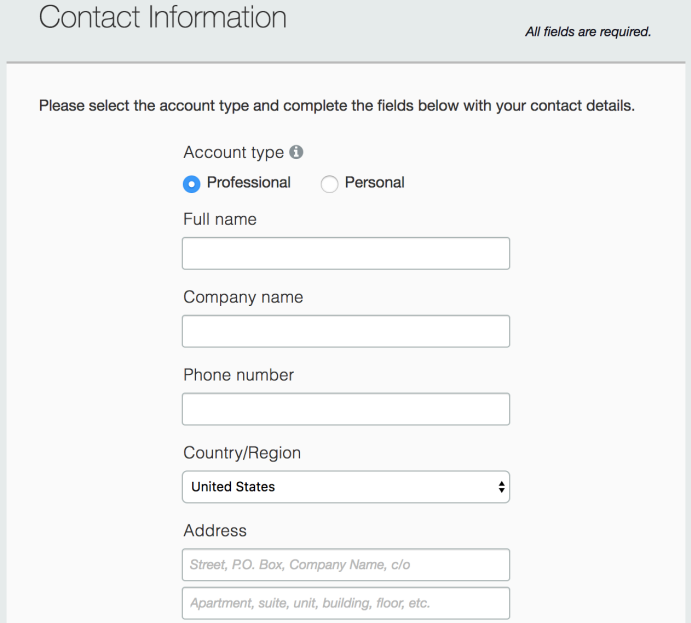


STEP 2: Enter an email address. If your company has a business need to access to the AWS SOC report, please sign up using your company email address, as approval will be required to download the report.

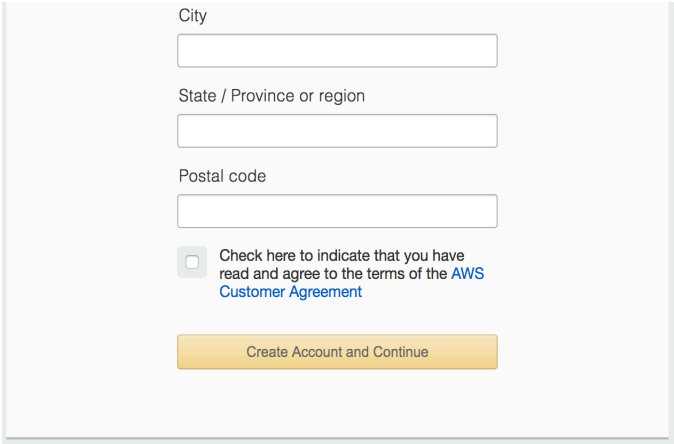


Download AWS Compliance Reports with [AWS Artifact]

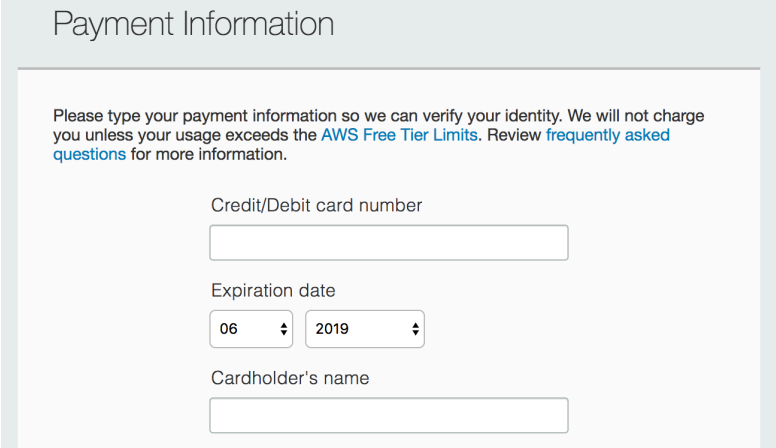
STEP 3: Complete the form.



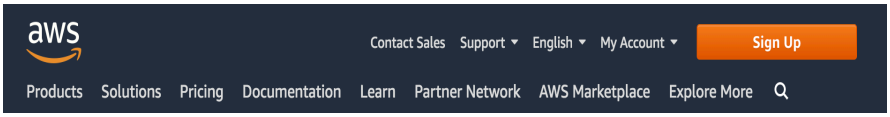
STEP 4: Continue filling out the form. Please make sure to check the box to indicate you're accepting the Customer Agreement.



