



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.

Header 6

List View

- General Information**
- Contact
- Default Values
- Discount
- Document Information
- Clarification Request

Procurement Folder: 2012913

Procurement Type: Central Contract - Fixed Amt

Vendor ID:

Legal Name:

Alias/DBA: FRC

Total Bid: \$946,584.00

Response Date:

Response Time:

Responded By User ID:

First Name:

Last Name:

Email:

Phone:

SO Doc Code: CRFQ

SO Dept: 0231

SO Doc ID: OOT2700000002

Published Date: 8/6/26

Close Date: 8/11/26

Close Time: 13:30

Status: Closed

Solicitation Description:

Total of Header Attachments: 6

Total of All Attachments: 6



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: 2012913
Solicitation Description: Addendum No 4-Governance, Risk and Compliance Auto Platform
Proc Type: Central Contract - Fixed Amt

Solicitation Closes	Solicitation Response	Version
2026-08-11 13:30	SR 0231 ESR08102600000000906	1

VENDOR
VS0000053091
Federal Resources Corporation

Solicitation Number: CRFQ 0231 OOT2700000002
Total Bid: 946584 **Response Date:** 2026-08-11 **Response Time:** 12:56:53
Comments: Please see the Pricing Narrative Document for additional details on pricing structure.

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

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

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 Maintenance and Support Year One (Initial term)	1.00000	EA	272436.000000	272436.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: Includes:

- TrustCloud Enterprise Edition Large Platform: Enterprise GRC foundation supporting one parent and up to 125 child organizational segments with unlimited users, common controls, policy management, SSO, data connectors, notifications, training, enterprise support/SLA, dashboards, and audit reporting. Provided at a nominal \$1.00 discounted price.
- TrustLens Third-Party Risk Assessments: Third-party registry supporting up to 50 annual vendor assessments and risk assessments for 125 child segments, with procurement/risk integrations, custom scoping and tiering, questionnaires, framework alignment, and advanced reporting. Additional child segments can be added on an ad-hoc basis following tiered pricing described in the attached Pricing Narrative.
- TrustOps Compliance Assurance: Control and policy mapping across up to 10 selected compliance framework families using a test once, comply many approach.
- Managed Services: Ongoing technical, operational, project management, and technical account support following implementation.
- Professional Services for implementation (one-time)

Extended Description:
Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	GRC Software Maintenance and Support Year 2 renewal	1.00000	EA	224716.000000	224716.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: Includes:

- TrustCloud Enterprise Edition Large Platform: Enterprise GRC foundation supporting one parent and up to 125 child organizational segments with unlimited users, common controls, policy management, SSO, data connectors, notifications, training, enterprise support/SLA, dashboards, and audit reporting. Provided at a nominal \$1.00 discounted price.
- TrustLens Third-Party Risk Assessments: Third-party registry supporting up to 50 annual vendor assessments and risk assessments for 125 child segments, with procurement/risk integrations, custom scoping and tiering, questionnaires, framework alignment, and advanced reporting. Additional child segments can be added on an ad-hoc basis following tiered pricing described in the attached Pricing Narrative.
- TrustOps Compliance Assurance: Control and policy mapping across up to 10 selected compliance framework families using a test once, comply many approach.
- Managed Services: Ongoing technical, operational, project management, and technical account support following implementation.

Extended Description:
Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	GRC Software Maintenance and Support Year 3 renewal	1.00000	EA	224716.000000	224716.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: Includes:

- TrustCloud Enterprise Edition Large Platform: Enterprise GRC foundation supporting one parent and up to 125 child organizational segments with unlimited users, common controls, policy management, SSO, data connectors, notifications, training, enterprise support/SLA, dashboards, and audit reporting. Provided at a nominal \$1.00 discounted price.
- TrustLens Third-Party Risk Assessments: Third-party registry supporting up to 50 annual vendor assessments and risk assessments for 125 child segments, with procurement/risk integrations, custom scoping and tiering, questionnaires, framework alignment, and advanced reporting. Additional child segments can be added on an ad-hoc basis following tiered pricing described in the attached Pricing Narrative.
- TrustOps Compliance Assurance: Control and policy mapping across up to 10 selected compliance framework families using a test once, comply many approach.
- Managed Services: Ongoing technical, operational, project management, and technical account support following implementation.

Extended Description:

Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	GRC Software Maintenance and Support Year 4 renewal	1.00000	EA	224716.000000	224716.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: Includes:

- TrustCloud Enterprise Edition Large Platform: Enterprise GRC foundation supporting one parent and up to 125 child organizational segments with unlimited users, common controls, policy management, SSO, data connectors, notifications, training, enterprise support/SLA, dashboards, and audit reporting. Provided at a nominal \$1.00 discounted price.
- TrustLens Third-Party Risk Assessments: Third-party registry supporting up to 50 annual vendor assessments and risk assessments for 125 child segments, with procurement/risk integrations, custom scoping and tiering, questionnaires, framework alignment, and advanced reporting. Additional child segments can be added on an ad-hoc basis following tiered pricing described in the attached Pricing Narrative.
- TrustOps Compliance Assurance: Control and policy mapping across up to 10 selected compliance framework families using a test once, comply many approach.
- Managed Services: Ongoing technical, operational, project management, and technical account support following implementation.

Extended Description:

Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9



REQUEST FOR QUOTE RESPONSE

WEST VIRGINIA OFFICE OF TECHNOLOGY

BID FOR GOVERNANCE, RISK, AND COMPLIANCE AUTOMATION PLATFORM

CRFQ 0231 OOT2700000002

RESPONSE DATE: 08/11/2026

SUBMITTED TO:
DEPARTMENT OF ADMINISTRATION,
PURCHASING DIVISION
TOBY.L.WELCH@WV.GOV

SUBMITTED BY:

FRC

1401 STATE STREET, STE 201
ERIE, PA 16501
PHONE: 814-636-8020
FAX: 301-990-1378

DUNS: 102932709
CAGE: 1QBT0
UEI: FZK7KZZJYNQ9

FRC POINT OF CONTACT:

CHRIS ZEIDERS

VICE PRESIDENT –
TECHNOLOGY AND INNOVATION
(703)-795-3257
CZEIDERS@FEDRESOURCES.COM

This response includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this response. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in all sheets.

