



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 7

List View

General Information

Contact

Default Values

Discount

Document Information

Procurement Folder: 722642

SO Doc Code: CRFQ

Procurement Type: Central Master Agreement

SO Dept: 0231

Vendor ID: VC0000073567

SO Doc ID: OOT2000000003

Legal Name: RELATIONAL SECURITY CORPORATION

Published Date: 6/2/20

Alias/DBA:

Close Date: 6/17/20

Total Bid: \$706,094.25

Close Time: 13:30

Response Date: 06/16/2020

Status: Closed

Response Time: 19:08

Solicitation Description: Addendum No. 03-GRC Software Solution (OT20131)

Total of Header Attachments: 7

Total of All Attachments: 7



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

**State of West Virginia
 Solicitation Response**

Proc Folder : 722642

Solicitation Description : Addendum No. 03-GRC Software Solution (OT20131)

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2020-06-17 13:30:00	SR 0231 ESR06162000000007661	1

VENDOR

VC0000073567

RELATIONAL SECURITY CORPORATION

Solicitation Number: CRFQ 0231 OOT2000000003

Total Bid : \$706,094.25

Response Date: 2020-06-16

Response Time: 19:08:29

Comments:

FOR INFORMATION CONTACT THE BUYER

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

Signature on File

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				\$706,094.25

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description : See attached Pricing Page

Comments: Detailed Pricing Page is attached in Step 3.

ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO.: CRFQ 0231 COT2000000003

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)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input checked="" type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> 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.

Relational Security Corporation

Company

dibla galvanize

Denise Custaney

Authorized Signature

06/16/2020

Date

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

Revised 6/8/2012

Galvanize Master Subscription Agreement

This Galvanize Master Subscription Agreement (the "**MSA**") is made between each customer who acquires and uses Galvanize products and services ("**Customer**") and ACL Services Ltd. dba Galvanize of 1500, 980 Howe Street, Vancouver, British Columbia, Canada, V6Z 0C8 or, where stated on the Order Form, Relational Security Corporation dba Galvanize of One Harmon Plaza, Suite 700, Secaucus, NJ 07094 ("**Galvanize**").

This MSA is entered into by Galvanize and Customer as of the date Customer purchases, or otherwise accesses or uses, Galvanize products and services. This MSA may be updated from time to time. Updates will not apply until Customer renews its subscription.

1. Scope

1.1 Agreement. The provision and use of Products and Services is subject to and governed by the terms of this MSA and the applicable Order Form (together, the "**Agreement**"). This MSA includes and incorporates the following attached schedules, as applicable:

Schedule "A" – Service Level Agreement
Schedule "B" – Security Schedule
Schedule "C" – Data Processing Addendum

1.2 Disclaimer – Trial, Evaluation, Beta, Academic Use. THE WARRANTIES, INDEMNITIES AND REMEDIES PROVIDED BY GALVANIZE UNDER THIS MSA DO NOT APPLY TO PRODUCTS PROVIDED FOR TRIAL, EVALUATION, BETA TESTING, DEMO OR EDUCATIONAL USE (I.E. THROUGH THE GALVANIZE ACADEMIC NETWORK PROGRAM OR A TEXTBOOK PUBLISHER). SUCH PRODUCTS ARE PROVIDED "AS IS" WITHOUT WARRANTY AND ARE USED AT CUSTOMER'S OWN RISK. GALVANIZE DOES NOT WARRANT THE PERFORMANCE OR SECURITY OF SUCH PRODUCTS.

2. Definitions

2.1 "Affiliate" means an entity which controls, is controlled by, or is under common control with a party, where "control" means more than 50% ownership interest in such entity, or the power to direct the management of such entity, whether through the ownership of voting securities, by contract, or otherwise.

2.2 "Cloud Products" means the Galvanize cloud-based Software-as-a-Service (SaaS) offerings.

2.3 "Customer Data" means any data, information or other material which Customer and its Named Users upload, enter, create and store in the Cloud Products.

2.4 "Customer Systems" means Customer's own systems, infrastructure and personnel used to access and operate the Products, including, but not limited to, Customer's servers, hardware, devices, data systems, internet connectivity, electric power, operating software and software applications (other than the Products).

2.5 "Named User" means a specific individual authorized by Customer to access and use the Products on behalf of Customer, and for whom Customer has paid the applicable subscription fees. Named Users may include employees and individual contractors or consultants of Customer, its Affiliates or their third-party service providers.

2.6 "Order Form" means the ordering document or invoice issued to Customer by Galvanize, its Affiliates or one of their authorized resellers for purchase of Product subscriptions and Services, or such other ordering document agreed and accepted by both parties. "Order Form" includes any statement of work signed by both parties.

2.7 "Products" means the Cloud Products and Software listed in an Order Form, including their applicable User Documentation.

2.8 "Resources" means the self-serve online user resources that Galvanize makes available from time to time for Product assistance, education and self-learning, such as online training, tools & templates and a peer community forum.

2.9 "Services" means consulting and training services purchased by Customer under an Order Form, which may be further detailed in a statement of work signed by both Customer and Galvanize.

2.10 "Software" means the Galvanize downloadable on-premise software.

2.11 "Third Party Content" means third party regulations, standards, guidelines, frameworks and industry practices related to governance, risk management and compliance (such as COSO, COBIT, PCI-DSS, OMB A-133 and NIST SP 800-53) which Galvanize has obtained from publicly available sources or licensed from third party content providers.

2.12 "User Documentation" means the user and technical help documentation for the Products which is made available through a secure area of the Galvanize website.

3. Purchase Terms

3.1 Purchase. Customer may purchase Product subscriptions and Services by entering into an Order Form. The following terms will be addressed in the Order Form and not in this MSA: (a) the type and quantity of Product subscriptions and Services being purchased; (b) the subscription term; (c) pricing and applicable fees; and (d) payment terms.

3.2 Taxes. Unless otherwise specified in the Order Form, fees do not include applicable taxes. Customer will pay all applicable sales, use, withholding and excise taxes, and any other assessments in the nature of taxes, duties or charges resulting from this Agreement (excluding Galvanize's income and franchise taxes). Applicable

taxes will be charged to and payable by Customer based on the shipping address specified in the Order Form. If Customer is a tax-exempt institution or entity, and provides Galvanize with a tax exemption certificate, Galvanize will not charge the tax from which Customer is exempt.

- 3.3 **Late Payment.** If any fees remain unpaid more than thirty (30) days past their due date, Galvanize may, without limiting its other rights and remedies, suspend Customer's access to the related Products or Services until such amounts are paid in full. Galvanize will provide at least seven (7) days prior notice that fees are overdue before any such suspension. Galvanize will not exercise its suspension right if Customer is disputing the applicable fees reasonably and in good faith, and is cooperating diligently to resolve the dispute. Unless otherwise specified in the Order Form, interest at a rate of 1.5% per month (18 percent per annum), or at an interest rate equal to the maximum rate permitted by the applicable law, whichever is less, may be charged on overdue amounts.
- 3.4 **Expenses.** Unless otherwise specified in the Order Form, Customer will pay any reasonable out-of-pocket expenses incurred by Galvanize to provide Services (e.g. hotel, travel and meals). Such expenses will be invoiced at actual cost in accordance with Customer's reasonable travel and expense policy, or as otherwise agreed by the parties. If Customer reschedules or cancels any Services for which Galvanize has incurred non-refundable out-of-pocket expenses, Customer will reimburse Galvanize for such non-refundable expenses
- 3.5 **Refunds or Payment on Termination.** If Customer terminates this Agreement pursuant to Section 11.2 (Termination for Cause) or Section 14.2 (Warranty Remedies), Galvanize will refund any prepaid fees for the remaining unused portion of the subscription term and any fees pre-paid for Services not actually performed. If Galvanize terminates this Agreement pursuant to Section 11.2 (Termination for Cause), Customer will remain liable for any unpaid fees for the remaining portion of the current subscription term.

4. Products

- 4.1 **Rights Granted.** Subject to the terms and conditions of this Agreement, Galvanize will make the Products available to Customer's Named Users for the subscription type(s), quantity and subscription term purchased by Customer as set out in an Order Form. Galvanize grants Customer a non-exclusive, non-transferable right and license to access, use and, where applicable, download the Products and Resources during such subscription term for Customer's internal business purposes. Products are accessed and delivered electronically through a secure area of the Galvanize website, and are deemed delivered when they are made available for access or download by Customer, as applicable.
- 4.2 **Service Levels.** Galvanize will make the Cloud Products available in accordance with the service levels set out in the Service Level Agreement attached as Schedule "A". Customer is responsible for providing and maintaining the Customer Systems. Galvanize will not be liable for

any failures arising from or relating to the Customer Systems.

- 4.3 **Customer Support.** During the Product subscription term, Customer will have access to the Galvanize support center, at no additional charge, to assist Customer with its use of the Products. Support center services are available via chat, email, telephone and the Galvanize community and are provided in accordance with the current support center policies posted at: www.wegalvanize.com/support-center/, or such other url as Galvanize may use for this purpose. Customer will also have access to new releases and upgrades of the Products when they become commercially available.
- 4.4 **Non-Production.** Products provided for non-production use, such as staging, testing, disaster recovery or failover, may only be used in a non-production environment and only for such non-production purposes.

5. Use of Products

- 5.1 **Named Users.** The Products may be accessed and used by up to the maximum number of Named Users included in Customer's subscription. Customer will not make the Products or Resources available to anyone other than its Named Users. Sharing or pooling a Named User's access among multiple individuals to allow for temporary use by multiple users is strictly prohibited. Customer may, however, permanently replace a Named User with another individual as long as the number of Named Users does not exceed the number of Named Users purchased. If Customer exceeds, or wishes to increase, the number of Named Users using a Product, additional fees will apply.
- 5.2 **Accounts.** Customer will provide accurate, current and complete information when activating its Product subscription and Named User accounts. Customer will keep all Named User ID's, passwords and other account information confidential and will follow best practices for maintaining the security of its passwords and account credentials. Customer is responsible for all activities that occur under its accounts and for the acts or omissions of its Named Users.
- 5.3 **Acceptable Use Policy.** Customer will, and will cause its Named Users to, use the Products and Resources solely as contemplated by this Agreement and the applicable User Documentation, and abide by any posted guidelines or policies related to acceptable use and conduct when accessing or using Resources or the customer support center. Customer will not, and will not permit or assist anyone else to: (a) use the Products or Resources to send spam or otherwise duplicative or unsolicited messages in violation of applicable laws; (b) knowingly send or store infringing, threatening, libelous or otherwise unlawful or tortious material, including material which violates any individual's privacy rights; (c) post or transmit any file which contains viruses, worms, Trojan horses or any other contaminating or destructive features, or otherwise interfere with or disrupt the integrity or performance of the Products or the data contained in the Products; (d) attempt to gain unauthorized access to the Products, Resources or related systems or networks, or circumvent or remove any security or use protection mechanisms; (e) frame or

mirror any part of the Products or Resources on any server or wireless or internet-based device, other than on Customer's own intranets or otherwise for its own internal business purposes or as permitted in the User Documentation; or (f) conduct any tests or analysis on the security or performance of the Products or Resources, including any benchmark tests, without Galvanize's prior written consent, or publicly disclose the results of any such tests or analysis.

- 5.4 Suspension. Galvanize may, without limiting any other rights or remedies available to it, suspend Customer's use of the Products or Resources (as applicable), or take other appropriate remedial action, to address any violation or suspected violation of this Section 5.

6. Third Party Content

- 6.1 Available. Galvanize may, from time to time, make certain Third Party Content available to Customer through the Products. Third Party Content may be offered with or without charge as specified in the Order Form. Galvanize warrants that it has the rights necessary to provide Third Party Content to Customer in accordance with, and subject to, the terms of this Section 6 (Third Party Content).

- 6.2 Right to Use. Customer may access and use Third Party Content on the condition that: (a) Customer uses the Third Party Content solely in conjunction with the Products, and does not copy, publish or distribute any Third Party Content separate from Customer's use of the Products; (b) Customer does not license or sell Third Party Content and does not remove or alter any copyright, trademark or other proprietary notice appearing on or within the Third Party Content; (c) PCI-DSS materials are used in accordance with the current PCI Security Standards Council, LLC License Agreement made available through the PCI SSC website at www.pcisecuritystandards.org and also through the Products prior to download of such materials; and (d) the owners of the Third Party Content are third party beneficiaries of this Agreement as it pertains to their proprietary rights.