STEP 5: You'll be taken to the payments screen. Since AWS Artifact is a free service, **you do not need to enter in CC Information**. Instead, just type in www.aws.amazon.com into your browser.

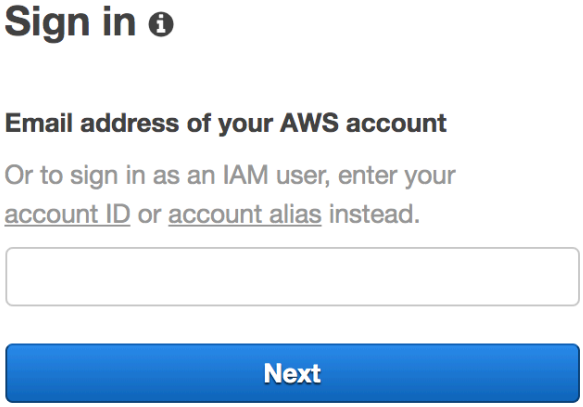


STEP 6a: Click the AWS Management Console link under "My Account".

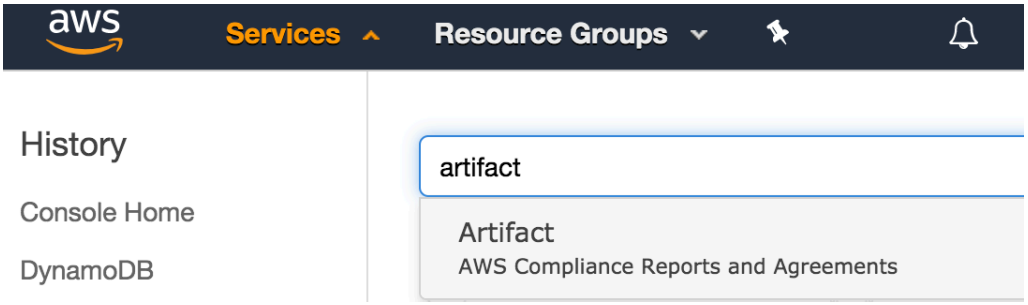


Download AWS Compliance Reports with [AWS Artifact]

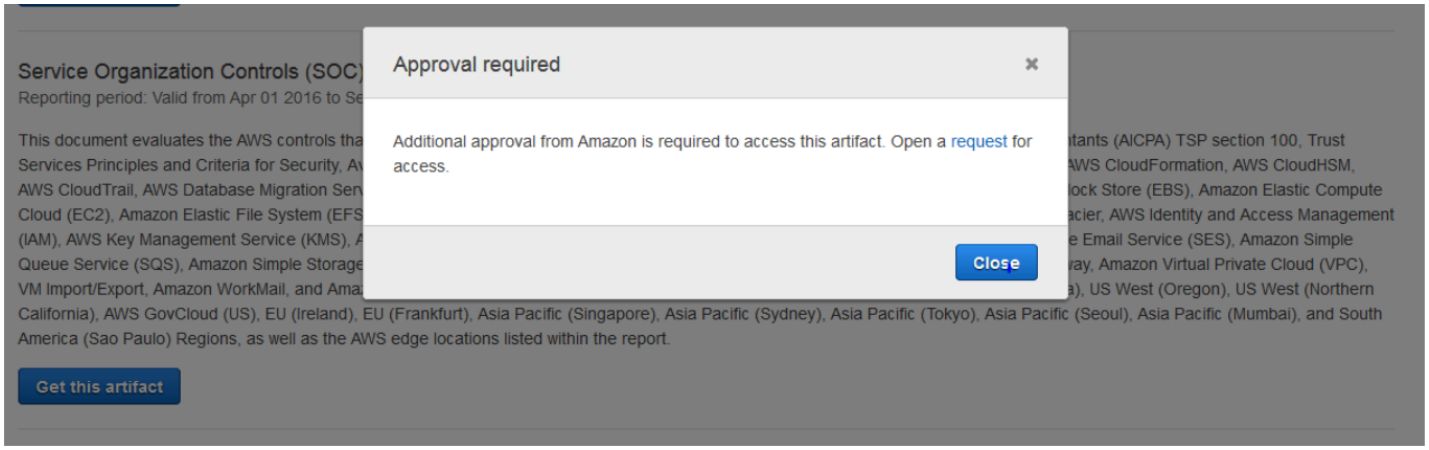
STEP 6b: Login using the credentials you setup on step 3.