TABLE OF CONTENTS

Table of Contents	1
Executive Summary.....	2
Introduction.....	2
Qualifications	3
3.1 Authorized by GRC Software Company.....	3
Mandatory Requirements	4
4.1 Software Maintenance and Support	4
4.2 Training Deliverables	5
4.3 Architectural, RBAC, & Dashboard Requirements	5
4.4 Platform Authentication & Single Sign-On (SSO)	6
4.5 Tiered and Modular Licensing Requirements	7
4.6 Custom Assessments & Framework Questionnaire Engine	8
4.7 Hybrid Environment Tracking (Cloud & On-Premise)	9
4.8 Risk Register & POAM Management	9
4.9 Service Level Agreement (SLA) & Support	10
Contract Manager	10

EXECUTIVE SUMMARY

The West Virginia Office of Technology (WVOT) is seeking a cloud-based Governance, Risk, and Compliance (GRC) platform to strengthen statewide cybersecurity governance, standardize compliance assessments, improve enterprise risk visibility, and automate governance processes across approximately 125 participating agencies and organizations. The solution must support the West Virginia Cybersecurity Framework (WVCSF), NIST Cybersecurity Framework (CSF), centralized evidence management, Plan of Action and Milestones (POA&M) tracking, workflow automation, and comprehensive reporting.

Federal Resources Corporation (FRC) is pleased to submit this response proposing the TrustCloud Governance, Risk, and Compliance platform. TrustCloud is a secure, cloud-native Software-as-a-Service (SaaS) solution that unifies governance, risk, compliance, policy management, third-party risk management, and workflow automation within a single platform. Through configurable workflows, continuous evidence collection, native integrations with Microsoft Entra ID and other enterprise technologies, agency-specific workspaces, role-based access, and centralized administration, TrustCloud enables WVOT to efficiently manage cybersecurity, compliance, and risk activities across the enterprise.

FRC will serve as the prime contractor and single point of accountability, supported by TrustCloud's implementation, cybersecurity, product, and customer success professionals. Together, FRC and TrustCloud offer a proven solution that satisfies the technical, functional, operational, and support requirements of the solicitation while providing a scalable platform that supports WVOT's long-term cybersecurity and compliance objectives.

INTRODUCTION

FRC is pleased to submit this proposal in response to **CRFQ # 0231 OOT2700000002, External Governance, Risk, and Compliance Automation Platform**. Our proposed solution is designed to satisfy the functional, technical, operational, and security requirements identified in the solicitation while supporting the West Virginia Office of Technology's mission to strengthen cybersecurity governance, improve compliance visibility, and enable consistent risk management practices across State government.

FRC is a 100% U.S.-owned small business headquartered in Erie, Pennsylvania. Since 1998, FRC has delivered cybersecurity, information technology, and professional services to Federal, state, and local government organizations. FRC maintains mature quality and project management processes, including ISO 9001:2015 certification and CMMI Maturity Level 3 appraisal. For this engagement, FRC will serve as the prime contractor and single point of accountability for contract administration, implementation, invoicing, and customer support.

FRC has partnered with **TrustCloud** (<https://www.trustcloud.ai/>) to deliver a modern Governance, Risk, and Compliance solution tailored to WVOT's objectives. TrustCloud provides an integrated SaaS platform that aligns with the operational, security, and functional requirements identified in this RFQ. By combining governance, enterprise risk

management, compliance management, policy management, third-party risk management, workflow automation, evidence management, reporting, and dashboarding within a single platform, TrustCloud enables WVOT to replace manual processes with standardized, repeatable workflows while improving visibility into enterprise compliance and cybersecurity activities.

Throughout this proposal, we will refer to FRC and TrustCloud collectively as “**Team FRC**”. The following sections describe the proposed solution and demonstrate how Team FRC satisfies the requirements set forth in the solicitation.

Understanding WVOT’s Objectives

Team FRC understands that WVOT is seeking more than a software application. The State is establishing an enterprise GRC platform that will strengthen cybersecurity governance, standardize compliance assessments, improve visibility into enterprise risk, and provide a scalable foundation for managing governance, risk, compliance, and third-party risk activities across approximately 125 participating agencies and organizations.

The solicitation emphasizes the need for a centralized solution that supports the West Virginia Cybersecurity Framework (WVCSF), NIST Cybersecurity Framework (CSF), automated evidence collection, Plan of Action and Milestones (POA&M) management, configurable workflows, role-based access, Microsoft Entra ID integration, agency-specific workspaces, and executive reporting. These capabilities are intended to reduce manual effort, improve consistency across participating agencies, and provide WVOT with timely, actionable information to support cybersecurity and compliance oversight.

TrustCloud directly aligns with these objectives by providing a cloud-native SaaS platform that integrates governance, enterprise risk management, compliance management, third-party risk management, policy management, workflow automation, and reporting within a single environment. The platform is designed to automate compliance activities, centralize evidence management, streamline assessment workflows, and provide the visibility and operational efficiency necessary to support WVOT's enterprise governance and cybersecurity program while remaining flexible as the State's requirements evolve.

QUALIFICATIONS

Team FRC meets the mandatory qualifications outlined in the RFQ.

3.1 AUTHORIZED BY GRC SOFTWARE COMPANY

Qualification 3.1: Vendor must be authorized by GRC software company to provide software maintenance and support for the Licenses and provide proof of authorization upon request.

FRC is an authorized TrustCloud partner and provides software maintenance and support for the licensed platform throughout the contract term, with proof of authorization from TrustCloud available on request. Maintenance, updates, and technical support are delivered jointly by FRC and TrustCloud.

As part of our submission, we have included a Manufacturer Authorization Letter, which will be uploaded as an attachment to our submission on the portal.

MANDATORY REQUIREMENTS

Team FRC meets all the designated mandatory requirements outlined in the RFQ, outlined in Section 4.

4.1 SOFTWARE MAINTENANCE AND SUPPORT

4.1.1. Deployment Sizing: *The baseline platform license must natively include the central WVOT hub and 125 fully segregated child workspaces (tenants) upon deployment.*

Yes. TrustCloud supports a federated, parent-child architecture in which a central WVOT hub delivers aggregate, real-time visibility while each agency operates in its own fully data-isolated workspace, an approach already proven across dozens of agencies (e.g., State of New Mexico). The central hub plus 125 fully segregated child workspaces can be provisioned at deployment with strict tenant isolation and workspace-scoped RBAC.

4.1.2. Initial Contract Term: *The contract awarded from this Solicitation shall be for an initial period of one (1) year.*

Accepted. FRC/TrustCloud will provide the platform under an initial one-year term.