- 6.3 Third Party Content Disclaimer. THIRD PARTY CONTENT IS FOR EDUCATIONAL AND INFORMATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE LEGAL, ACCOUNTING OR OTHER PROFESSIONAL ADVICE. THIRD PARTY CONTENT SHOULD NOT BE DEEMED TO SET FORTH ALL APPROPRIATE PROCEDURES, TESTS OR CONTROLS OR TO SUGGEST THAT OTHER PROCEDURES, TESTS OR CONTROLS THAT ARE NOT INCLUDED MAY NOT BE APPROPRIATE. GALVANIZE DOES NOT CLAIM THAT USE OF THIRD PARTY CONTENT WILL ASSURE A SUCCESSFUL OUTCOME. CUSTOMER AND ITS NAMED USERS ARE RESPONSIBLE FOR APPLYING PROFESSIONAL JUDGEMENT TO THE SPECIFIC CIRCUMSTANCES PRESENTED TO DETERMINE THE APPROPRIATE PROCEDURES, TESTS OR CONTROLS. USE OF THIRD PARTY CONTENT AND RELATED MATERIALS ARE AT CUSTOMER'S OWN RISK AND, BY SO USING THEM, CUSTOMER RELEASES GALVANIZE AND ITS LICENSORS FROM ANY AND ALL

LIABILITY THAT MAY ARISE IN CONNECTION WITH SUCH USE.

7. Services

- 7.1 Services. Galvanize will provide Customer with the Services set forth in an Order Form and in any statement of work signed by the parties. If Customer has purchased an annual allotment of hours of Services, such hours may be used and drawn down on a time and materials basis throughout Customer's annual subscription term for the Products. Each annual allotment of hours is non-transferable and will expire at the end of each annual subscription term if not used. Unused hours will not carry over to the following subscription term. If Customer cancels its subscription to the applicable Products, all remaining hours will be forfeited at the time of cancellation.

- 7.2 Customer Policies. If Services are to be performed by Galvanize personnel on Customer's premises or require access to Customer Systems, Galvanize will adhere to Customer's applicable information security and safety policies of which Galvanize has been informed in writing, including, where appropriate, applicable background checks of Galvanize personnel. Customer will not impose any background check or other security requirement that would violate, or may cause Galvanize to violate, applicable laws in the jurisdiction where Galvanize and its personnel are located.

- 7.3 Services Deliverables. Subject to Section 12.1 (Ownership), and unless otherwise provided in the applicable statement of work, Customer owns all right, title and interest in and to any reports, documents or other materials created by Galvanize specifically for Customer as part of the Services and provided as a deliverable of the Services under the applicable statement of work (the "**Deliverables**"). To the extent a Deliverable includes any Galvanize Property (as defined in Section 12.1), upon payment of the fees for the applicable Deliverable, Galvanize grants Customer, during Customer's subscription term for the Products, a non-exclusive, worldwide, royalty-free license to use such Galvanize Property in conjunction with the applicable Deliverable, and to modify such Galvanize Property for Customer's internal business purposes. Unless otherwise specified in the applicable statement of work, Galvanize is not required to maintain, support or otherwise repair any Deliverable or Galvanize Property after its delivery to Customer.

- 7.4 Independent Contractor. Galvanize will perform the Services as an independent contractor and will not act, hold itself out as, or be an agent of Customer. Galvanize personnel are not, and will not be construed as, Customer's employees and will not be entitled to any benefits offered by Customer to its employees. Galvanize is responsible for complying with applicable laws, rules and regulations relating to its employees and personnel including, but not limited to, those related to immigration, taxation and workers' compensation.

8. Customer Data

- 8.1 Ownership of Customer Data. Customer owns all right, title and interest in and to all Customer Data and Customer Systems. Customer grants Galvanize a non-exclusive, limited license to use Customer Data solely as necessary to perform Galvanize's obligations under and in accordance with this Agreement. Customer warrants that it has all rights necessary to grant such license and that its collection and use of Customer Data complies with applicable laws.
- 8.2 Control and Access. Customer determines what Customer Data it uses and retains full control over the access to and use of its Customer Data. Galvanize will not access Customer Data, except as instructed or authorized by Customer, where necessary to prevent or address service or technical problems affecting Customer, or if required by law, regulation or court order. Galvanize is not responsible or liable for the deletion, damage, loss, corruption of or unauthorized access to any Customer Data, except to the extent caused by Galvanize's failure to meet its obligations under this Agreement.
- 8.3 Personal Data. To the extent Customer Data includes personal data, or Galvanize otherwise stores or processes personal data on behalf of Customer (including, but not limited to, personal data governed by the EU General Data Protection Regulation or the California Consumer Privacy Act of 2018), the terms of the Data Processing Addendum attached as Schedule "C" will apply.

9. Security

- 9.1 Security Safeguards. Galvanize will implement and maintain the security safeguards set forth in the Security Schedule attached as Schedule "B". Customer is responsible for assessing the suitability of such safeguards for the type of Customer Data it uses. Galvanize will cooperate with Customer to provide the information reasonably necessary for Customer to assess the security of the Cloud Products, including completion of Customer security assessments and providing Customer with a copy of Galvanize's current SOC 2 report in accordance with Schedule "B".
- 9.2 Customer Obligations. Customer is responsible for the security of its Customer Systems and for the end-user security and access controls for its Cloud Product environment. Customer will take reasonable security precautions in connection with its use of the Cloud Products as set forth in Schedule "B". Customer will notify Galvanize immediately if it becomes aware of any unauthorized use of its subscription accounts or any user ID and password, or if Customer becomes aware of any other known or suspected breach of security related to its use of the Cloud Products.
- 9.3 Security Breach. Galvanize will notify Customer without undue delay if Galvanize determines that the security of the Cloud Products has been breached resulting in Customer Data being accessed by or disclosed to an individual or entity who is not authorized to access or receive such information (a "**Security Breach**").

Galvanize will follow the Security Breach procedures set forth in Schedule "B". Galvanize's notification of or response to a Security Breach will not be construed as an acknowledgement by Galvanize of any fault or liability.

- 9.4 Remedy for Security Breach. If a Security Breach is caused by Galvanize's failure to meet its security obligations under this Agreement, Galvanize will, upon Customer's written request, reimburse Customer for reasonable and documented costs incurred by Customer to meet its legal or regulatory obligations to notify affected individuals, government authorities or regulatory agencies, and to provide credit and identity theft monitoring services for affected individuals. If a Security Breach is caused by Customer Systems or by Customer's failure to meet its security obligations under this Agreement, Customer will, upon Galvanize's written request, reimburse Galvanize for reasonable and documented costs incurred by Galvanize in reporting, investigating and remediating the Security Breach. Neither party will have any obligation under this Section 9.4 to the extent the Security Breach was caused by the other party or was caused by a third party who was not authorized by or acting on behalf of a party to this Agreement.

10. Renewal and Cancellation

- 10.1 Renewal. At least ninety (90) days prior to expiration of each Product subscription, Galvanize will provide Customer with advance written notice of Customer's upcoming subscription renewal. Customer may renew its subscription prior to expiration by: (a) executing a renewal Order Form; (b) issuing a purchase order for the renewal; or (c) requesting or confirming renewal through the Product's online renewal process. If none of these has occurred at least thirty (30) days prior to expiration of the current subscription term, and Customer has not cancelled its subscription as provided in Section 10.2 (Cancellation), Customer will be deemed to have renewed its subscription on the terms set forth in the notice of renewal.
- 10.2 Cancellation. Customer may cancel a Product subscription by providing Galvanize with notice of cancellation at least thirty (30) days prior to expiration of the current subscription term. Galvanize may cancel a Product subscription by providing Customer with notice of cancellation at least ninety (90) days prior to expiration of the current subscription term. A Product subscription which has been cancelled will expire and terminate at the end of its current subscription term and will not be renewed.

11. Termination

- 11.1 Termination for Convenience. Customer may terminate this Agreement at any time for convenience by providing written notice to Galvanize. Upon termination for convenience, Customer will not be entitled to a refund of fees, or relieved of future payment obligations, for the unused portion of the remaining subscription term.
- 11.2 Termination for Cause. Either party may terminate this Agreement for cause if the other party: (a) is in material

breach of this Agreement (including, a failure to pay fees when due) and does not remedy such breach within thirty (30) days after receiving written notice of the breach from the non-breaching party; or (b) becomes insolvent or bankrupt, becomes the subject of any proceedings under bankruptcy, insolvency or debtors' relief law, has a receiver, manager or receiver-manager appointed, makes an assignment for the benefit of its creditors or takes the benefit of any applicable law or statute in force for the winding up or liquidation of corporations.

11.3 Effect of Expiration or Termination. Subject to Section 11.4 (Data Retention Policy), upon expiration or termination of this Agreement, or any Product or Services subscription, Customer's access to and use of such Products or Services will be terminated. Each party will immediately return to the other party all Confidential Information of the other party in its possession or control. If the Product includes Software, Customer will destroy the original and all copies of such Software in its possession or control, and will certify in writing that this has been done within thirty (30) days of a written request from Galvanize.

11.4 Data Retention Policy. Customer is responsible for determining its own data retention controls for Customer Data and for deleting its Customer Data from the Cloud Products. Customer will have a period of thirty (30) days following expiration or termination of Customer's subscription to remove or delete its Customer Data. Upon Customer's written request, Galvanize will assist Customer with the deletion of its Customer Data and may extend the period for removing and deleting Customer Data.

11.5 Survival. The termination of this Agreement will not constitute a waiver of any fees or amounts due by Customer, nor will termination in any way reduce or compromise any other rights of either party pursuant to this Agreement. All terms that by their nature should survive termination of this Agreement will survive.

12. Intellectual Property Rights

12.1 Ownership. Galvanize and its licensors own their respective rights, title and interests in and to: (a) the Products, Resources, Third Party Content, Services and all related materials and technology used to provide them; (b) all scripts, analytics, compliance maps, frameworks, configurations, enhancements and derivative works of the Products which are developed by Galvanize either separate from or as part of the Services (collectively, the "**Galvanize Property**"); and (c) all methodologies, concepts, know-how, and intellectual property and proprietary rights related to any of the foregoing. Except for the limited rights expressly granted to Customer in this Agreement, Galvanize and its licensors reserve all of their right, title and interest in and to the above.

12.2 IP Restrictions. Except as expressly permitted in this Agreement, Customer will not: (a) modify, adapt or translate any Products or Resources; (b) create derivative works from the Products, Resources or Galvanize Property; (c) sell, lease, rent, assign, sub-

license or distribute any Products, Resources or Galvanize Property to any third party; (d) except as permitted by applicable law, de-compile, reverse engineer or disassemble any Products, Resources or Galvanize Property, or otherwise reduce any object code to source code; (e) use or include any Products, Resources or Galvanize Property in any service bureau or fee generating service offered to third parties; or (f) use any Products, Resources or Galvanize Property to create works which are competitive to the Products or which use similar features, functions or graphics.

12.3 Feedback. Customer grants Galvanize and its Affiliates a non-exclusive, royalty-free, worldwide, perpetual and irrevocable right and license to use, and exercise the intellectual property rights in, Customer's suggestions or feedback regarding the Products and Resources, including incorporating such suggestions or feedback into any Products, Resources or Galvanize Property.

13. Confidentiality

13.1 Confidential Information. For the purposes of this Agreement, "**Confidential Information**" means any oral, written or electronic information, documents, materials or data provided or disclosed by a party to the other party which is proprietary in nature and is not readily available to the public. Confidential Information includes, without limitation: (a) the Products; (b) Customer Data; (c) the terms and pricing of Customer's subscription; (d) a party's financial information, product plans, product roadmaps, business methods and trade secrets; (e) non-public information regarding a party's customers or employees; and (f) information which, given its nature or the circumstances surrounding its disclosure, the receiving party reasonably knows or ought to know is confidential.

13.2 Exclusions. Confidential Information does not include information that: (a) is or becomes a part of the public domain through no act or omission of the receiving party; (b) was in the receiving party's lawful possession prior to the disclosure and had not been obtained by the receiving party either directly or indirectly from the disclosing party; (c) was lawfully disclosed to the receiving party by a third party without restriction on disclosure; or (d) is independently developed by the receiving party without the use or benefit of the disclosing party's Confidential Information.

13.3 Obligations. The receiving party agrees to keep the disclosing party's Confidential Information in confidence and to use such Confidential Information solely for the purposes of exercising its rights and fulfilling its obligations under this Agreement. Subject to Section 13.4 (Compelled Disclosure), the receiving party will not disclose the disclosing party's Confidential Information to any third party, except to those of its and its Affiliates' employees, contractors, service providers, advisors, attorneys and auditors who need to know and who have agreed in writing to maintain the confidentiality of such Confidential Information. Customer Confidential Information which is stored in the Cloud Products will be governed by the terms of Section 8 (Customer Data) and Section 9 (Security) instead of this Section 13.3 (Obligations).

13.4 Compelled Disclosure. If the receiving party is requested or required by applicable law or legal process to disclose any of the disclosing party's Confidential Information, the receiving party will provide the disclosing party with prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the disclosing party's cost, if the disclosing party wishes to contest the disclosure. Any such disclosure will be limited to only what is required and will be subject to confidentiality protections to the extent reasonably practicable. Any disclosure of Confidential Information that is required by applicable law or legal process will not be a breach of this Agreement.

14. Warranty

14.1 Warranties. Subject to Section 14.3 (Exclusions), Galvanize warrants that during the subscription term: (a) the User Documentation will accurately describe the applicable functionality of the Products; (b) the Products will perform substantially in compliance with their applicable User Documentation when Customer administers, accesses and uses the Products in accordance with such User Documentation; (c) Galvanize will not materially decrease the overall security or functionality of the Products; and (d) the Services will be provided in a professional and workmanlike manner by personnel with sufficient skill, knowledge and experience to perform the Services.