STEP 7: Sign in and search 'Artifact' or 'Compliance Reports'

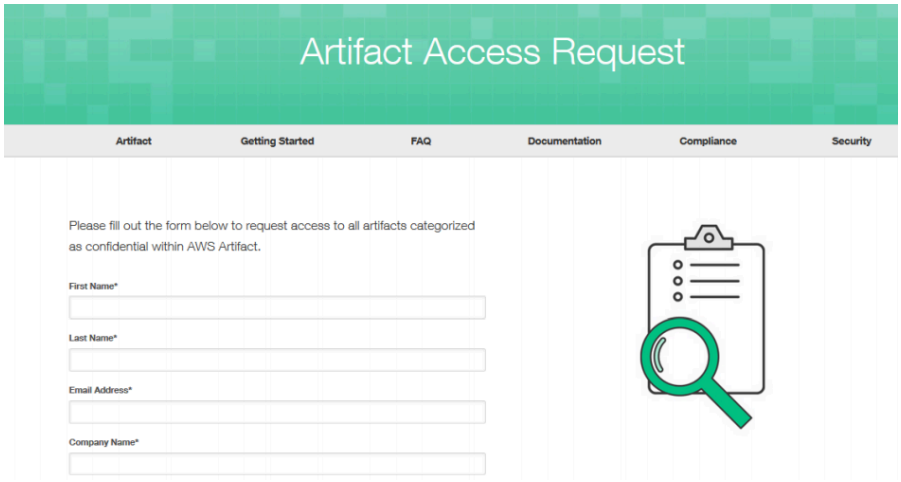


STEP 8: You can now begin downloading AWS Compliance Reports! Access to some reports, such as the AWS PCI report, will require you sign a click-through NDA with AWS before downloading. The AWS SOC report requires additional approval to download. This is because only companies with a business need are granted access. The SOC report is not available to customer for personal purposes. You will be prompted to open a request, as shown below.

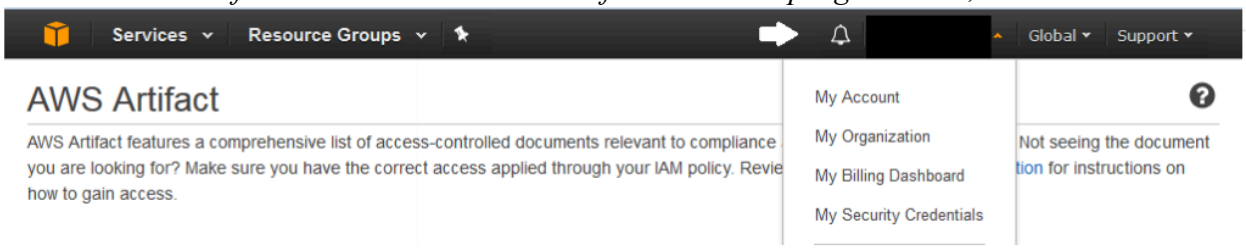


Download AWS Compliance Reports with [AWS Artifact]

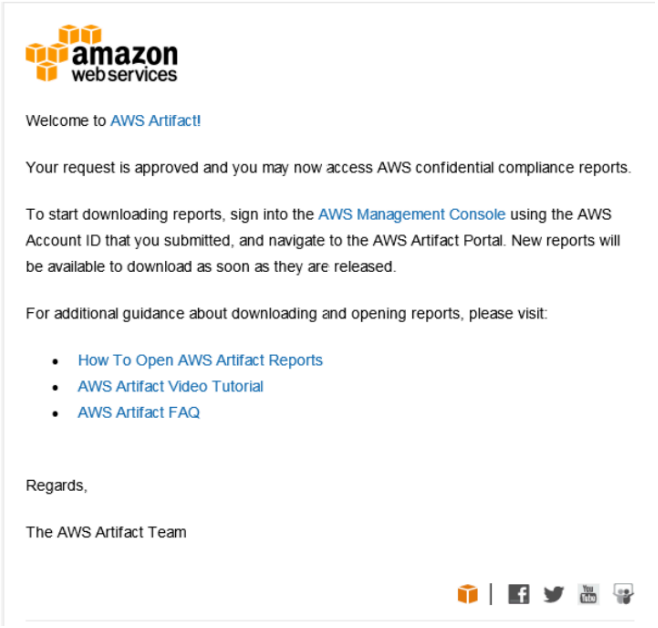
STEP 9: Fill out the form and you will be granted permanent access moving forward. Please be sure to include your Company name and Company email to receive access. Access will be granted within 24 hours and you will receive an email confirmation once it is available for download. When new SOC reports are released by AWS, you will immediately have access to download the report via [AWS Artifact].