4.1.3. Renewal Term Clauses: *The contract may be renewed upon mutual written consent of the Agency and the Vendor, and approval of the Purchasing Division, for up to three (3) optional one-year renewal periods (for a total potential contract life of 4 years), under the same pricing, terms, and conditions as specified herein. Each subsequent terms will run consecutively to the prior term.*

Accepted. The agreement will accommodate up to three optional one-year renewal periods (four-year total potential term) at the agreed pricing, subject to mutual consent and Purchasing Division approval.

4.1.4. On-Demand Workspace Expansion: *The platform must support the dynamic provisioning of additional workspace licenses via a fixed, on-demand unit price structure. Any additional workspace licenses added mid-term must be billed on a prorated basis for the remainder of the active contract year and shall renew at the full annual unit rate at the start of the subsequent renewal term.*

Yes. Additional agency workspaces can be provisioned on demand beyond the baseline 125, and FRC can hold a fixed per-workspace unit price for the contract. Mid-term additions can be billed on a prorated basis for the remainder of the active contract year and renew at

the full annual unit rate in the next term, consistent with the RFP. Final proration and unit-price mechanics will be reflected on the Pricing Page and subscription agreement.

4.2 TRAINING DELIVERABLES

4.2.1 Train-the-Trainer Program: *Vendor must provide a formal program consisting of virtual, instructor-led sessions for central WVOT administrators.*

Yes. Team FRC delivers role-based, instructor-led enablement sessions virtually (or in person), and these can be recorded for future playback and internal reuse, supporting a train-the-trainer model for central WVOT administrators and agency roles. Training scope is defined during implementation onboarding.

4.2.2 On-Demand Materials: *Vendor must provide on-demand digital training materials, video tutorials, or manuals for local agency-level end users.*

Yes. All users receive access to TrustCloud FlightSchool, an on-demand knowledge base with user guides, interactive tutorials, and video walkthroughs covering every module. The library is searchable and continuously updated, supporting self-service learning for agency end users.

4.3 ARCHITECTURAL, RBAC, & DASHBOARD REQUIREMENTS

4.3.1 Central WVOT Hub: *The platform must provide a centralized dashboard for the WVOT Chief Information Security Officer (CISO) to view the aggregate, real-time compliance and risk posture of all state entities.*

Yes. TrustCloud provides an out-of-the-box CISO/enterprise dashboard that aggregates real-time compliance and risk posture across all entities, with agency-specific data isolated by RBAC. This gives the WVOT CISO a single, real-time view of the aggregate posture of all state entities from the central hub.

4.3.2 Granular, Role-Based Access Control (RBAC): *The platform must enforce strict RBAC to ensure that local agency entities can only view, edit, or manage data within their own sandbox workspace. Agency users must be restricted to their own specific audit information, risk assessments, evidence lockers, and remediation plans.*

Yes. RBAC is enforced at the individual workspace/tenant level, so local agency users can only view, edit, or manage data within their own sandboxed workspace, including their own audit information, risk assessments, evidence lockers, and remediation plans. Isolation is achieved through instance-level segmentation combined with granular, least-privilege role permissions.

4.3.3 Predefined Platform Roles: *The platform must support predefined and custom roles, including Agency Security Officer (read/write internal), External Auditor (read-only to specific audit files), and Executive Observer (dashboard view only). Central WVOT administrators must retain global master access across all workspaces.*

Yes. TrustCloud ships with out-of-the-box roles and supports fully custom roles, which can be mapped to WVOT's defined roles: Agency Security Officer (read/write in their workspace), External Auditor (read-only to specific audit files), and Executive Observer (dashboard view only), while WVOT central administrators retain global master access. Roles can also be mapped from directory groups for streamlined onboarding/offboarding. We recommend a short mapping session to align OOTB roles precisely with WVOT's ASO/EA/EO definitions.

4.3.4 Executive Dashboards & Audit Exporting: *The platform must include automated report generation capabilities, allowing WVOT and agencies to export executive dashboards, compliance summaries, and System Security Plans (SSPs) in standard formats (e.g., PDF, Excel, CSV) for external auditors and executive leadership.*

Yes. Executive dashboards and compliance summaries export in standard formats (PDF, Excel, CSV), and control test results and evidence export as audit packets with full traceability. TrustCloud also supports OSCAL-formatted authorization artifacts (SSP, SAP, SAR, POA&M). If WVOT provides its preferred SSP template, TrustCloud can populate and generate SSPs against it. In addition, TrustCloud provides API access to all tenant data enabling our customers to build dashboards with their preferred data visualization tool.

4.4 PLATFORM AUTHENTICATION & SINGLE SIGN-ON (SSO)

4.4.1 Native Integration: *The platform must natively support SAML 2.0 and OpenID Connect (OIDC) protocols to allow seamless federated Single Sign-On (SSO). MF A must be supported for the platform.*

Yes. The platform natively supports federated SSO via SAML 2.0, OAuth 2.0, and OpenID Connect (OIDC), and MFA is supported. These are standard, in-production capabilities across TrustCloud deployments.

4.4.2 WVOT Tenant Authentication: *The system must integrate directly with WVOT's centralized Microsoft Entra ID tenant to allow state-issued corporate credentials to authenticate users.*

Yes. TrustCloud integrates directly with Microsoft Entra ID (Azure AD), allowing WVOT's state-issued corporate credentials to authenticate users, with support for Just-in-Time provisioning and directory-group role mapping.

4.5 TIERED AND MODULAR LICENSING REQUIREMENTS

4.5.1. The Core Tier (Mandatory for All Workspaces): *Every workspace must include access to the core framework libraries (including WVCSF, NIST, and other industry-recognized standards), audit logging, RBAC, Entra ID SSO authentication, and the custom questionnaire engine.*

Yes. The Core Tier capabilities are supported: TrustCloud's Common Control Framework provides 1,000+ prebuilt controls across 20+ standards (including NIST), with audit logging, RBAC, Entra ID SSO, and the custom questionnaire engine included in every workspace. WVCSF would be loaded as a custom framework and mapped to TrustCloud's control set (AI-assisted mapping accelerates this).

4.5.2 Continuous Control Monitoring (CCM) Add-On Module: *The platform must allow WVOT to enable native API automated evidence collection strictly for select workspaces. The platform must natively support and pull configuration data from the State's existing infrastructure, which includes Microsoft Entra ID, Google Workspace, Palo Alto Networks, SentinelOne, and Active Directory.*

Yes. Continuous Control Monitoring is native to TrustOps and a core strength, using API-based connectors to automatically collect and test evidence, and it can be selectively enabled per workspace. TrustCloud has native connectors for Microsoft Entra ID, Google Workspace, and Active Directory, among others. Any connectors not yet available can be built as new data feeds (typically within weeks).

4.5.3. Native Integration Maintenance: *The Vendor is solely responsible for maintaining and updating these native API connectors throughout the life of the contract at no additional cost to the State.*

Yes. TrustCloud maintains and updates its library of 150+ native API connectors as part of the platform and adds new connectors as customers require them. We can commit to maintaining the connectors WVOT uses throughout the contract.

4.5.4 Third-Party Risk Management (TPRM) Add-On Module: *The platform must allow WVOT to selectively enable the Vendor Risk Management module (for external vendor compliance tracking and questionnaire automation) for specific workspaces.*

Yes. TrustCloud's Third-Party/Vendor Risk Management module (TrustLens) supports selective enablement by WV personnel. It supports full-lifecycle vendor risk; onboarding, assessment, continuous monitoring, and offboarding, and can be selectively enabled for specific workspaces. Vendor questionnaires and scoring align to the same control framework used elsewhere in the platform.

4.5.5 Implementation Timeline & Support: *Vendor must provide dedicated implementation professional services to assist WVOT with the initial API integrations to the core security stack.*

Confirmed. Team FRC provides dedicated implementation professional services, including establishing and configuring the API integrations to WVOT's core security stack, control-to-framework mapping, and evidence-collection validation. A typical engagement runs on the order of ~10 weeks and includes a dedicated Customer Success Manager.

4.6 CUSTOM ASSESSMENTS & FRAMEWORK QUESTIONNAIRE ENGINE

4.6.1 Custom Questionnaire Builder: *The platform must feature a flexible, custom questionnaire engine allowing WVOT administrators to design, schedule, and distribute custom risk assessments to any activated workspace.*

Yes. TrustCloud's questionnaire/assessment engine lets WVOT administrators design, configure, schedule, and distribute custom risk assessments to any activated workspace, with conditional logic, version control, assignment tracking, reminders, and exception handling. Assessments can be built manually or AI-assisted from the control graph.

4.6.2 Framework Specific Assessment Alignment: *The tool must allow WVOT to map these custom questionnaires directly to the controls of the West Virginia Cyber Security Framework (WVCSF) as well as industry-standard frameworks such as NIST. When an agency answers a custom question and attaches evidence, the system must automatically score, cross-map, and update that agency's active maturity baselines across all selected frameworks simultaneously.*

Yes. This is a core strength. Custom questionnaire items map to controls in selected frameworks (NIST and others), and because controls are cross-mapped, a single answered question with attached evidence automatically scores and updates the agency's maturity baselines across all selected frameworks simultaneously ('test once, satisfy many'). WVCSF would be loaded as a custom framework and mapped to the control set so it participates in the same cross-mapping and scoring.

4.7 HYBRID ENVIRONMENT TRACKING (CLOUD & ON-PREMISE)

4.7.1 Hybrid Operations Baseline: *The platform must support concurrent hybrid compliance tracking capability inside individual sandboxed workspaces.*

Yes. Each agency operates in its own isolated ('sandboxed') workspace that can track cloud and on-premises compliance concurrently. TrustCloud's Hybrid Data Fabric ingests evidence from native integrations and also supports secure manual upload, all governed by workspace-level RBAC. This lets each agency maintain a complete hybrid posture within its segregated environment.

4.7.2 Automated Evidence Ingestion: *Ability to ingest dynamic configuration checks from AWS, Azure, GCP, Active Directory, Cisco, and Palo Alto networks environments.*

Yes. TrustCloud provides automated evidence ingestion via 150+ connectors, with native support for AWS, Azure, GCP, and Active Directory among the listed sources. Where a source is not yet available out of the box, TrustCloud can build the data feed (typically within weeks).

4.7.3 On-Premises Workflow Portals: *Clean, workflow-driven portals for manual evidence gathering for legacy systems that cannot utilize direct automated validation checks to manually upload physical security proofs, System Security Plans (SSPs), and text/CSV configuration exports.*

Yes. For legacy or on-premises systems that cannot be validated automatically, TrustCloud provides clean, workflow-driven portals for manual evidence gathering, allowing upload of physical security proofs, SSPs, and text/CSV configuration exports. Uploaded artifacts are version-controlled, metadata-tagged, and stored in an RBAC-governed evidence repository.

4.8 RISK REGISTER & POAM MANAGEMENT

4.8.1 POAM Tracking: *The platform must include a centralized Risk Register capable of generating and tracking Plans of Action and Milestones (POAMs).*

Yes. TrustRegister provides a centralized Risk Register that tracks POAMs/remediation items and continuously monitors their status to reflect real-time residual risk. If WVOT provides its POAM template, TrustCloud can generate the artifacts accordingly.

4.8.2 Exception Workflows: *The platform must support a formal Risk Exception workflow, allowing local agencies to submit exception requests and justification documentation for central WVOT CISO review and approval.*

Yes. TrustCloud supports formal exception handling, enabling local agencies to submit risk exception requests with justification documentation for central WVOT CISO review and approval, with routing and statuses tracked in the platform.

4.9 SERVICE LEVEL AGREEMENT (SLA) & SUPPORT

4.9.1 System Uptime: *The proposed SaaS platform must guarantee a minimum 99.9% system uptime.*

Yes. TrustCloud is a SaaS platform hosted on AWS with a multi-availability-zone architecture and automatic failover designed for high availability, and Availability is covered

under its SOC 2 Type II. The specific 99.9% uptime commitment will be documented in the SaaS subscription/SLA agreement.

4.9.2 Support Availability: *The Vendor must provide standard technical support (minimum 8:00 AM - 5:00 PM EST, Monday through Friday) for central WVOT administrators, with defined response times for critical system outages.*

Yes. Team FRC provides standard technical support for central WVOT administrators and can meet the required 8:00 AM–5:00 PM ET (M–F) coverage, with defined response times by severity, including expedited response for critical outages. Severity-based response targets are documented in TrustCloud's SLA.

4.9.3 Agreement Submission: *Vendor must provide a copy of all applicable maintenance, support, and SaaS subscription agreements prior to contract award for review and approval by the State of West Virginia.*

Accepted. FRC/TrustCloud will provide copies of all applicable maintenance, support, and SaaS subscription agreements prior to contract award for the State's review and approval.

CONTRACT MANAGER

FRC certifies that, throughout the performance of the Contract, FRC will designate and maintain a primary Contract Manager responsible for overseeing Team FRC's responsibilities under the Contract. The designated Contract manager will be available during normal business hours to address customer service or other issues related to this Contract.

Contract Manager: Corey Luthringer

Telephone Number: 814.392.2236

Fax Number: 301.990.1378

Email Address: cluthringer@fedresources.com

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ OOT27*002

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:

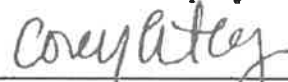
(Check the box next to each addendum received)

☒ Addendum No. 1	☐ Addendum No. 6
☒ Addendum No. 2	☐ Addendum No. 7
☒ Addendum No. 3	☐ Addendum No. 8
☒ Addendum No. 4	☐ Addendum No. 9
☐ Addendum No. 5	☐ 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.

Federal Resources Corporation, dba FRC

Company



Authorized Signature

August 10, 2026

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

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.

(Printed Name and Title) Corey Luthringer, VP of Operations & Administration

(Address) 1401 State Street, Ste 201, Erie, PA 16501

(Phone Number) / (Fax Number) 814-392-2236 (phone) / 301-990-1378 (fax)

(email address) cluthringer@fedresources.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract 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/Contract 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 this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; 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.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Federal Resources Corporation, dba FRC

(Company)

Corey Luthringer

(Signature of Authorized Representative)

Corey Luthringer, VP of Operations & Administration, August 10, 2026

(Printed Name and Title of Authorized Representative) (Date)

814-392-2236 (phone) / 301-990-1378 (fax)

(Phone Number) (Fax Number)

cluthringer@fedresources.com

(Email Address)



TrustCloud Corporation
16 Spy Pond Parkway
Arlington, MA 02474
www.trustcloud.ai
support@trustcloud.ai

Date: August 10, 2026

To: State of West Virginia, Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, West Virginia 25305
Attention: Toby L. Welch, Senior Buyer – Purchasing Division

RE: Manufacturer Authorization Letter for Solicitation # CRFQ 0231 OOT2700000002

Dear Toby L. Welch:

We, TrustCloud Corporation ("TrustCloud"), being the original equipment manufacturer of TrustCloud Trust Assurance platform and its modules — TrustOps, TrustRegister, TrustLens, TrustShare, together with the TrustCloud Common Control Framework and native API integration library, having our principal place of business at 16 Spy Pond Parkway, Arlington, MA 02474, do hereby authorize Federal Resources Corporation (dba FRC), located at 1401 State Street, Ste 201, Erie, PA 16051, as our official and authorized reseller/partner for the term of this project.

Under this authorization, the said reseller is granted the full right to quote, market, sell, and supply the TrustCloud platform for the aforementioned project or tender reference CRFQ 0231 OOT2700000002.

We hereby confirm that Federal Resources Corporation is an active, certified partner in good standing. We extend our full manufacturer backing as follows:

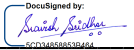
- We guarantee that the products supplied are genuine, brand new, and carry our standard manufacturer warranty of three (3) years.



- We confirm that we will provide technical support and authorized parts/maintenance backstopping through our authorized channels for the duration of the project commitment.

This authorization remains valid until 12/31/2030 unless revoked or extended in writing by TrustCloud.

Sincerely,


DocuSigned by:
Sravish Sridhar
5F7146085C3B464

Sravish Sridhar
Chief Executive Officer
TrustCloud Corporation
(512) 294-4201
ss@trustcloud.ai

FRC-TrustCloud MASTER SERVICE AGREEMENT

This Master Service Agreement (“MSA”) is incorporated into and made part of the Agreement between **Federal Resources Corporation (FRC)** (“Prime Contractor”) and the **[Customer]** (“Customer”). The following terms and conditions are flowed down from TrustCloud and shall apply to the Customer’s use of the Products.

This agreement establishes the general terms and conditions under which Prime Contractor may provide products and/or services to the Customer pursuant to one or more written purchase orders (“POs”), statements of work (“SOWs”) or quotes referencing this Agreement.

1. Software License

TrustCloud grants the Customer a limited, non-exclusive, non-transferable, royalty-free, worldwide license during the term of this Agreement, solely for internal business purposes and in accordance with the limitations set forth in the applicable Order:

- (a) to access, use, perform, and digitally display the Software in accordance with the Documentation; and
- (b) to use and reproduce a reasonable number of copies of the Documentation solely to support use of the Software.

Except as expressly permitted, the Customer shall not:

- license, sublicense, sell, resell, transfer, assign, distribute, or otherwise commercially exploit the Software;
- modify or create derivative works;
- frame or mirror the Software on another server or device;
- decompile, disassemble, reverse engineer, or attempt to obtain source code;
- use the Software for competitive purposes;
- interfere with operation or access via unapproved interfaces; or
- use the Software in any manner inconsistent with law, Documentation, or this Agreement.

2. Acceptable Use

The Customer shall not, and shall not permit any third party to:

- Store infringing, obscene, unlawful, or tortious material;
- Store material containing viruses, worms, Trojan horses, or harmful code;
- Interfere with or disrupt the integrity or performance of the Software or data;
- Attempt to gain unauthorized access to the Software or related systems.

3. Customer Responsibilities

The Customer shall:

- Ensure Authorized Users comply with these Terms of Service;

- Be responsible for the content of Customer Data and provide TrustCloud with accurate information;
- Manage Authorized User credentials and maintain password security;
- Use commercially reasonable efforts to prevent unauthorized access and promptly notify TrustCloud of any such incidents.

4. Support and Availability

TrustCloud will provide support and availability in accordance with the terms attached hereto as Exhibit A.

5. Assurance AI Features

TrustCloud uses generative AI functionality (“Assurance AI”) to enhance the Software. By using the Software, the Customer consents to processing of Customer Data for the purposes outlined below.

- Customer Data may be used only:
 - as input for generative AI models to create content (answers, notes, summaries, remediation plans, suggestions). Generative AI models do not store Customer Data or use it beyond generating requested content.
- TrustCloud will not use Customer Data to train global generative models.
- TrustCloud adheres to SOC 2 cybersecurity standards and ISO 42001 AI governance standards. Details are available on the TrustCloud security and trust portal (<https://trust.TrustCloud.ai>).
- The Customer may opt-out of Assurance AI for TrustShare (if module is applicable) at any time by submitting a written request to support@TrustCloud.ai. TrustCloud will disable Assurance AI for the TrustShare module within seven (7) days of receipt.
- TrustCloud will operate Assurance AI in accordance with its AI Governance principles.

6. Flow-Down

These TrustCloud Terms of Service are flowed down to the Customer as a condition of TrustCloud’s licensing.

Federal Resources Corporation Representative	[Customer] Representative
---	----------------------------------

Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

EXHIBIT A: Enterprise Uptime and Support SLA

ENTERPRISE UPTIME SLA

Scope

TrustCloud's enterprise uptime SLA covers the Services.

Service Commitment

TrustCloud provides Customer access to the TrustCloud platform twenty-four hours a day, seven days a week (24x7) with a Monthly Uptime Percentage commitment ("Service Commitment") for the Services, as defined below:

- **Premium Service Commitment:** 99.9% Monthly Uptime Percentage

Monthly Uptime Percentage

To avoid intermittent and transient fluctuations, an outage period shall begin after observing four consecutive minutes of downtime in which the Services are unresponsive to the Customer during a period other than Scheduled Maintenance Downtime or Excluded Downtime ("Service Outage"). Furthermore, downtime must affect a significant number of requests or core functionality to qualify as a Service Outage.

"Monthly Uptime Percentage" will be calculated as follows: the number of minutes the Services are accessible and not suffering from a Service Outage as recorded by TrustCloud during each calendar month, divided by the total number of minutes in the calendar month. The resulting quotient is then multiplied by 100 to give a percentage.

Scheduled Maintenance and Excluded Downtime

TrustCloud reserves the right to perform regularly scheduled maintenance of the Services during non-core business hours ("Scheduled Maintenance Downtime"). Non-core business hours are defined as 10:00 PM to 4:00 AM (US Eastern Time Zone). TrustCloud may schedule additional Scheduled Maintenance Downtimes outside of the standing scheduled maintenance window by providing notification to the Customer at least three business days in advance. Additionally, any downtime caused by factors outside of TrustCloud's reasonable control do not factor into the Monthly Uptime Percentage calculation, including any force majeure event, internet services unavailability outside of TrustCloud's Services, any downtime resulting from outages of subprocessors, third party connections or utilities, and actions or inactions of the Customer ("Excluded Downtime").

Support Requests

The Customer must report and TrustCloud will respond to uptime related incidents and requests based on the process and response SLAs defined in the TrustCloud Enterprise Support SLA terms. If the Customer fails to report a Service Outage within two (2) days of the occurrence of such Service Outage, the Customer shall not be entitled to any Service Credit for such Service Outage.

Service Credits

If the Monthly Uptime Percentage fails to meet TrustCloud’s Service Commitment, the Customer will be eligible to receive a Service Credit, as detailed in the table below. Service credits provided under this SLA are available remedies for applicable service-level failures; provided, however, that such service credits shall not limit or exclude any rights or remedies available to Customer under the applicable agreement or mandatory State of West Virginia contract requirements. To receive a Service Credit, the Customer must submit a claim via one of the communication channels listed in the TrustCloud Support SLA. To be eligible, the credit request must be received by TrustCloud within 30 days after which the Service Outage occurred and must include: the dates and times of each Service Outage incident and logs or other types of evidence that document and corroborate the claimed Service Outage. If the Service Outage in the claim is confirmed by TrustCloud and the Monthly Uptime Percentage calculated by TrustCloud for the month when the Service Outage occurred is less than the Service Commitment, then TrustCloud will issue the Service Credit to the Customer within 60-days of the request having been confirmed by TrustCloud. Failure to provide the request and other information as required above will disqualify the Customer from receiving a Service Credit.

Premium Service Commitment: 99.9%

Monthly Uptime Percentage	“Service Credit”
99.9% or higher	Meets SLA. No Service Credit
< 99.9% but >= 99.5%	5% of monthly value of the subscription fees paid for the use of the Services or \$4,000, whichever is smaller.
< 99.5% but >= 98.0%	10% of monthly value of the subscription fees paid for the use of the Services or \$5,000, whichever is smaller.
< 98.0% but >=95.0%	20% of monthly value of the subscription fees paid for the use of the Services or \$7,000, whichever is smaller.
Below 95.0%	30% of monthly value of the subscription fees paid for the use of the Services or \$10,000, whichever is smaller.

ENTERPRISE SUPPORT SLA

Scope

TrustCloud's enterprise support SLA covers support for Services.

Support Commitment

As part of its enterprise uptime SLA, TrustCloud offers 24x7 support for Critical (SEV1) tickets and 24x5 support for all other times of support requests, bound by the Response Time SLA listed below. The support Response Time SLA below are the time frames in which the Customer can expect the first response. The TrustCloud support team will make commercially reasonable efforts to resolve any issues as quickly as possible. However, the SLA times are not an expected time-to-resolution.

Issue Qualification

When submitting a support ticket, the Customer will select both an impact priority level and a type. The impact priority will display definitions aligning with the table below. TrustCloud reserves the right to modify the priority level if the criteria for the priority level are not met.

Impact Priority Levels

Critical (SEV1):

- TrustCloud is down and unable to function AND no workaround is available; or
- All or a majority of Customer's data is at significant risk of loss or corruption; or
- Customer's business operations have been severely disrupted

High (SEV2):

- Operations can continue in a restricted fashion, although long-term productivity might be adversely affected; or
- A major milestone, project, or customer is at risk

Normal (SEV3)

- There is a problem with no notable impact or a minor impact on operations

Low (SEV4):

- There is a general question about functionality or features

Response Time SLA

The following table details the first response time support levels:

Impact Priority	First Response Time SLA	Hours of Operation	Support Initiation Process
Critical (SEV1)	2 hours	24 x 7	Customer is required to submit this type of support request through the TrustCloud Support Portal or by emailing support@trustcloud.ai .
High (SEV2)	4 hours	24 x 5	Customer is required to submit this type of support request through the TrustCloud Support Portal or by emailing support@trustcloud.ai .
Normal (SEV1)	8 hours	24 x 5	Customer is required to submit this type of support request through the TrustCloud Support Portal or by emailing support@trustcloud.ai .

For more information on opening a support ticket as part of the support initiation process, please review TrustCloud's Customer Support Process.

Phone and video call support

TrustCloud does not offer support via inbound or on-demand calls by default. If you wish to avail of call-based support, please speak to your account executive.

TrustCloud support engineers communicate with the Customer about tickets primarily through updates in the tickets themselves. At times it may be useful to conduct a call, video call, or screen sharing session with the Customer to improve the progress of a ticket. The support engineer may suggest a call for that reason. The Customer may also request a call if the Customer feels one is needed. Either way, the decision to conduct a call always rests with the support engineer, who will determine whether a call is necessary and whether TrustCloud has sufficient information for a successful call.

Note: Calls scheduled by TrustCloud Support are on the Zoom or Google Workspace platform. If neither of these work for you, TrustCloud support can join a call on the following other platforms: Microsoft Teams, Cisco Webex. Other video platforms are currently not supported.

Support SLA Credits

In the event of a violation of First Response Time SLA for Critical tickets, the Customer will be issued a Support SLA Credit of \$200 per incident. Requests for Support SLA Credits must be made within 30 days of the incident that triggered the credit, along with evidence that the

Support Initiation Process was followed and any other documentation to corroborate the claimed violation of First Response Time SLA. In no event shall total Support SLA Credits exceed \$5,000. A pending credit does not release the Customer from its obligation to pay TrustCloud's submitted invoices in full when due. Support SLA Credits are the Customer's sole and exclusive remedy to violations of this SLA.



PRICING NARRATIVE RESPONSE

WEST VIRGINIA OFFICE OF TECHNOLOGY

BID FOR GOVERNANCE, RISK, AND COMPLIANCE AUTOMATION PLATFORM

CRFQ 0231 OOT2700000002

RESPONSE DATE: 08/11/2026

SUBMITTED TO:
DEPARTMENT OF ADMINISTRATION,
PURCHASING DIVISION
TOBY.L.WELCH@WV.GOV

SUBMITTED BY:

FRC

1401 STATE STREET, STE 201
ERIE, PA 16501
PHONE: 814-636-8020
FAX: 301-990-1378

DUNS: 102932709
CAGE: 1QBT0
UEI: FZK7KZZJYNQ9

FRC POINT OF CONTACT:

CHRIS ZEIDERS

VICE PRESIDENT –
TECHNOLOGY AND INNOVATION
(703)-795-3257
CZEIDERS@FEDRESOURCES.COM

This response includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this response. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in all sheets.

TABLE OF CONTENTS

Introduction.....	2
Pricing Summary.....	2
TrustCloud Enterprise Edition – Large Platform.....	3
Additional Child Organizational Segments	3
TrustLens Third-Party Risk Assessments – Advanced Module.....	3
Additional Child Organizational Segments	4
TrustOps Compliance Assurance.....	5
Managed Services	5
Professional Services – Implementation	6
Overall Pricing Structure and Value.....	7
Pricing Assumptions and Clarifications.....	7

INTRODUCTION

FRC is pleased to submit this proposal in response to **CRFQ # 0231 OOT2700000002, External Governance, Risk, and Compliance Automation Platform**. This document accompanies our technical response to further elaborate on the pricing information provided via the WVoasis portal.

PRICING SUMMARY

Line Item	Total Price to WVOT
GRC Software Maintenance and Support Year One (Initial Term)	\$272,436.00
GRC Software Maintenance and Support Year 2 Renewal	\$224,716.00
GRC Software Maintenance and Support Year 3 Renewal	\$224,716.00
GRC Software Maintenance and Support Year 4 Renewal	\$224,716.00

The first year cost includes the recurring subscription and managed-services components plus the one-time implementation effort. The recurring annual cost excludes the one-time implementation fee. The Enterprise Edition TrustCloud Platform is being provided to WVOT at a nominal discounted cost of \$1.00.

Each component of the total solution is detailed in the table below.

Solution Component	List Price	Price to WVOT Year 1	Price to WVOT Years 2-4
TrustCloud Enterprise Edition Large Platform	\$180,000.00	\$1.00	\$1.00
TrustLens Third-Party Risk Assessments Advanced Module (Includes 50 annual vendor assessments and 125 agency assessments)	\$280,000.00	\$99,000.00	\$99,000.00
TrustOps Compliance Assurance (Includes a Compliance Pack of 10 Frameworks)	\$70,000.00	\$50,715.00	\$50,715.00
Managed Services (Annual Recurring)	\$83,842.50	\$75,000.00	\$75,000.00
Professional Services – Implementation (One-time)	\$52,000.00	\$47,720.00	--
TOTAL	\$665,842.50	\$272,436.00	\$224,716.00

Descriptions of each of the Solution components follows.

TRUSTCLOUD ENTERPRISE EDITION – LARGE PLATFORM

The Enterprise Edition provides the foundational TrustCloud software-as-a-service platform for one year. It includes the TrustCloud Common Control Framework, policy module and policy templates, Enterprise SSO using SAML, hybrid data fabric and data connectors, email notification engine, documentation center and training content, unlimited TrustCloud users, up to 125 organizational segments, Enterprise Edition support and uptime SLA, and executive dashboarding and audit exporting.

This enterprise foundation is designed to support a broad, multi-entity governance model. The inclusion of unlimited users and up to 125 organizational segments allows West Virginia to establish a common platform while maintaining appropriate separation and reporting across participating agencies, organizations, or other operating units. The hybrid data fabric and connectors provide the technical foundation for integrating source systems and automating evidence collection, while the dashboards and audit-export capabilities provide visibility for operational, executive, and audit stakeholders.

Entitlements include:

- TrustCloud Common Control Framework
- TrustCloud Policy Module and Policy Templates
- TrustCloud Enterprise SSO (SAML)
- TrustCloud Hybrid Data Fabric and Data Connectors
- TrustCloud Email Notification Engine
- TrustCloud Documentation Center and Training Content
- Unlimited users using TrustCloud
- One Parent organizational segment and up to 125 Child organizational segments
- Enterprise Edition support and uptime SLA
- Executive Dashboarding & Audit Exporting

Additional Child Organizational Segments

Additional child organizational segments beyond 125 are available for ad-hoc purchasing and will be prorated to co-term with the annual license fees. These are provisioned under the TrustLens component in the following section.

TRUSTLENS THIRD-PARTY RISK ASSESSMENTS – ADVANCED MODULE

TrustLens adds third-party/vendor risk management capabilities to the platform. The quoted annual subscription supports maintaining a third-party/vendor registry and conducting third-party risk assessments. Included capabilities consist of up to 50 vendor assessments, a third-party vendor registry, API capabilities to support integration with procurement tools and automate third-party ingestion, custom scoring and tiering, integration with external risk-scoring tools, and advanced reporting.

In addition to vendor assessments, the proposed configuration supports annual risk assessments for 125 sub-entities. West Virginia administrators will be able to use a custom questionnaire builder to design, schedule, and distribute custom risk assessments to any activated workspace, including conditional logic, version control, assignment tracking, reminders, and exception handling. Assessments may be built manually or with AI assistance from the control graph. Framework-specific assessment alignment is also included, allowing custom questionnaires to map to controls from a single framework, such as the WVSFS, or another industry-standard framework.

Entitlements and capabilities include: SaaS subscription license to maintain a third-party/vendor registry and conduct third-party risk assessments.

- Up to 50 vendor assessments
- Third-party vendor registry
- API to enable integration with procurement tools to automate third-party ingestion
- Custom scoping and tiering
- Integration with outside-in risk scoring tools
- Advanced reporting

This will cover annual risk assessments for 125 sub-entities including:

- Custom questionnaire builder enabling WVOT administrators to design, schedule, and distribute custom risk assessments to any activated workspace, including conditional logic, version control, assignment tracking, reminders, and exception handling.
- Assessments can be built manually or AI-assisted from the control graph.
- Framework Specific Assessment Alignment: Map custom questionnaires to controls of a single framework like WVCSF or another industry-standard framework.

Additional Child Organizational Segments

Additional child organizational annual risk assessments beyond 125 are available for ad-hoc purchasing and will be prorated to co-term with the annual license fees. These are provisioned under the TrustLens component with the volume discounted pricing as shown below:

Additional Assessments (Additional Child Organizational Segments)	Annual Cost	Effective Per Assessment Cost
1 Additional Assessment	\$960.00	\$960.00
5 Additional Assessments	\$4,320.00	\$864.00
10 Additional Assessments	\$7,776.00	\$777.60
20 Additional Assessments	\$13,997.00	\$699.85

TRUSTOPS COMPLIANCE ASSURANCE

TrustOps provides the compliance-assurance capabilities needed to manage and continuously evaluate compliance against up to 10 selected commercial, NIST, regulatory, or privacy compliance framework families. This module operates within the TrustCloud Enterprise Edition platform.

Framework support includes control and policy mappings aligned to the selected framework; continuous control monitoring for selected compliance frameworks; automated evidence ingestion consistent with the proposed functional requirements; workflow-driven portals for manual evidence gathering; dashboards that visualize adherence levels and compliance gaps; export of an audit-ready package containing controls, policies, and evidence available in the platform; and evidence data retention for up to five years.

This component is intended to reduce reliance on periodic, manually assembled compliance evidence and provide a repeatable mechanism for maintaining framework mappings, evidence, status, and audit artifacts over time.

Entitlements and capabilities include: SaaS subscription license for up to 10 compliance frameworks belonging to commercial, NIST, or Regulatory / Privacy compliance framework families (excludes FedRAMP) - using the TrustOps module of the TrustCloud Platform (Enterprise Edition).

Framework Support Includes:

- Control and policy mappings aligned to the selected framework
- Continuous control monitoring (ConMon) of controls in the selected compliance frameworks
- Automated Evidence Ingestion as per details outlined in TrustCloud/FRC's response to functional requirements checklist.
- Clean, workflow-driven portals for manual evidence gathering, as per TrustCloud/FRC's response to functional requirements checklist.
- Dashboard that visualizes level of adherence to the framework and gaps
- Ability to export an audit-ready package with controls, policies, and evidence available in the platform
- Evidence Data retention for up to 5-years

MANAGED SERVICES

The annual managed-services component provides continuing technical and operational support after implementation. Services include design and onboarding of the risk-assessment template, development of evaluation criteria for risk assessments, export of assessment data from the TrustCloud platform, launch of assessments to all in-scope agencies as required, technical account management services with weekly calls and ongoing project management, and solution-architecture support to map West Virginia requirements to TrustCloud functionality.

This recurring service is intended to supplement the software subscription with hands-on expertise so that the configured solution remains aligned to program needs, assessment activities are successfully executed, and technical questions or configuration needs can be addressed throughout the year.

Entitlements include:

- Design and onboarding of Risk Assessment template
- Development of evaluation criteria for Risk Assessment
- Export of assessment data from TrustCloud Platform
- Launching assessments to all in-scope Agencies as required
- Technical Account Management Services - Weekly calls and ongoing Project Management
- Solution Architecture - Mapping requirements to TrustCloud product

PROFESSIONAL SERVICES – IMPLEMENTATION

The one-time implementation services establish and configure the solution for production use. The implementation scope includes project management, kickoff, and project planning through go-live; WVoT hub and 125-tenant setup with per-workspace isolation; Entra ID single sign-on and role-based access control configuration; WVSFS/NIST framework and control mapping; migration of existing risk/control registers and evidence; dashboard configuration; administrator and end-user training; train-the-trainer activities; user acceptance testing; cutover; and post-go-live hypercare.

These services provide the initial configuration, integration, migration, validation, and enablement work necessary to transition from contract award to an operational TrustCloud environment. The implementation approach also establishes the tenant structure, access model, framework mappings, and migrated data foundation that the recurring platform and managed services will support thereafter.

Entitlements include:

- Project management, kickoff, and project plan through go-live
- WVoT hub and 125-tenant setup with per-workspace isolation
- Entra ID SSO and RBAC configuration
- WVCSE/NIST framework, control mapping
- Migration of existing risk/control registers and evidence
- Dashboards, admin/end-user training, and train-the-trainer
- UAT, cutover, and post-go-live hypercare

OVERALL PRICING STRUCTURE AND VALUE

The proposed pricing intentionally separates one-time implementation activities from recurring software and managed services. This structure provides transparency into the initial cost to establish the environment and the annual cost to operate and support it thereafter.

The proposed package provides a single integrated environment for enterprise GRC, compliance assurance, agency risk assessments, third-party risk management, evidence management, reporting, and ongoing technical support. The Enterprise Edition establishes the common platform; TrustLens extends the platform to third-party and agency assessment workflows; TrustOps provides compliance framework and continuous-assurance capabilities; managed services support ongoing operation; and professional services establish the configured production environment.

PRICING ASSUMPTIONS AND CLARIFICATIONS

- All subscription and managed-service pricing shown above is based on a one-year term.
- Professional Services – Implementation is a one-time fee and is not included in the recurring annual cost.
- The pricing narrative reflects the quantities and scope shown in the provided pricing schedule, including one unit of each quoted entitlement.
- The TrustLens entitlement includes up to 50 vendor assessments and annual risk assessments for 125 child segments as described in the pricing schedule. Additional child segments are priced with volume discounting on an ad-hoc basis and prorated to co-term with the annual license.
- The TrustOps entitlement includes support for up to 10 selected compliance framework families.
- Any scope, integrations, assessments, frameworks, services, or quantities beyond those expressly included in the quoted entitlements may require additional pricing after a scoping discussion.