14.2 Warranty Remedies. If any Product or Services fail to comply with the above warranties, and Customer notifies Galvanize in writing during the subscription term of the nature of such non-compliance, Galvanize will make commercially reasonable efforts to promptly remedy such non-compliance without charge. If Galvanize does not remedy the non-compliance within a reasonable period agreed by the parties, Customer may terminate its subscription to the related Product or Services and receive a refund in accordance with Section 3.5 (Refunds or Payment on Termination). The foregoing remedy provides the sole and exclusive remedy for breach of warranty.

14.3 Exclusions. Galvanize does not warrant or promise that the Products, User Documentation, Resources or any Services will be uninterrupted, error-free or will meet Customer's specific needs or requirements. Galvanize does not warrant the performance or security of the Internet. Galvanize is not responsible or liable for any issues or losses related to risks inherent in Internet connectivity (such as hackers, phishing and malware), except to the extent such issues or losses result from Galvanize's breach of its security obligations under this Agreement.

14.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES STATED IN THIS AGREEMENT, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, ORAL, WRITTEN OR OTHERWISE. EACH PARTY SPECIFICALLY DISCLAIMS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT (BUT NOT IN DEROGATION OF ITS INDEMNITY

OBLIGATIONS UNDER SECTION 15 (INDEMNITY)). Some jurisdictions do not allow the exclusion of implied warranties, in which case any implied warranties are limited to a ninety (90) day period commencing on the date Customer activates its Product subscription.

15. Indemnity

15.1 Galvanize Indemnity. Galvanize will defend, at its cost, any claim made against Customer by a third party which asserts that Customer's use of a Product, Service or Deliverable in accordance with this Agreement infringes such third party's intellectual property rights. Galvanize will indemnify Customer from actual damages and costs (including reasonable legal fees) finally awarded against Customer in respect of such claim, or settlement amount agreed to be paid in settlement of such claim.

15.2 Remedy for Infringement Claims. Upon notice of an infringement claim, or if in Galvanize's opinion such a claim is likely, in addition to its obligations under Section 15.1, Galvanize has the right, at no cost to Customer, to: (a) procure the right for Customer to continue using the affected Product, Services or Deliverable; (b) replace or modify such Product, Services or Deliverable so that it is non-infringing and provides substantially the same or greater functionality and performance as the affected Product, Services or Deliverable; or (c) if, in Galvanize's opinion, neither option (a) or (b) is commercially reasonable in the circumstances, Galvanize may terminate the affected Product subscription or Services upon thirty (30) days written notice to Customer, and will refund to Customer any prepaid fees for the remaining unused portion of the current subscription term. Sections 15.1 and 15.2 set out Galvanize's entire obligation and liability, and Customer's sole and exclusive remedy, with respect to the infringement of the intellectual property and proprietary rights of others.

15.3 Customer Indemnity. Customer will defend, at its cost, any claim made against Galvanize by a third party: (a) which asserts that Customer's collection and use of Customer Data infringes such third party's rights or otherwise violates applicable law or regulation; or (b) which results from Customer's breach of Section 5.3 (Acceptable Use Policy). Customer will indemnify Galvanize from actual damages and costs (including reasonable legal fees) finally awarded against Galvanize in respect of any such claim, or settlement amount agreed to be paid in settlement of any such claims. Customer will have no obligation to defend or indemnify any claim which arises solely from a Product itself or is caused by Galvanize's breach of this Agreement.

15.4 Indemnity Conditions. A party's obligations under Section 15.1 (Galvanize Indemnity) and Section 15.3 (Customer Indemnity) are conditioned on: (a) the indemnitee giving the indemnitor prompt notice of the claim; (b) the indemnitee giving the indemnitor sole control of the defense and all negotiations for its settlement or compromise (provided this does not require an admission of guilt or liability by the indemnitee); and (c) the indemnitee providing the indemnitor with reasonable assistance, at the indemnitor's expense. The indemnitee may, at its own cost, engage counsel of its choice.

15.5 **Exclusions.** Galvanize will have no obligations under this Section 15 (Indemnity) in respect of any infringement claim that does not state with specificity that a Product, Service or Deliverable is the cause of the infringement, or any infringement claim which arises out of or relates to: (a) use of an outdated version of a Product which is no longer commercially supported by Galvanize; (b) any modification of the Product, Services or Deliverable by Customer or by anyone other than Galvanize; (c) use or combination of the Product or Deliverable with programs, components or products not provided by Galvanize or authorized by Galvanize in the User Documentation; (d) use of a Product, Service or Deliverable in any manner which breaches this Agreement or which is not in accordance with the applicable User Documentation; (e) Customer's use of Customer Data; or (f) any Customer Systems.

16. Mutual Limitation of Liability

16.1 **Limitation of Liability.** SUBJECT TO SECTION 16.3 (EXCLUSIONS), THE AGGREGATE CUMULATIVE LIABILITY OF EACH PARTY, TOGETHER WITH ITS AFFILIATES, ARISING OUT OF OR RELATED TO THIS AGREEMENT WILL BE LIMITED TO 125% OF THE FEES PAYABLE BY CUSTOMER FOR THE PRODUCTS IN THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE LIABILITY. THIS LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT (INCLUDING NEGLIGENCE) AND REGARDLESS OF THE THEORY OF LIABILITY. THIS LIMITATION WILL NOT APPLY TO LIMIT CUSTOMER'S OBLIGATION TO PAY FEES IN ACCORDANCE WITH THIS AGREEMENT.

16.2 **No Liability.** SUBJECT TO SECTION 16.3 (EXCLUSIONS), NEITHER PARTY NOR ANY OF ITS AFFILIATES WILL HAVE ANY LIABILITY FOR ANY OF THE FOLLOWING DAMAGES OR LOSSES (EVEN IF SUCH DAMAGES OR LOSSES WERE FORESEEABLE, KNOWN OR CAUSED BY THE PARTY'S NEGLIGENCE, AND EVEN IF A PARTY'S REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE): (A) LOST PROFITS, LOST REVENUE, BUSINESS INTERRUPTION, LOSS OF GOODWILL, LOSS OF REPUTATION, COSTS OF SUBSTITUTE GOODS; OR (B) ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OR LOSSES (IN CONTRACT, TORT OR OTHERWISE) (BUT NOT IN DEROGATION OF A PARTY'S OBLIGATIONS UNDER SECTION 9.4 (REMEDY FOR SECURITY BREACH)).

16.3 **Exclusions.** The limitations and exclusions of liability in this Section 16 (Mutual Limitation of Liability) will not apply to: (a) a party's indemnification obligations under this Agreement; (b) a violation of Galvanize's intellectual property rights or breach of Section 12.2 (IP Restrictions); or (c) any damages or liabilities that cannot be limited or excluded under applicable law, including, but not limited to, (i) those arising out of a party's gross negligence, willful misconduct, deceit or fraud, or (ii) liability for death or personal injury caused by a party's negligence.

17. Insurance

17.1 **Coverage.** Galvanize will, at its own expense and without limiting its obligations for liability under this Agreement,

obtain and maintain the following insurance coverage during the subscription term: (a) commercial general liability insurance with limits no less than two million dollars (\$2,000,000) per occurrence and two million dollars (\$2,000,000) as an annual aggregate against liability for bodily injury and property damage; (b) employer's liability insurance with limits no less than two million dollars (\$2,000,000); (c) professional liability insurance with limits no less than two million dollars (\$2,000,000) per claim and two million dollars (\$2,000,000) as an annual aggregate; (d) non-owned automobile liability insurance with limits no less than one million dollars (\$1,000,000); (e) cyber and privacy liability insurance with limits no less than two million dollars (\$2,000,000); and (f) workers compensation insurance as required by applicable law. Customer will obtain and maintain, at its own expense, appropriate insurance for its own business operations and for the risks associated with its use of the Products and Services.

17.2 **Evidence.** Galvanize will have the above insurance in full force and effect as of the start date of Customer's subscription. If requested by Customer, Galvanize will provide Customer with a certificate or memorandum of insurance confirming the insurance coverage. The fact that Galvanize carries insurance will not be construed to increase Galvanize's liability under this Agreement.

18. Compliance with Laws

18.1 **Anti-Corruption/Anti-Bribery.** Each party will comply with applicable anti-corruption laws, including, but not limited to, the Canadian Corruption of Foreign Public Officials Act, the United States Foreign Corrupt Practices Act and the UK Bribery Act, 2010, as each may be amended from time to time. Each party agrees that it has not received or been offered any illegal or improper bribe, kickback, payment, gift or item of value from any of the other party's employees or resellers in connection with this Agreement, excluding reasonable gifts and entertainment provided in the ordinary course of business. In no event will either party be obligated under this Agreement to take any action that it believes, in good faith, would cause it to be in violation of any laws, rules, ordinances or regulations applicable to it.

18.2 **Export.** Products provided under this Agreement may be subject to export or import laws in the United States and other countries outside Canada. Customer and Galvanize each represent that it is not named on any U.S. government denied-party list. Customer will not permit access to or use of the Products in a U.S.-embargoed country or region in violation of United States export laws or regulations.

19. Governing Law and Dispute Resolution

19.1 **Governing Law.** This Agreement is governed by and will be construed in accordance with the following laws: (a) the laws of the State of New York if Customer is located in the United States; (b) English laws if Customer is located in the United Kingdom, Europe, the Middle East or Africa; (c) Singapore laws if Customer is located in Asia (other than the Middle East); or (d) the laws of the Province of British Columbia and the applicable federal laws of Canada if Customer is located in any other

country or location. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded.

- 19.2 **Dispute Resolution.** Subject to and without restricting the rights of a party to injunctive relief or other interim measures of relief, the parties will attempt to resolve any controversy or claim relating to this Agreement through consultation and negotiation in good faith. By mutual agreement, the parties may agree to use some form of non-binding alternative dispute resolution, such as mediation. The use of any alternative dispute resolution procedure will not be construed as a waiver or estoppel to affect adversely the rights of either party. Any dispute which the parties cannot resolve between themselves within sixty (60) days after the claim or controversy first arose will be referred to, finally settled and determined by binding arbitration in accordance with Section 19.3 (Arbitration).
- 19.3 **Arbitration.** Arbitration will be conducted in the English language before a single arbitrator who has substantial experience in resolving intellectual property and commercial technology contract disputes. Arbitration will be held and conducted: (i) in New York, NY, USA in accordance with the commercial arbitration rules of the American Arbitration Association if Customer is located in the United States; (ii) in London, England in accordance with the LCIA (London Court of International Arbitration) Rules if Customer is located in the United Kingdom, Europe, the Middle East or Africa; (iii) in Singapore in accordance with SIAC (Singapore International Arbitration Centre) Rules if Customer is located in Asia (other than the Middle East); or (iv) in Vancouver, B.C., Canada in accordance with the International Centre for Dispute Resolution Canada (ICDR) and its International Arbitration Rules or its Canadian Arbitration Rules (as applicable) if Customer is located in Canada or any other country or region.

20. General

- 20.1 **Complete Agreement.** This Agreement is the complete and exclusive statement of the agreement between the parties with respect to its subject matter. This Agreement supersedes and merges all prior representations, proposals, understandings, discussions or other agreements between the parties (whether oral, written, expressed or implied) relating to the matters contained in this Agreement. The terms of any Customer purchase order or other general terms of Customer will not be binding on the parties and will not be construed to modify this Agreement. Any changes to or variations from this Agreement may only be made in a written addendum signed by both parties. If the parties have entered into a written agreement with respect to the Products or Services which is signed by both Customer and Galvanize, such written agreement will take precedence over this Agreement.
- 20.2 **Assignment.** Neither party may assign this Agreement without the other party's prior written consent (not to be unreasonably withheld), except to an Affiliate or in connection with a merger, acquisition, corporate reorganization or sale of all or substantially all of its assets. A permitted assignment will not be effective

unless the assigning party notifies the other party of the assignment and has obtained the assignee's written agreement to be bound by all of the terms of this Agreement. Subject to the foregoing, this Agreement will enure to the benefit of and be binding upon the parties and their respective successors and permitted assigns.

- 20.3 **Notices.** Any notice that either party is required or permitted to give to the other party under this Agreement will be in writing and (except for email notice) will be delivered to Galvanize at its address set out on page 1 of this Agreement (Attention: Legal Department) and to Customer at the address provided on the most recent Order Form. Either party may change their address for notice by providing written notice of the change to the other party. The delivery of notice will be by personal delivery, courier, regular mail or confirmed e-mail, except that e-mail notice will not apply for notices required under Section 13.4 (Compelled Disclosure), Section 15 (Indemnity) or Section 19.2 (Dispute Resolution). Delivery will be deemed effective upon receipt (provided that, for delivery by email, no automated or other response is received indicating non-delivery or the absence of the recipient).
- 20.4 **Waiver and Severability.** The waiver of a breach of any provision of this Agreement will not operate or be interpreted as a waiver of any other breach or any subsequent breach. If any provision of this Agreement is unenforceable, that provision will be construed, limited, modified or, if necessary, severed to the extent necessary to eliminate its unenforceability and the other provisions of this Agreement will remain in full force.
- 20.5 **Verification.** Galvanize may, upon reasonable notice to Customer, and no more than once per year, request information to verify that Customer's use of the Products complies with the terms of this Agreement. If Galvanize reasonably believes that such information does not correctly disclose Customer's Product usage, Galvanize, or a third party appointed by Galvanize, may conduct an audit to verify that Customer's use of the Products complies with this Agreement. If the audit shows that Customer is in violation of this Agreement, Customer will reimburse Galvanize for its reasonable expenses related to the audit and will pay any appropriate additional fees.
- 20.6 **Product Research and Development.** Customer acknowledges that Galvanize may use aggregated and anonymized data regarding use of the Products for Galvanize's internal business purposes, such as research, development and Product improvement. Such information will not include Customer Data and the foregoing does not affect or limit Galvanize's obligations under Section 9 (Security) or Section 13 (Confidentiality) of this Agreement.
- 20.7 **US Federal Government.** The Products, including related software and technology, are "Commercial Items" as that term is defined in FAR 2.101. Government technical data and software rights related to the Products include only those rights customarily provided to the commercial marketplace as specified in this Agreement. This customary commercial license is provided in accordance with FAR § 12.211 (Technical Data) and FAR § 12.212 (Software) and, for Department of Defense transactions,

DFAR 252.227- 7015 (Technical Data – Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a need for rights not granted under this Agreement, it must negotiate with Galvanize to determine if there are acceptable terms for granting those rights, and a mutually acceptable written addendum specifically granting those rights must be included in any applicable agreement.

- 20.8 Non-Solicitation. During the performance of the Services and for a period of one (1) year after completion of the Services, neither party will solicit, for the purposes of employment or retention as an independent contractor, any of the other party's employees or contractors involved in providing the Services. The foregoing will not prohibit either party from employing any individual who applies for a position in response to an internal posting, employment advertisement or other general solicitation of employment.
- 20.9 Subcontractors. Galvanize may use subcontractors in its performance of this Agreement. Such subcontractors will have the skills and experience necessary to perform the work assigned to them. Any subcontracting will not release Galvanize from its obligations under this Agreement. Galvanize will remain responsible for the work performed by its subcontractors to the same degree as if the work had been performed by Galvanize itself. Upon written request, Galvanize will identify to Customer any subcontractors performing work in respect of this Agreement.
- 20.10 Force Majeure. Neither party will be liable or responsible for any delay or failure in performance caused by a force majeure event, such as fire, flood, strike, government or military authority, earthquake, act of terrorism, internet or telecommunications failure or any other cause beyond its reasonable control (which expressly excludes a lack of sufficient funds).
- 20.11 No Third Party Beneficiaries. Except as expressly provided in this MSA, no person, other than a party to this MSA, will be entitled to enforce any term of this MSA.
- 20.12 Language. If there is any conflict or ambiguity between the English language version of this MSA and any other language version of this MSA, the English language version will prevail and will be the authentic text for the purposes of interpretation.

v. Jan 28-2020

Schedule "A" Service Level Agreement

This Service Level Agreement ("SLA") is attached to and made part of the Galvanize Master Subscription Agreement ("MSA") and sets out the service levels for the Cloud Products. Capitalized terms used but not defined in this SLA have the meanings given to them in the MSA.

1. **Service Level.** Galvanize will use commercially reasonable efforts to make the Cloud Products operational and available to Customer at least 99.9% of the time in any calendar month, excluding periods of Scheduled Maintenance (the "**Performance Commitment**"). If Galvanize does not meet the Performance Commitment, Customer will be eligible to receive the Service Credits described below. If Galvanize fails to meet the Performance Commitment for three (3) consecutive calendar months during a subscription term, Customer may terminate its subscription for cause. This SLA states Customer's sole and exclusive remedy for any unavailability of the Cloud Products.
2. **Definitions.**
 - a. "**Downtime**" means a period of at least ten (10) consecutive minutes during which the Cloud Product is unavailable and cannot be accessed or used. Intermittent interruption, downtime for a period of less than ten (10) minutes or unavailability of the Cloud Product caused by circumstances beyond Galvanize's reasonable control (such as external forces affecting the reliability of the internet or Customer's own systems or devices) will not be counted as Downtime. Downtime may be measured through an independent third party monitoring service selected by Galvanize.
 - b. "**Monthly Uptime Percentage**" means the Scheduled Service Uptime (as defined below) minus the total number of minutes of Downtime in a calendar month, divided by the Scheduled Service Uptime.
 - c. "**Scheduled Maintenance**" means occasional maintenance of the Cloud Products to add resources, upgrade software, install security patches or carry out other routine maintenance procedures. Scheduled Maintenance typically occurs during the period of lowest anticipated system usage. System notification is provided in advance of Scheduled Maintenance. During Scheduled Maintenance, certain components of the Cloud Products may be offline, or may be operating in less redundant modes, or may be operating at reduced capacity levels.
 - d. "**Scheduled Service Uptime**" means the total number of minutes in a calendar month (e.g., 43,200 minutes in a 30-day month) less the number of minutes of Scheduled Maintenance in such month.
3. **Service Credits.** If the Monthly Uptime Percentage for any calendar month is less than 99.9% and Customer is impacted by any Downtime (ie, the Downtime occurs during regular business hours when Customer is accessing the Cloud Product), Galvanize will extend Customer's

subscription term, at no charge, by the applicable number of days noted in the table below.

Monthly Uptime %	Additional Subscription Days
< 99.9% - ≥ 99.0%	3 days
< 99.0% - ≥ 95.0%	7 days
< 95.0%	15 days

To claim a Service Credit, Customer must notify Galvanize within thirty (30) days from the last day of the calendar month for which Customer wishes to receive a Service Credit. No Service Credits will be issued after this thirty (30) day period. The maximum number of Service Credits available in any single calendar month is fifteen (15) days. Service Credits may not be exchanged for, or converted to, monetary amounts.

4. **Exclusions.** The Performance Commitment does not apply to, and no Service Credits are available for, any interruption or unavailability of a Cloud Product: (a) caused by factors outside Galvanize's reasonable control, such as external forces affecting the reliability of the internet or any force majeure event; (b) that results from Customer's actions or inactions or those of any employee, contractor, agent or third party acting on Customer's behalf; (c) that results from Customer Systems (as defined in the Agreement) or from any non-Galvanize equipment, software or technology (other than third party equipment within Galvanize's direct control); (d) Scheduled Maintenance; or (e) that results from a suspension or termination of Customer's right to use the Cloud Product in accordance with the terms of the MSA.

v. Jan 28-2020

Schedule "B" Security Schedule

This Security Schedule is attached to and made part of the Galvanize Master Subscription Agreement ("**MSA**") and sets out the security for the Cloud Products. Capitalized terms used in this Schedule have the meanings given to them in the MSA.

1. Shared Security Model

Security involves a joint effort by both Galvanize and the Customer. Galvanize manages the overall security of the Cloud Products. The Customer manages the end-user security and access controls for its Cloud Product environment and is responsible for determining the types of data to be used in connection with the Cloud Products.

2. Policies and Procedures

Galvanize has implemented a security policy framework based on ISO 27001/2 to define minimum security requirements and expectations for security across its organization. The Cloud Products are supported by various operational and security policies, standards and procedures, including, but not limited to, those related to:

- o Access Control
- o Human Resources
- o Change Management
- o Information Classification
- o Media Security
- o Business Continuity
- o Disaster Recovery
- o Secure Software Development Lifecycle
- o Vulnerability Management
- o Security Incident Response
- o Third-party Management
- o Remote Access
- o Logging and Monitoring
- o Compliance

3. Security Measures

Galvanize has implemented and will maintain commercially reasonable, industry-standard technical and organizational security measures designed to prevent the unauthorized access, use or disclosure of Customer Data stored in the Cloud Products. Such security measures include, but are not limited to, the following:

- a. Access Control. Galvanize uses a principle of least privilege for internal administration. Access is granted on a need to know basis using a ticketing and approval system. Administrative access is protected with a combination of IP whitelisting, username/password, multi-factor authentication and private keys. Session limits for inactivity are set. All access is tracked and monitored for suspicious activity. Access to production system and internal applications is removed immediately upon personnel termination. Access rights are reviewed on a quarterly basis.
- b. Personnel. Hiring practices ensure new personnel are qualified for their role. Background check procedures are in place for personnel who may have contact with Customer Data. Personnel are required to complete annual security, confidentiality and privacy training upon hire and annually thereafter.
- c. Data Encryption. Galvanize provides encryption of data in transit and at rest. Encryption in transit is achieved via the industry-standard TLS (Transport Layer Security) protocol, including AES (Advanced Encryption Standard) with up to 256-bit key lengths. Encryption at rest is achieved by leveraging AWS storage encryption, which also relies on the AES encryption algorithm with strong 256-bit keys.
- d. Physical Security. Galvanize physical premises are kept locked during non-business hours and are protected by security guard and alarm services. Security cameras are visibly placed in high traffic or sensitive locations. Badges are required to gain entry into Galvanize offices and must be visible at all times. Physical access is audited quarterly. Physical security at the data center is the responsibility of Amazon Web Services.
- e. Network Security. Galvanize uses a combination of web application firewalls, intrusion detection and prevention capabilities, as well as real time alerting. Galvanize has developed procedures for monitoring HighBond systems for performance, availability, and security related events. These events are investigated promptly by the Galvanize production operations team.
- f. Hosted Environment. The Cloud Products are hosted by Amazon Web Services (AWS). Within the hosted environment, Customer is provided with its own application environment (your Galvanize service). AWS provides the physical facility and physical infrastructure of server hardware, networking and related services for the Cloud Products and the hosting of Customer Data.
- g. Asset Management & Endpoint Security. Information assets are classified and assigned in accordance with an asset management policy. Endpoint devices are managed through an endpoint management tool, including patches, encryption, anti-virus software updated at least once a day, and filtering malicious web content. Upon termination of personnel, laptops and building access cards are returned.
- h. Penetration Testing. Galvanize uses independent 3rd parties to perform regular penetration testing to check for security vulnerabilities, such as cross-site scripting, SQL Injection, session and cookie management. A summary of the most recent penetration test report can be made available to Customer subject to the confidentiality provisions of the MSA or a separate non-disclosure agreement.
- i. Vulnerability Management. Vulnerability scanning is performed at least weekly for operating systems, software components, dynamic web applications, and static code analysis. All vulnerabilities are prioritized by severity using Common Vulnerability Scoring System. When possible, mitigations will be put in place for critical vulnerabilities while a full patch is being developed.

4. Backup and Disaster Recovery

Galvanize maintains processes to ensure failover redundancy. In addition, full system/instance backups are taken on a regular basis for the purpose of restoring data integrity due to systemic or database failure, but not for purposes of restoring user deleted data. Backup media is encrypted and stored securely offsite. Galvanize also maintains a Business Continuity Plan and Disaster Recovery Procedures.

5. Security Breach Procedures

Galvanize maintains an Incident Response Plan managed by its Security Incident Response Team (SIRT). Galvanize will notify Customer without undue delay if Galvanize determines that the security of the Cloud Products' systems has been breached and this results in Customer Data being accessed by or disclosed to an individual or entity who is not authorized to access or receive such information. Notice will include a brief description of the incident, including the nature of the breach, the date it occurred and, if known, the general type(s) of data involved.

Galvanize will report to Customer on the corrective action being taken and will cooperate with Customer to mitigate the effects of any lost or compromised Customer Data. Galvanize will conduct a root cause analysis to determine the cause of the incident and to ensure corrective actions are focused on the true root cause of the incident. Customer will implement any corrective measures required by Galvanize.

6. Customer Security Obligations

Customer controls the end-user security and access controls for its Cloud Product environment and manages the entire Customer Data life cycle. Customer determines what data to use, how long data should be retained, what data should be deleted, who can access the data, addition and removal of users, and configuration of system settings. Customer is responsible for implementing appropriate security measures in connection with its use of the Cloud Products and its Customer Data, including, without limitation, the following:

- o use of security features made available through the Cloud Products
- o establishing and enforcing use of strong passwords and setting password expiries
- o establishing account access controls, such as configuring SSO (Single Sign On), challenging user accounts after multiple failed logins and using activity tracking to log access and system use
- o setting session expiries
- o specifically identifying permissible user IP addresses
- o following industry best practices for de-identifying sensitive data
- o backing-up Customer Data
- o limiting the type and amount of Customer Data, as well as its storage, to only what is necessary for the intended purpose

Customer will notify Galvanize immediately if it becomes aware of any known or suspected breach of security related to its use of the Cloud Products.

7. Security Assessments

On Customer's written request, Galvanize will complete Customer's reasonable security assessment questionnaire and provide Customer with further information regarding the security measures for the Cloud Products. Security assessment questionnaires will be completed no more than once annually and may require reimbursement of the time expended by Galvanize personnel, depending on the complexity and length of the questionnaire.

8. Security Controls Audit

Galvanize has and will maintain a current SOC 2 Type II report (or industry-accepted successor security audit) prepared by a third party auditor consisting of a comprehensive internal controls assessment covering the internal controls and information security related to the Cloud Products. Upon request, Galvanize will provide a copy of its then-current SOC 2 report to Customer. The report is Confidential Information of Galvanize and is subject to the confidentiality provisions of the MSA.

v. Jan 28-2020

Schedule "C" Data Processing Addendum

This Data Processing Addendum ("DPA") is attached to and made part of the Galvanize Master Subscription Agreement ("MSA"). This DPA applies when Galvanize or any of its Affiliates Processes Personal Data on behalf of Customer in connection with the Cloud Products or any related services. Capitalized terms not otherwise defined in this DPA will have the meanings given to them in the MSA and the applicable Data Protection Laws.

Definitions

1. **"Data Protection Laws"** means all laws and regulations applicable to the Processing of Personal Data pursuant to the MSA, including, but not limited to, the EU General Data Protection Regulation ("**GDPR**") and the California Consumer Privacy Act of 2018 ("**CCPA**"), each as may be amended from time to time.
2. **"Personal Data"** means "personal data" or "personal information" as those terms are defined in the applicable Data Protection Laws, including, by way of example, an individual's name, address, email address, username, IP address, billing information or other like information.
3. **"Process" or "Processing"** means the collection, use, storage, disclosure, erasure or destruction of Personal Data, or any other operation or set of operations performed on Personal Data, whether or not by automated means.

Terms

1. **Roles.** Customer will act as the "Controller", being the party who determines the purposes and means of the Processing of Personal Data. Galvanize will act as the "Processor" being the service provider who Processes Personal Data on behalf of the Customer. Customer authorizes Galvanize to engage sub-processors in accordance with the terms of this DPA. Each party will comply with the provisions of the Data Protection Laws that apply to its role as Controller or Processor, respectively.
2. **Purpose and Duration of Processing.** Each party will Process Personal Data only as necessary for the provision and use of the Cloud Products and related services, and for as long as Customer has a valid paid subscription to the Cloud Products.
3. **Categories of Personal Data.** The categories of Personal Data to be Processed will be determined solely by Customer and may include: name, address, email address, employee data or billing information. The categories of individuals whose Personal Data may be processed are: employees, contractors or representatives of Customer or of Customer's clients, suppliers or business partners. Galvanize does not collect Personal Data directly from individuals.
4. **Storage Location.** Customer Data will be stored in the regional data centre(s) chosen by Customer (e.g. in the United States, Germany, Singapore, Australia, Canada or such other location offered by Galvanize from time to time). User names and email addresses of Customer's users of the Cloud Products will be stored in the United States.
5. **Customer Obligations.** Customer represents and warrants that its Processing of Personal Data in connection with the Cloud Products will comply at all times with applicable Data Protection Laws. In any circumstances where providing Personal Data will not comply with Data Protection Laws, Customer must not submit or provide such Personal Data.
6. **Galvanize Obligations.** Galvanize will:
 - a. Process Personal Data only on the written instructions of Customer. This DPA and the MSA are Customer's written instructions for this purpose. Customer warrants that it is and will remain authorized to give these instructions, as well as any future instructions regarding the Processing of Personal Data, and that Customer's instructions will comply with Data Protection Laws. Galvanize will notify Customer if it believes Customer's instructions violate any Data Protection Laws;
 - b. ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Galvanize will ensure that access to Personal Data is limited to only those individuals who need to know or access the Personal Data for purposes of providing the Cloud Products and related services in accordance with the MSA;
 - c. not "sell" (as that term is defined in the CCPA) Personal Data and will not retain, use or disclose Personal Data obtained from Customer (i) outside the direct relationship between Galvanize and Customer; (ii) for any purposes other than for the specific purposes of providing the Cloud Products and related services specified in the MSA; or (iii) for any "commercial purpose" (as defined in the CCPA) other than providing the Cloud Products and related services;
 - d. implement and maintain appropriate technical and organizational measures to protect the security, confidentiality and integrity of the Personal Data Processed by Galvanize as set forth in the security provisions of the MSA. Galvanize will regularly monitor compliance with these measures;
 - e. use only sub-processors who maintain at least the same level of security measures and adequate safeguards as required under this DPA and who have entered a written agreement (which may be electronic) with Galvanize requiring such measures and safeguards. Galvanize will provide Customer with a list of such sub-processors upon request. Galvanize will inform Customer of any intended

change to its sub-processors and will provide Customer with an opportunity to object to such change. If a sub-processor fails to fulfill its data protection obligations, Galvanize will be liable for the performance of such obligations;

- f. notify Customer, without undue delay and, where feasible, within 48 hours, after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by Galvanize, and take all steps reasonably within Galvanize's control to mitigate and remediate the breach. Galvanize will not assess the contents of Customer Data to identify information subject to specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer. Galvanize's notification of or response to a breach of security will not be construed as an acknowledgement by Galvanize of any fault or liability with respect to such breach;
- g. notify Customer promptly, and where feasible within 15 days, if Galvanize receives requests from individuals to exercise their rights with respect to their Personal Data being Processed by Galvanize. Galvanize will not respond to such individuals without Customer's prior written consent, except to confirm that such request relates to Customer;
- h. meet its obligations under the applicable Data Protection Laws to: (i) assist Customer in responding to individuals' requests to exercise their rights with respect to their Personal Data being Processed by Galvanize; and (ii) meet Customer's legal obligations with respect to breach notification, data protection impact assessments, or the cooperation or prior consultation with a supervisory authority with respect to Personal Data Processed by Galvanize; provided and to the extent Customer does not otherwise have access to the relevant information and taking into account the nature of the Processing and the information available to Galvanize. Customer will be responsible for any costs arising from Galvanize's provision of such assistance, except to the extent prohibited by applicable Data Protection Laws;
- i. upon the written request of Customer, either delete or return Personal Data to Customer to the extent Customer is unable to do so itself through the Cloud Products, subject to any legal or regulatory obligations to maintain or store the Personal Data; and
- j. provide Customer with all information necessary to demonstrate Galvanize's compliance with applicable Data Protection Laws, and contribute to audits or inspections to be conducted by or on behalf of Customer no more than once in any calendar year, unless an additional audit is required by the Data Protection Laws or regulatory authority, or is reasonably necessary due to genuine concerns regarding Galvanize's compliance with this DPA. Customer will provide reasonable advance notice of any audit and will abide by Galvanize's reasonable

security requirements. Before commencement of any such audits or inspections, the parties will mutually agree upon the scope, timing and duration of the audit or inspection. Unless restricted by applicable Data Protection Laws, Galvanize may charge for any time expended for such audit or inspection at Galvanize's then-current rates, which will be made available to Customer.

- 7. Data Transfers. Pursuant to the GDPR, the legal mechanisms in place to safeguard Personal Data transferred by Customer to Galvanize or its Affiliates in a country outside the European Union, the EEA, Switzerland or the United Kingdom include an adequacy decision, EU-US Privacy Shield certification, binding corporate rules and the Standard Contractual Clauses located at www.wegalvanize.com/terms which are incorporated herein by reference and will apply to any transfers not covered by the other legal mechanisms. Galvanize will not onward transfer Personal Data that is subject to the GDPR to a country outside the European Union, the EEA, Switzerland or the United Kingdom, except where appropriate legal mechanisms are in place to safeguard such Personal Data in compliance with GDPR.

v. Jan 28-2020

Software designed for effective IT Risk & Compliance management

USE AUTOMATION TO DRIVE PRODUCTIVITY AND INSIGHT INTO YOUR IT RISK & COMPLIANCE POSTURE.

How easy is it for your organization to assess IT risk for any given asset? The assessment process can be time-consuming and inefficient, especially if you are using manual or homegrown systems or a rigid platform that can't adapt to your unique environment.

ITGRCBond was designed to automate the spectrum of nuances, users, assets, and situations. It also makes it easy to manage and meet risk and compliance requirements. ITGRCBond enables you to identify the target of the assessment, calculate the criticality and risk, record meta information, and automate the entire assessment. Once gathered, context-based workflow helps you centrally manage compliance gaps for remediation, track risk exceptions, and identify compensating controls. Reports and interactive storyboards empower users to give context and enable management to make sound decisions based on risk.

ITGRCBond has a full content library of cross-mapped controls. This library is managed and updated continually. The solution's compliance and control framework allows for flexible logic in how assets are classified, what workflow to enable, and if a gap should be generated. Users are able to leverage our existing content or create their own with the ability to map to specific compliance domains and follow a logic sequence. Controls are matched to all relevant areas in an "ask once, update many" fashion.

Key features

- + Automate manual tasks for a more effective, streamlined assessment program in a centrally managed platform.
- + Control costs and save time by creating repeatable processes.
- + Get a complete view of risk and compliance posture by geography, line of business, and domain in easy-to-create dashboards, reports, and storyboards.
- + Increase accuracy and accountability of assessment data through pre-built prescriptive control content and response audit trails.
- + Easily manage an inventory of risks and controls for a multitude of use cases.

Why choose Galvanize?

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 7,000 customer organizations in 140 countries, Galvanize is connecting teams in 60% of the Fortune 1,000, 72% of the S&P 500, and hundreds of government organizations, banks, manufacturers, and healthcare organizations.

Whether these professionals are managing threats, assessing risk, measuring controls, monitoring compliance, or expanding assurance coverage, HighBond automates manual tasks, blends organization-wide data, and broadcasts it in easy-to-share dashboards and reports. But we don't just make technology—we provide tools that inspire individuals to achieve great things and do heroic work in the process.



THIRDPARTYBOND

ThirdPartyBond Quick Start Bundle

DEPLOY AN END-TO-END THIRD-PARTY RISK LIFECYCLE MANAGEMENT SOLUTION IN NINE WEEKS.*

Most organizations understand the need to automate vendor risk management (VRM) activities to keep up with increasing scope and scrutiny. The ThirdPartyBond Quick Start Bundle allows you to leverage Galvanize's expertise to get you up and running quickly.

Quick Start Bundle benefits

- + **Automated workflows for vendor lifecycle.** Automate your vendor onboarding, classifications, and criticality assessments.
- + **Centralized vendor repository.** Manage vendor on-boarding, assessment, and off-boarding.
- + **Harmonized assessment questionnaire.** Map content to key industry standards and regulations.
- + **Dedicated vendor-portal.** Collaborate with vendors on completing assessments.
- + **Executive dashboards.** Quickly and easily communicate compliance assessment progress and outcomes
- + **Data analytics and automation.** Perform advanced data analytics, and automate IT control monitoring and risk assessments.
- + **Dedicated account team to help you get set up.** Receive training and help through all stages—configuration, deployment, and post-deployment.
- + **24/5 live support.** Access comprehensive support, as well as a dedicated Client Partner and Customer Success Manager.

Case study

A Healthcare Provider achieved incredible results with ThirdPartyBond:

50%

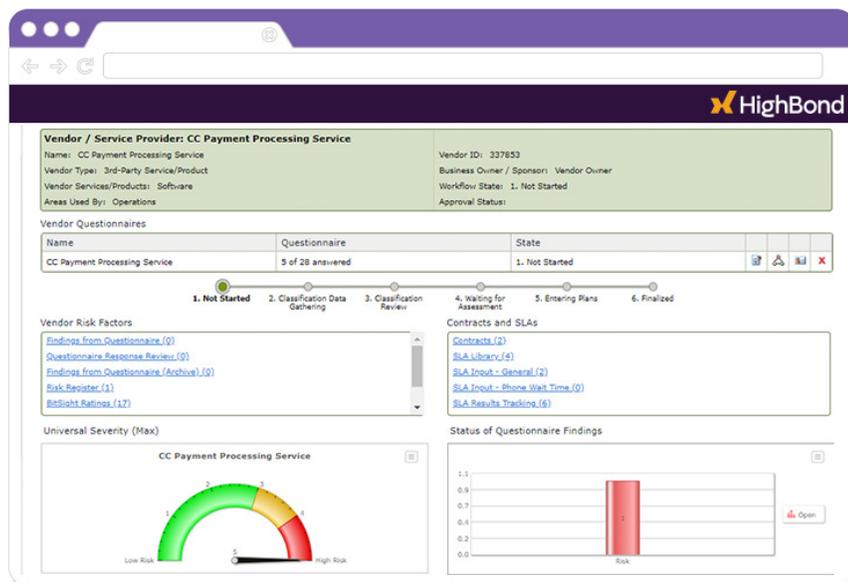
Reduction in time to complete a medium-risk vendor assessment.

373%

Increase in yearly completed assessments.

1300 hrs

Total vendor assessment time savings annually.



*Standard implementations only. Full details in statement of work.

Scope and Assumptions for Standard Configuration (Baseline) of ThirdPartyBond and ITGRCBond Services

I. Scope of Work (Summary)

This document details the steps Galvanize Professional Services performed to implement the Standard Configuration of ThirdPartyBond and/or ITGRCBond for new customers. Standard Configuration for these two packages includes pre-configured structures and workflow based on industry best practices. Pre-defined Professional Services are provided to assist customers with the implementation of the Standard Configuration as documented in the Standard Configuration Guides and Step-by-Step Tutorials for each of the modules included in the purchased bond.

II. Implementation Activities Included in a Standard Configuration

The following are the steps included to implement a standard configuration for ThirdPartyBond and/or ITGRCBond:

Note: All changes identified as out-of-scope will require change requests and additional professional services. Examples of out-of-scope changes are listed in Section III of this document.

- **Architecture review:** to ensure usage of consistent structure and universal components across all related modules to the product purchased which include the following:
 - ITGRC Bond
 - Rsam Framework
 - Risk Register
 - Risk and Compliance Assessments
 - Harmonized IT Security Assessment Contact Pack
 - Findings Management
 - ThirdPartyBond
 - Rsam Framework
 - Risk Register
 - Vendor Risk Management
 - Vendor Portal
- **Product Walkthrough and Scoping:**
 - As part of the configuration walkthrough, review potential in-scope modifications to standard product that are critical to business operations and adoption of the product. Modifications can include:
 - Modification of generic attributes (for example – Data Center, Business Units, Locations, etc.)
 - Addition of up to 15 additional attributes

- Addition of existing workflow states, workflow buttons, and workflow roles
 - Reduction of workflow steps within standard workflows
 - Addition of up to 6 additional searches/charts
 - Addition of up to 2 additional home pages
 - Addition of up to 5 additional email notifications
 - Addition Customer Branding
 - Modification of existing data import profiles
 - Configuration/Modification of synch related items, including API synch configuration of Objects/Records, migration of configurations to External Instance, and scheduled jobs for synch related items (ThirdPartyBond)
- Configure approved in-scope changes to configuration.
 - Data Import of customer data into Development instance (See below for data considered in-scope for standard implementation).

Note: Data must be provided by the customer using a Galvanize provided Excel template. Imports from other sources are not considered part of the Standard Configuration unless otherwise noted. Efforts towards Data cleansing to make it compatible with the template requirements are not included in the standard implementation. This exercise is expected to be done by the customers internally.

- **Data Imports In-Scope:**

- Issues/findings from Excel Templates.
- Risks from Excel Templates.
- User provisioning for users identified for Testing in customer's Development/Test instance
- Testing Support: for the standard product and modifications completed as part of in-scope configuration.

Note: Changes identified from testing will be managed in the internal Galvanize tool (PRT) and assessed against budget and timeline for inclusion in scope.

- **Production Deployment**

- Clean-up of test data
- Configure Migration script from Development instance.
- Migrate Configurations from Development instance to Production.
- Import of in-scope customer data into Production instance.

Note: Data must be provided by the customer using a Galvanize provided Excel template. Imports from other sources are not considered part of the Standard Configuration unless otherwise noted.

- Setup user and group provisioning for the customer in Production.

- **Support & Training**

- Updates to Standard Configuration documentation based on any customizations made as part of the implementation.
- One week of hypercare support after production go-live to monitor the customer's implementation and support any issues discovered during roll-out to the end-users.
- Remote End-User Enablement/Training (maximum of 8 hours per Bond) performed within 1 month of go-live. On-demand Academy courses
NOTE: Instructor-led Rsam Administrator training is offered for an additional cost.

III. Out of Scope (Excluded)

The following capabilities are not included as part of the standard configuration implementation. Described functionality will need to be added via customized configurations:

- Adding workflow steps to standard workflow (Reducing workflow steps is in-scope)
- Addition of Record Categories, Record Types, Object Types.
- Addition of more than 15 Attributes
- Addition of Custom Controls
- Addition of Risk Analytics Handlers
- Custom scoring, the product provides scoring based on best practices.
- Modification of out-of-the-box SSRS Reports.
- Custom SSRS Reports.
- Custom Stored Procedures.
- Additional Email Notifications other than the Five (5) included per Bond.
- Additional Searches/Charts other than the Six (6) included per Bond.
- Additional Home Pages other than the Two (2) included per Bond.
- Onsite End User Enablement/Training (End User Enablement will be performed remotely. If Onsite Enablement is required, additional scoping and separate SOW/Estimates will be required).
- Creation of Test Scripts for User Acceptance Testing.
- Dynamic tailoring to add / remove controls on a per-System basis, based on individual Confidentiality, Integrity, or Availability security objectives.
- Link control standards based on organization policy.
- Archiving of assessment data from current assessment cycle to next assessment cycle.
- Importing/Addition of Custom Assessment Questions/Controls.
- CCT Module and NIST CSF modules within ITGRC, implementation will require additional professional services.

IV. Assumptions

The following are assumptions for implementing a standard configuration of ThirdParty and ITGRC Bond:

- Implementation estimates are based on the customer being cloud hosted with Galvanize resources having access to the Customer's Development and Production environments.
- Installation of VPN, LDAP, Email Listener, SSRS, and other configurations will be installed prior to implementation activities. Installation of these configurations are managed by Galvanize Support and Cloud Services teams in coordination with customer technical resources.
- Development will take place in a development environment and migrated to a production environment. Migration to additional environments (Test/QA/Etc.) are not included as part of implementation of a Standard Configuration.
- Customer has a dedicated Rsam Administrator or has made arrangements to engage Managed Services support.
- Customer's Rsam Administrator has taken or is scheduled for Rsam Basic Administrator training available on-demand through the Galvanize Academy.
- Customer will ensure appropriate business resources are available for the walkthroughs and testing.
- Customer is responsible for maintaining the Rsam configuration once the implementation project is completed unless the customer has established Managed Services support agreement.
- In-scope Data provided for import by the customer will be provided in a Galvanize provided template following data definitions configured in the standard configuration.
- Customer is responsible for ongoing user and group maintenance
- If out-of-scope requirements are identified and determined to be required, Customer will procure sufficient professional services hours to support any out of scope requirements.
- Customer is responsible to have sufficient licensing purchased to cover all use cases implemented.
- Only current-cycle assessments data will be available in Rsam searches and reports.
- The previous year's assessment data will be preserved in documents generated via reports. This archived data will not be searchable within the Rsam application.
- Vendors will submit questionnaires on the external instance (ThirdPartyBond only).
- Customers will have to purchase another external instance if they want a corresponding instances for testing lower environments (i.e. Development). An external instance can only be linked with one internal instance. (ThirdPartyBond).

EXHIBIT A – Pricing Page
GRC Software Solution RFQ - OT20131

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	117500.00	\$ 117,500.00
4.1.3	Contract Item #2: Post Implementation Customization	HR	200.00	295.00	\$ 59,000.00
4.1, 4.2	Optional Renewal Year 2: Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	109675.00	\$ 109,675.00
4.1.3	Optional Renewal Year 2: Contract Item #2: Post Implementation Customization	HR	200.00	295.00	\$ 59,000.00
4.1, 4.2	Optional Renewal Year 3: Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	117352.25	\$ 117,352.25
4.1.3	Optional Renewal Year 3: Contract Item #2: Post Implementation Customization	HR	200.00	295.00	\$ 59,000.00
4.1, 4.2	Optional Renewal Year 4: Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	125567.00	\$ 125,567.00
4.1.3	Optional Renewal Year 4: Post Implementation Customization	HR	200.00	295.00	\$ 59,000.00
Total Cost				\$	706,094.25

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: *Dennis Anthony* Date: 10.16.2020



Galvanize Response to:

State of West Virginia

RFQ OT20131| Governance, Risk and Compliance (GRC) Software Solution



June 17, 2020

Denise M. Cushaney

Public Sector Account Executive

E: denise.cushaney@wegalvanize.com | P: 708.254.8343



June 17, 2020

Jessica S. Chambers
Bid Clerk – Department of Administration
Purchasing Division
2019 Washington St E
Charleston, WV 25305

Via: wvOASIS

Dear Ms. Chambers:

We are proud of the role our solutions and services play in helping organizations manage their risk and compliance programs. We appreciate being included in the State of West Virginia's RFQ process for a Governance, Risk and Compliance Solution. As a leader in the Integrated GRC market, Relational Security Corporation dba Galvanize ("Galvanize") is confident our solution will not only meet your current needs but also be flexible enough to grow and adapt with your organization.

For over 30 years, the companies that combined to form Galvanize have been committed to providing technology solutions that help our customers manage their governance, risk and compliance programs. Our ITGRC solution ("RSAM") was built by industry experts for industry experts. The RSAM platform unites risk management, compliance, security, and audit professionals around a single source of truth—delivering its users with the insight and automation to drive change. Our technology and expertise help our clients deliver a well-managed program with greater visibility and efficiency to increase assurance and reduce costs.

We have every confidence that our proposed solution will meet all your goals and business requirements both today and in the future. An investment in an ITGRC solution should be a long-term investment, able to meet your immediate needs while being flexible enough to adapt to changing frameworks. Galvanize is the perfect partner for that long-term engagement, evidenced by our over 96% net customer retention rate. We have every confidence that our solutions can meet all your operational and strategic goals both today and in the future. We look forward to demonstrating our solution to West Virginia. Please contact me with any questions or comments at (708) 254-8343 or denise.cushaney@wegalvanize.com.

Sincerely,

Denise M. Cushaney, Public Sector Account Executive
Galvanize

This proposal is valid until August 1, 2021.

Table of Contents

Executive Summary	1
Understanding West Virginia’s (“WV”) Needs and Project Purpose	1
Proposed Solution	1
Why Customers Choose Galvanize	2
Why is Galvanize the Right Partner for WV?	3
Summary	3
Qualifications	4
Response to Mandatory Requirements	5
Miscellaneous:	14
Attachments	14

Executive Summary

Understanding West Virginia's ("WV") Needs and Project Purpose

Galvanize understands that WV is seeking an GRC Solution that will enhance the ability of the State to maintain compliance with industry regulatory requirements, federal regulatory requirements, applicable laws and security expectations. WV is looking for a 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.

Galvanize (Relational Security Corporation dba Galvanize) is proposing its ITGRC solution, which will provide WV the ability to standardize enterprise efforts in governance, risk and compliance. The Galvanize solution will provide WV with:

- Automated workflows for the IT asset lifecycle
- A centralized IT asset inventory
- A Risk Register
- Harmonized assessment questionnaire – which allows you to map content to key industry standards and regulations.
- Executive dashboards
- Data analytics and automation
- A Dedicated account team

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 6,300 customer organizations in 130 countries, Galvanize is connecting teams in many of the Fortune 1,000 and S&P 500 companies, and hundreds of government organizations, banks, manufacturers, and healthcare organizations. Whether these professionals are managing threats, assessing risk, measuring controls, monitoring compliance, or expanding assurance coverage, HighBond automates manual tasks, blends organization-wide data, and broadcasts it in easy-to-share dashboards and reports. But we don't just make technology—we provide tools that inspire individuals to achieve great things and do heroic work in the process.

In February 2019, Rsam and ACL joined forces to create a category-defining platform for integrated risk management. This was a marriage of Rsam's dynamic flexibility, universal IT systems integration, and deep industry content with ACL's SaaS platform, including risk assurance, advanced analytics/robotic process automation, and top-rated user interface. Together, we're delivering a truly integrated governance solution. One that uses data to uncover the answers that drive strategic change.

It is important that WV evaluate solutions that have both the functionality and operational experience that WV needs today and can be easily configured to meet future requirements. WV can benefit from Galvanize's experiences, solutions, and services to obtain a robust GRC solution that can not only meet your needs today, but will also continue to grow with you as your organization matures.

Proposed Solution

To meet WV's requirements, Galvanize is proposing our ITGRC Bond. ITGRCBond was designed to automate the spectrum of nuances, users, assets, and situations. It also makes it easy to manage and meet risk and compliance

requirements. ITGRCBond enables you to identify the target of the assessment, calculate the criticality and risk, record meta information, and automate the entire assessment. Once gathered, context-based workflow helps you centrally manage compliance gaps for remediation, track risk exceptions, and identify compensating controls. Reports and interactive storyboards empower users to give context and enable management to make sound decisions based on risk. ITGRCBond has a full content library of cross-mapped controls. This library is managed and updated continually. The solution's compliance and control framework allows for flexible logic in how assets are classified, what workflow to enable, and if a gap should be generated. Users are able to leverage our existing content or create their own with the ability to map to specific compliance domains and follow a logic sequence. Controls are matched to all relevant areas in an "ask once, update many" fashion.

Why Customers Choose Galvanize

Galvanize's ITGRC Bond offers the most intuitive and flexible solutions to successfully manage your unique governance, risk and compliance needs. Our technology automates processes and transforms data into intelligence, allowing organizations to minimize risk exposure, maintain compliance, and gain business operations efficiencies. This enables you to reduce your risk and cost of compliance out of the gate and over time.

Specifically, with ITGRCBond WV will:

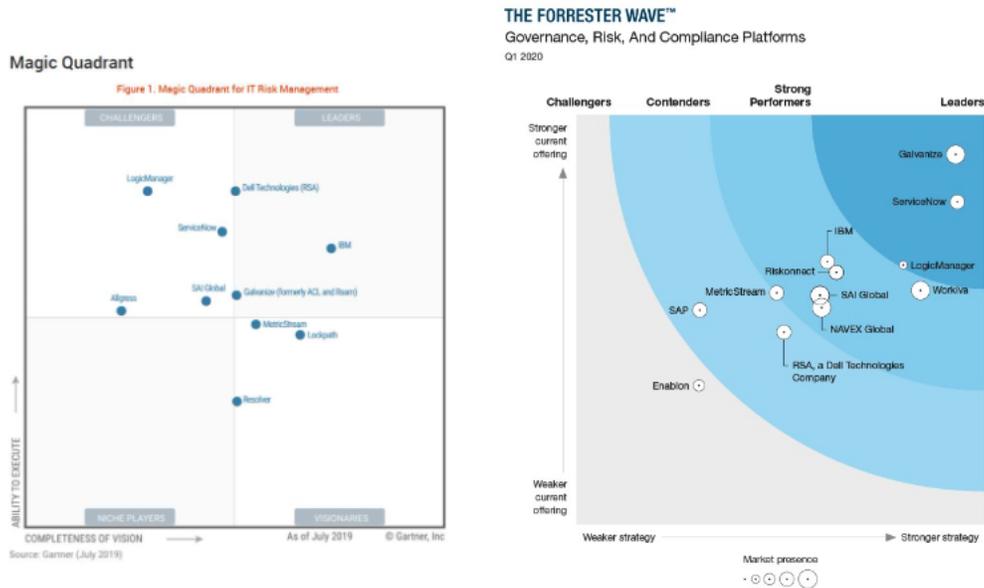
- Automate manual tasks for a more effective, streamlined assessment program in a centrally managed platform.
- Control costs and save time by creating repeatable processes.
- Get a complete view of risk and compliance posture by geography, line of business, and domain, in easy-to-create dashboards, reports, and storyboard.
- Increase accuracy and accountability of assessment data through pre-built prescriptive control content and response audit trails.
- Easily manage an inventory of risks and controls for multiple use cases including CISO Dashboards, risk register, and findings/issue management.

Why is Galvanize the Right Partner for WV?

We are the Leader in IT GRC

Our ability to deliver value quickly and empower customers to adapt our platform over time has been recognized by leading industry analysts. Galvanize has recently received the highest possible rankings through third-party analyst reviews including from: Gartner Group (Leader), Forrester (Leader), GRC 20/20 (Innovator), and Info-Tech (Leader). No other competitor has received this consistent high ranking. We encourage our buyers to evaluate both product functionality and a company's reputation. Below is a sample of the recent honors and analyst recognition awarded to Galvanize.

Galvanize named Leader in latest Gartner, Forrester GRC Analyst reports:



We have the Largest Global Community in the Industry

- Over 7000 organizations, including 72% of the Fortune 500 use HighBond
- 135 Countries where companies using HighBond are headquartered
- 900 agencies in national, state, provincial and local governments use High Bond
- Over 96% annual 'net' retention rate of Galvanize Customers

Domain Experts at Your Disposal

With a team of ex-Big Four professionals and over 100 years of combined GRC experience, we help bring your processes and data to life in HighBond by automating workflows, reporting, and storyboarding. In no time, you'll see the extent of efficiencies gained by using Galvanize products and automation to the fullest.

Summary

Galvanize is uniquely positioned within the GRC space to help WV implement an ITGRC solution. Galvanize's ITGRC Bond will automate manual tasks for a more effective, streamlined assessment program in a centrally

managed platform. The ITGRC solution will allow WV to get a complete view of risk and compliance posture by geography, line of business, and domain in easy-to-create dashboards, reports, and storyboards.

We have the experience, the staff, the solutions and the financial stability to be a long-term partner for WV, ensuring the investment in this ITGRC solution is utilized to its fullest potential.

We would be honored to have the opportunity to demo our solution to WV, so you can see first-hand how partnering with Galvanize will allow WV to transform its GRC program.

Qualifications

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

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

Over 900 agencies in national, state, provincial and local governments use a GRC solution from Galvanize.

3.2. 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.

Galvanize bases our Information Security Management on ISO 27001 and NIST. We are also FedRamp moderate compliant.

We use industry advanced and mature infrastructure-as-a-service (IaaS) providers to host our SaaS offering from four data center locations globally (North America, Europe, Asia, and Australia). The data centers provide many physical and logical security controls and are compliant with various certifications and third-party attestations, including but not limited to: ISO 27001, PCI DSS Level 1, SSAE-16/ISAE 3402 SOC 1 (previously SAS 70 Type II), SOC 2 & 3, and HIPAA. Below are examples of these controls:

- User Access
- Logical Security
- Data Handling
- Physical Security
- Change Management
- Data Integrity, Availability, and Redundancy
- Incident Handling

These controls ensure facility and equipment safeguards for areas such as multi-factor access controls, electronic surveillance, intrusion detection systems and environmental safeguards.

We review the certifications and third-party attestations provided by our sub service providers on an on-going basis to attest the services being provided and supplement complementary elements to our internal controls.

We have a current SOC 2 report prepared by a third-party auditor. This report is a comprehensive assessment of the internal controls and information security related to our service. Upon request and subject to customer's execution of our standard non-disclosure agreement (NDA), we will provide a copy of our current SOC 2 report.

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

3.3.1. 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.”*

Yes, if WV provides IP ranges to whitelist that limits access to US locations only, we can comply with this.

Response to 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.

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

4.1.1.1 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)

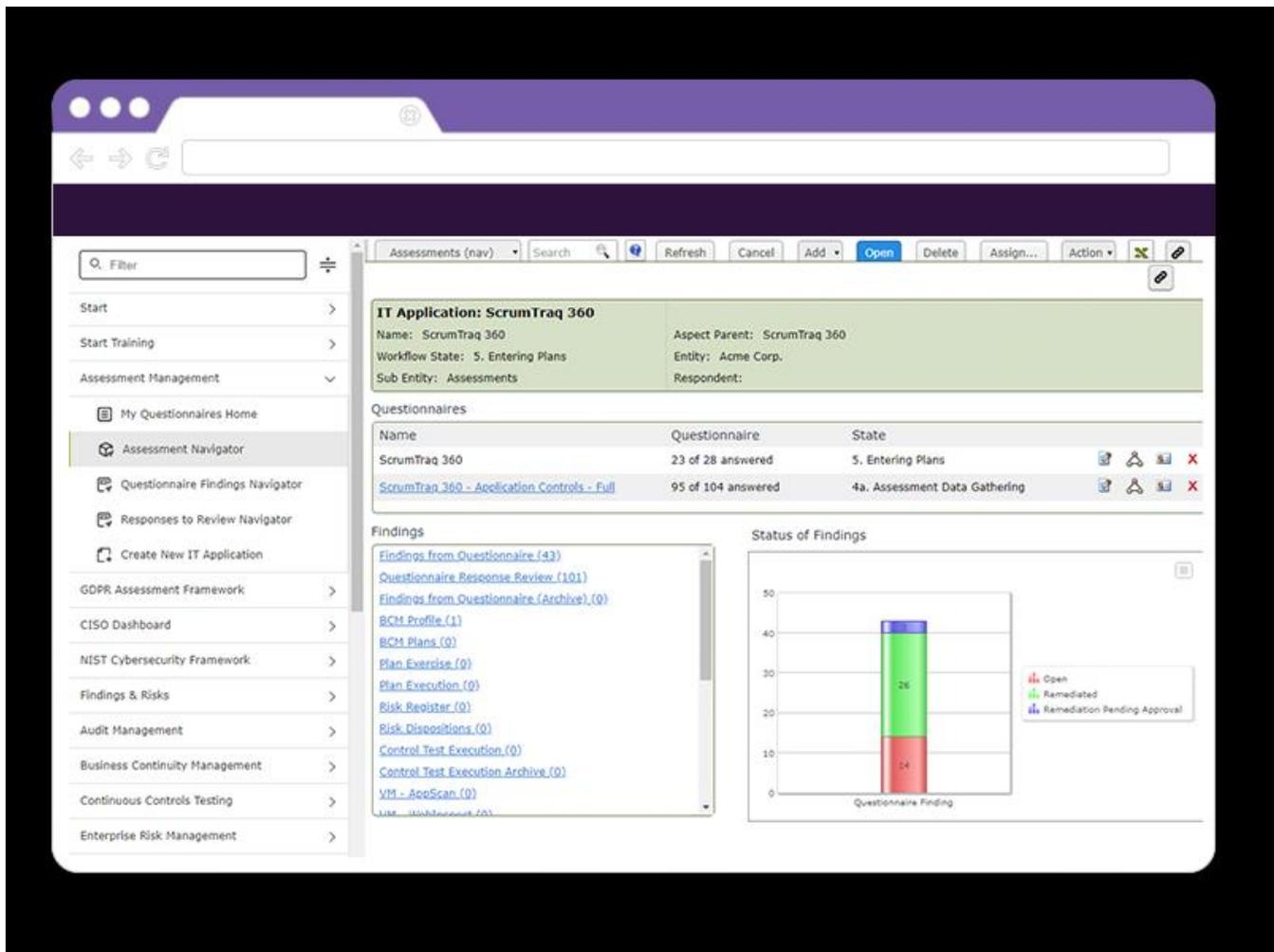
Galvanize’s ITGRC Bond offers the most intuitive and flexible solutions to successfully manage your unique governance, risk and compliance needs. Our technology automates processes and transforms data into intelligence, allowing organizations to minimize risk exposure, maintain compliance, and gain business operations efficiencies. This enables you to reduce your risk and cost of compliance out of the gate and over time.

Specifically, ITGRCBond provides:

- Flexible Enterprise GRC Platform – Single platform model with risk and compliance modules that leverage intelligence and flexibility across the organization.
- Fastest Time to Value – Get up and running quickly and easily iterate over time without additional recoding, heavy rework or resources. Superior reporting and metrics engine provides immediate visibility.
- Lowest Total Cost of Ownership – Easily scalable, expanding an organization’s risk and compliance program without custom coding or complicated redesign cycles.

4.1.1.2 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.

Galvanize provides and maintains frameworks including NCSF, NIST 800-53, PCI DSS, HIPAA, and FERPA. The CJIS framework and any other frameworks not maintained by Galvanize can be imported into the platform during implementation.



Built-in compliance content

- Use harmonized and strict content from authoritative domains like NIST and ISO.
- Map content to custom questionnaires to create a corporate compliance standard.
- View dynamic drag-and-drop dashboards by geography, line of business, compliance standard, and workflow status.
- Manage content creation lifecycles with workflows

4.1.1.3 Vendors GRC solution must automatically implement changes or updates in laws or compliance programs and alert users to relevant updates.

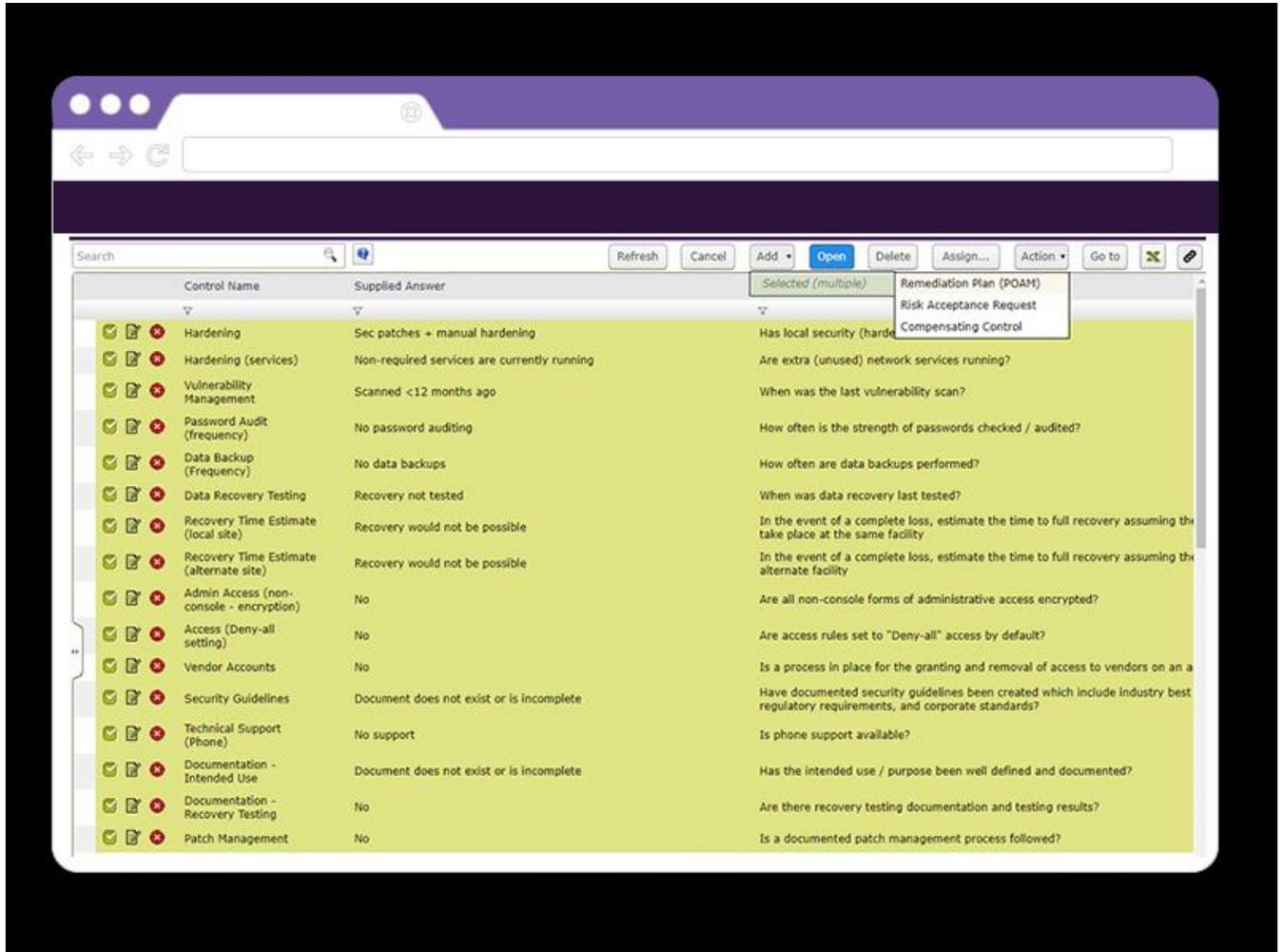
Galvanize has a dedicated content team that implements finalized changes or updates in laws or compliance programs. Users also received notice of an update change.

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

Yes, ITGRC Bond maintains the Security Requirements Traceability Matrix. The platform allows for the maintenance of libraries for objectives, risk, and controls. Any additional factors such as ranks, rates, etc. can be loaded into the platform. Client admins of the platform can provide periodic updates as needed.

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

Yes, the platform can be leveraged to identify and assess strategic risks, opportunities, and mitigating controls.



Identification of gaps

- Automatically identify gaps within your assessments and centrally collect remediation plans, risk acceptance, and compensating controls.
- Dynamically assign mitigation plans on any criteria like role, geography, and line of business.
- Use multiple workflows that can be automatically deployed based on your own business logic.
- Create custom user views to bring roles directly into prioritized work queues

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

Yes, the platform can monitor and manage strategic risks and opportunities as well as provide alerts if a risk or opportunity passes a certain threshold defined by the client.

4.1.1.7 Vendors GRC solution must report strategic risks and opportunities.

The platform's executive dashboard capability can report on strategic risk and opportunities along with any additional context the client wishes to provide.

4.1.1.8 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.

Yes, the platform has pre-built workflow and the ability to create custom workflow for users to process assets and data. These workflows can be shown or hidden based on the role of the user. User comments can be defined at each workflow step if desired.

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

Yes, The platform allows for triggers to automatically deploy control assessments to designated control owners at any given time the client chooses, including annually.

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

Yes, the platform allows for reminders, escalations, and feedback on the status of any item, including those overdue to be sent to all associated parties.

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

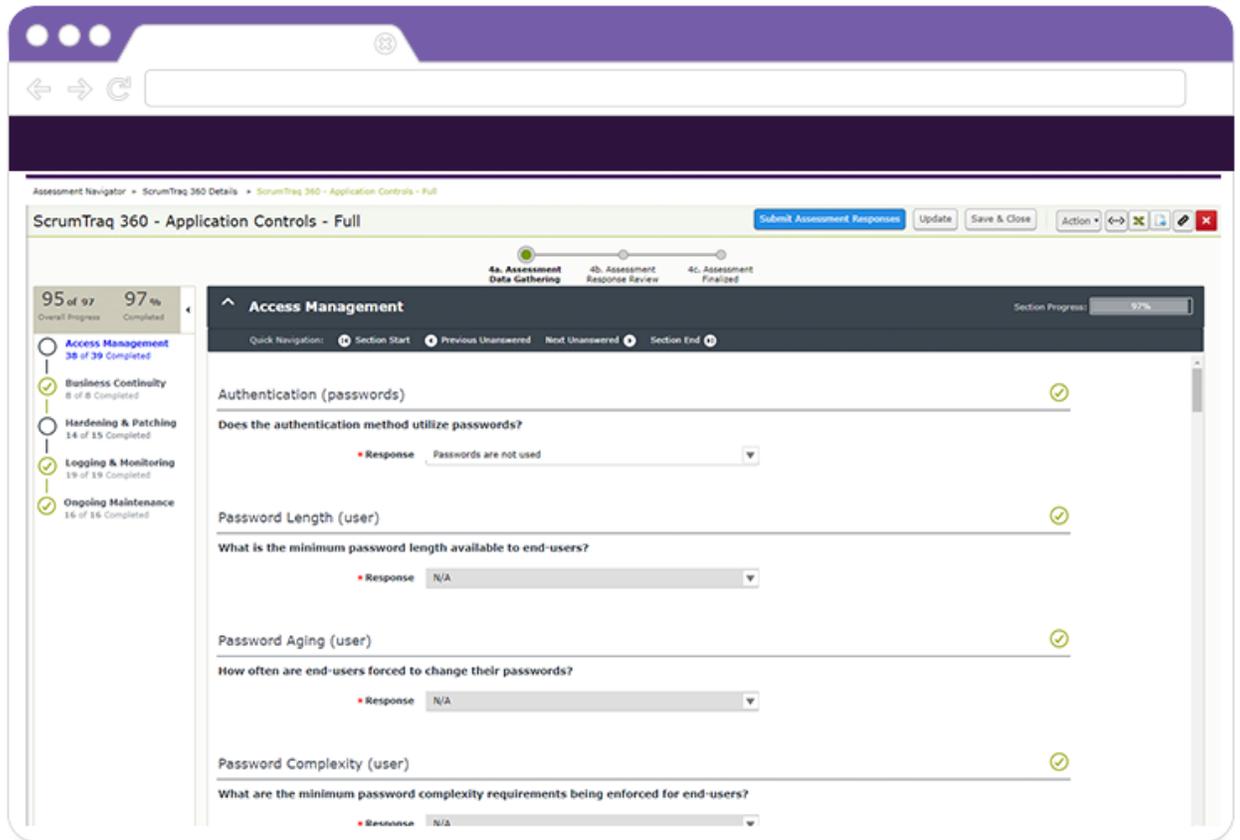
Yes, the platform allows its scheduler to automatically escalate based on the client's determined escalation threshold.

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

Yes, the Galvanize solution provides both standardized templates and dashboards that can be leveraged as well as the ability to create custom reports and dashboards. During implementation, any specific templates that Galvanize does not provide out of the box can be created as a template for your organization.

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

Yes, the platform provides out of the box use cases for documenting risk/control issues/findings/remediation plans.



Classification methodology

- Identify various applicable regulations and compliance areas.
- Gather meta data around assessment objects.
- Create user-configurable workflows that are simple and flexible.
- Rest assured with real-time notifications, alerts, and escalations for the entire assessment lifecycle.
- Configure your own standardized weighting methodology or use the out-of-the-box scoring.

4.1.1.14 Vendors GRC solution must track remediation deadlines/timelines.

The platform can be configured to track any deadline / timeline through dashboard reporting and metrics.

4.1.1.15 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.

Yes, the platform has dashboards out of the box that can be leveraged to meet this requirement.

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

Yes, the platform has built-in executive style data visualization tools as well as operational level visualization tools. Data can be exported to other tools as needed, including MS Office.

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

Yes, the platform has a data engine that allows users to search for, summarize, track, and report on data within the system.

4.1.1.18 Vendor must provide a means to summarize performance metrics.

The platform's data engine has pre-built saved searches to track performance metrics of the system. Additional performance metrics can be created either during implementation or by the client post-implementation.

4.1.1.19 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 platform is integrated with Active Directory.

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

The platform is role-based. All views from the main interface down to the tabular and field level are controlled based on the type of role a user has.

4.1.1.19.2 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)

The platform supports role-restricted access.

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

4.1.2.1 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.

In addition to train the trainer trainer, which included in our lump sum cost on the Pricing Page, additional training is provided through an online Academy portal which provides CPE credits upon completion, help docs, and community forums.

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

Galvanize is committed to meeting customer support SLA's and demonstrates this through providing post-enablement support and training in two tiers: Tier one support is available 24 hours per day 5 days

per week. Customers can create a ticket via email or web chat and support representatives will support the customer through a variety of communication methods including phone, email, web chat, and screen share.

Timely support for ongoing operations, including case reports with issue prioritization Galvanize users submit tickets via email, chat, or Galvanize’s online portal. Tickets are processed based on four severity levels: Urgent, High, Medium, Low. Case reports are available to customers

For tier two support, customers will be provided a designated Customer Success Manager (CSM). The CSM will conduct quarterly calls with key users to proactively address any issues and ensure the solution is meeting requirements. Any escalations will be sent to the CSM representative for tier two evaluation and support.

Severity ratings¹

SEVERITY:	Urgent	High	Medium	Low
Response Time ²	2 hours	4 hours	8 hours	12 hours

Coverage hours

Chat case submission	24 hours a day, five days a week Sunday 3pm–Friday 5pm PT
Online case submission ³	24x7
Galvanize Global Community ⁴	24x7

1 Severity level definitions (the determination of actual severity level for any given request is at Galvanize’s sole discretion)

- Urgent Severity: Production issue rendering software completely inoperable, error affecting all users, or loss of data.
- High Severity: Major functionality impacted or major performance degradation in non-urgent process.
- Medium Severity: Partial non-urgent functionality impacted, minor performance degradation, affecting limited users.
- Low Severity: General “how to” questions, documentation, or system configuration.

2 Response time means Galvanize will respond to you within the stated time. It does not mean Galvanize will resolve the issue within this time.

3 Online response time will be based on Chat case submission hours (i.e., 24 x 5, 6PM EST Sunday to 8PM EST Friday). Online case Submissions may be made 24 x 7, but Galvanize does not respond 24 x 7.

4 Response times do not apply to Support Center. If you believe you have encountered a security issue, availability or other type of incident on the HighBond platform, please contact us as soon as possible. We investigate all reports and strive to fix confirmed issues promptly.

4.1.2.3 The vendor must guarantee application has 99.9% uptime.

Galvanize will use commercially reasonable efforts to make the Cloud Products operational and available to Customer at least 99.99% of the time in any calendar month, excluding periods of Scheduled Maintenance.

4.1.2.4 The vendor must provide frequent progress reports during any outage.

Agreed.

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

Agreed

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

The vast majority of customers with active subscriptions rely on us to retain their data. However, you may choose to extract data for your own offline records as a secondary measure for data retention.

Upon termination of your Galvanize subscription, we will extend access to the system for an additional 30 days to copy or extract any data you wish to retain. Once you have extracted your data, you have the full ability and responsibility to delete any or all of your remaining data in the system.

Upon written request, Galvanize will destroy the customer system and all data content after the extract process. If 90 days has passed without written request to destroy the customer system, Galvanize reserves the right to destroy the customer system to regain system resources.

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

See response to 4.1.2.6

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

Yes. We provide strong encryption of all data in transit and at rest. Encryption in transit is achieved via the industry-standard TLS (Transport Layer Security) protocol supporting only the strongest encryption algorithms, including AES (Advanced Encryption Standard) with up to 256-bit key lengths.

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

Yes. We provide strong encryption of all data in transit and at rest. Encryption at rest is achieved by leveraging AWS EBS storage encryption, which also relies on the AES encryption algorithm with strong 256-bit keys.

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

This is supported.

4.1.2.11 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.

We have included 15 power user licenses in the lump sum cost of the Pricing Page within wvOASIS

4.1.3 Contract Item #2 Professional Services - Post Implementation Customization

4.1.3.1 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.

Agreed. We have included our post implementation customization rate in our price proposal.

4.1.4 Software as a Service Addendum

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

Galvanize reserves the right to negotiate the terms and conditions of a final contractual agreement after we are selected as your preferred vendor. Working with both our private and public sector customers in jurisdictions all around the world, we have found this approach to be mutually beneficial and efficient, allowing our customers to better understand the standardized solutions we offer and how they work to meet their requirements, in order to then assess and contract for how they can be used in a ways that are compliant with the laws and mandatory policies applicable to the customer.

We have attached a copy of our Master Subscription Agreement in the attachements section of wvOASIS.

Miscellaneous:

11.1 **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	Denise M. Cushaney
Telephone Number	708-254-8343
Fax Number	N/A
E-mail Address	Denise.cushaney@wegalvanize.com
Contract notices should be sent to	legal@wegalvanize.com

Attachments

Attachments Detail
<ul style="list-style-type: none">• Attachment 1 – Addendum Acknowledgement Form• Attachment 2 – Galvanize MSA• Attachment 3 – Scope and Assumptions for ITGRC QuickStart• Attachment 4 – Product Sheet: ITGRC Bond Quick Start Bundle• Attachment 5 – Product Sheet: ITGRC Bond• Attachment 6 – Exhibit A – Pricing Page