**If you are not sure what your 'AWS Account Number' is, you can find that number by visiting the 'My Account' section of the console. This section is found in the top right corner, as shown below.*



Step 10: Within 24 hours you will receive an email confirmation from awscompliance@amazon.com that your account has been granted access to download the AWS SOC report. You can now log back into your account and download the SOC reports.



DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Name, Title)

Joseph Darminio - Account Manager

(Printed Name and Title)

10411 Motor City Drive #700 Bethesda, MD 20817

(Address)

443-690-4109

(Phone Number) / (Fax Number)

jdarminio@jtekds.com

(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

JTEK Data Solutions

(Company)

(Authorized Signature) (Representative Name, Title)

Joseph Darminio - Account Manager

(Printed Name and Title of Authorized Representative)

10/6/20

(Date)

443-690-4109

(Phone Number) (Fax Number)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: OT20131

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

- [x] Addendum No. 1
- [x] Addendum No. 2
- [x] Addendum No. 3
- [x] Addendum No. 4
- [ ] Addendum No. 5
- [ ] Addendum No. 6
- [ ] Addendum No. 7
- [ ] Addendum No. 8
- [ ] Addendum No. 9
- [ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

JTEK Data Solutions
Company

Authorized Signature

10/6/20
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: [illegible]

Authorized Signature: [signature] Date: 10/6/20

State of Maryland

County of Montgomery, to-wit:

Taken, subscribed, and sworn to before me this ___ day of _____, 20___.

My Commission expires _____, 20___.

AFFIX SEAL HERE

NOTARY PUBLIC _____

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

Pursuant to *W. Va. Code* § 6D-1-2, a state agency may not enter into a contract, or a series of related contracts, that has/have an actual or estimated value of $1 million or more until the business entity submits to the contracting state agency a Disclosure of Interested Parties to the applicable contract. In addition, the business entity awarded a contract is obligated to submit a supplemental Disclosure of Interested Parties reflecting any new or differing interested parties to the contract within 30 days following the completion or termination of the applicable contract.

For purposes of complying with these requirements, the following definitions apply:

"Business entity" means any entity recognized by law through which business is conducted, including a sole proprietorship, partnership or corporation, but does not include publicly traded companies listed on a national or international stock exchange.

"Interested party" or *"Interested parties"* means:

(1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors;
(2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract. (This subdivision does not apply to a publicly traded company); and
(3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency. (This subdivision does not apply to persons or business entities performing legal services related to the negotiation or drafting of the applicable contract.)

"State agency" means a board, commission, office, department or other agency in the executive, judicial or legislative branch of state government, including publicly funded institutions of higher education: Provided, that for purposes of W. Va. Code § 6D-1-2, the West Virginia Investment Management Board shall not be deemed a state agency nor subject to the requirements of that provision.

The contracting business entity must complete this form and submit it to the contracting state agency prior to contract award and to complete another form within 30 days of contract completion or termination.

This form was created by the State of West Virginia Ethics Commission, 210 Brooks Street, Suite 300, Charleston, WV 25301-1804. Telephone: (304)558-0664; fax: (304)558-2169; e-mail: ethics@wv.gov; website: www.ethics.wv.gov.

Revised June 8, 2018

EXHIBIT A – Pricing Page
GRC Software Solution RFQ - OT21047

Section	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1, 4.2	Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	80288.40	$ 80,288.40
4.1.3	Contract Item #2: Post Implementation Customization	HR	200.00	875.00	$ 175,000.00
4.1, 4.2	Optional Renewal Year 2: Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	59944.00	$ 59,944.00
4.1.3	Optional Renewal Year 2: Contract Item #2: Post Implementation Customization	HR	200.00	108.00	$ 21,600.00
4.1, 4.2	Optional Renewal Year 3: Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	59944.00	$ 59,944.00
4.1.3	Optional Renewal Year 3:Contract Item #2: Post Implementation Customization	HR	200.00	108.00	$ 21,600.00
4.1, 4.2	Optional Renewal Year 4: Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	59944.00	$ 59,944.00
4.1.3	Optional Renewal Year 4:: Post Implementation Customization	HR	200.00	108.00	$ 21,600.00
			Total Cost	$	499,920.40

Contract will be evaluated on all lines but only awarded on first year. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

Vendor Signature: 10/7/20 Date: