RFP 22-68200 – Cloud-based Internal Control/Internal Audit Platform
Attachment F – Technical Proposal

Respondent:	Deloitte & Touche LLP

Instructions: Respondent(s) shall provide a written response to each of the questions/prompts listed below in the yellow text box. When stated, responses shall include all minimum response requirements and clearly indicate the applicable sub-bullet (e.g., a., b., c.) for all provided descriptions.

2.4.1 Critical Functionality	
1	Please describe in detail the application's capabilities as it relates to facilitating a centralized depository for documentation (Microsoft Office or in-house products) for Internal Controls, as well as a centralized library for past audits, workflow templates, and remediation plans.

Note: Through the Deloitte-Workiva alliance, Workiva has provided the relevant responses to the software-based questions within this response.

The Workiva platform is a modern solution that connects audit, control and risk contributors (i.e., administrators, department owners, process owners, employees, testers, key personnel) from across the agency, and enables a central repository for current and historical data, documents, templates and plans. This central and collaborative platform securely streamlines management and access to documentation, simplifies audit and control methodology, and creates more time for value-added work.

Within the Workiva platform, organizations are able to maintain risk assessments, templates, audit and issue workpapers, evidence and final reports. . Reconciling information and views between different teams and contributors is no longer required because audit, risk and control data and documents are stored and updated in the platform. Users are granted access to information and workflows according to their assigned roles/permissions, and access is granular (i.e., can limit a single user's access to a single cell in a report), and includes owner, editor, viewer-only and no access options.

The Workiva platform is fully compatible with Microsoft Office. Standard Microsoft functionality is part of the platform, such as formatting, formulas and spell check. In addition, the Workiva platform supports the import/export of documents and data as Microsoft files (e.g., Word, Excel, and PowerPoint), CSV (for spreadsheets), and PDF. Additionally, Workiva supports many file types, including Microsoft Office and Adobe Acrobat, to attach to workpapers and as evidence for mark up.

Microsoft Compatible: Workiva is fully compatible with Microsoft Office including Adobe and supports the import/export of documents and data as Microsoft files (e.g., Word, Excel, and PowerPoint), CSV (for spreadsheets), and PDF (export file as). Additionally, the Local File Sync feature enables client to download attachments on their local machine and open in the native application (e.g., Word, Excel, and PowerPoint) and upon saving changes, automatically re-upload (replace) the original file accordingly. The platform also integrates with Microsoft Office 365 which enables Excel (.xlsx), Word (.docx), and PowerPoint (.pptx) files to open in Office Online. With Office Online, client views and edits Microsoft file types in their native format use standard functions (e.g. spell check, formula check). Any edits to the documents flow back into the Workiva. Lastly, standard Microsoft functionality is part of the platform, such as formatting, formulas and spell check.

Workpaper Document Types: Workiva supports an extensive list of file types including but not limited to the following: accdb, .accde, .accdr, .accdt, .arf, .bmp, .cgm, .css, .csv, .dfb, .dfx, .dif, .doc, .docm, .docx, .dot, .dotm, .dotx, .egp, .emf, .eml, .eps, .gif, .hwp, .icml, .ics, .jpe, .jpeg, .jpg, .jtd, .jtt, .lis, .log, .lst, .met, .mht, .mml, .mp4, .msg, .mwv, .odg, .odm, .odp, .ods, .odt, .one, .onetoc2, .oth, .otg, .ott, .pct, .pcx, .pdb, .pbm, .pdf, .pgm, .pictclipping, .pfx, .plt, .png, .pot, .potm, .potx, .ppa, .ppam, .ppm, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prn, .psd, .psw, .pxl, .ras, .rtf, .rtp, .sda, .sdc, .sdd, .sdp, .sdw, .sgf, .sgv, .sgl, .sld, .slk, .smf, .sql, .stc, .sti, .stw, .svg, .svm, .sxc, .sxg, .sxi,

.sxm, .sxw, .tga, .tif, .tiff, .txt, .uof, .uop, .uos, .uot, .vdw, .vor, .vsd, .vsdm, .vsdx, .vss, .vssm, .vssx, .vst, .vstm, .vstx, .wb2, .wdesk, .wks, .wk1, .wmf, .wmv, .wpd, .wps, .xbm, .xla, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xpm, .xps, .xsd, .123, .602

2	What are the standard reports that your company provides to your customers? Please provide a list of your company's standard reports, including examples, as an attachment to your RFP response. Please note which are available online.

The Workiva platform is a connected compliance and reporting platform designed for many reporting needs. The familiar Microsoft-like design makes it easy for the DOR to adopt the solution, access standard reports/templates and configure new reports/templates without custom development. This can be done by using the audit, control and risk data stored within the platform. For example, DOR users can update final audit reports with one click because workpaper data is linked to the final report. This capability supports accurate and consistent information and saves DOR users time. Implementation services include the setup of standard audit management and internal controls management reports and templates. The list of standard reports is noted below.

List of Standard Internal Audit Management Reports and Templates: Final Audit Report; Procedure Results; Audit History; Audit Plan; PBC Request; Issue Logs; My Assigned Issues; My Audits; Time Log; My Dashboards; Audit Overview; Issues; Resource Management; Audit Risk Assessment; Audit Announcement Memo; and, Quarterly Audit Committee Report.

AuditNet®: Workiva partners with AuditNet® in order to provide a variety of commonly used audit templates that are accessible from within the platform. Thousands of auditors throughout the country create and use the templates provided by AuditNet®.

List of Standard Internal Controls Reports and Templates: Action Plans; COSO Point of Focus Coverage; COSO Point of Focus Gaps; Control Listing; Controls without Risks; Issue Listing; My Controls; Requests; Risk and Control Matrix; Risk Listing; Risks without Controls; Test Matrix; COSO Coverage Summary; Audit Committee Dashboard; Deficiency & Remediation Dashboard; Program Overview Dashboard; Test Planning Dashboard; Tester Monitoring Dashboard; and Testing Status Dashboard.

In addition to the list of standard internal controls reports and templates the following customer-provided documents, if applicable, are set up and linked as part of implementation services: Process Narratives; Process Flowcharts; 302/404 Certification Letter Templates; Audit Committee Presentation; Overdue Testing Status; Overdue PBC Request Status; and Issue Management Aging.

Dashboards: The Workiva platform offers dynamic, user-centric dashboards. The user-centric dashboards update in real-time as information is entered and updated, and tasks are completed. The one-click drill down feature offers quick access from the dashboards to the specific data populating a chart, graph or report. Dashboards are easy to create, and users can create multiple dashboards, if desired.

Marketplace: The Marketplace is an online central location (https://marketplace.workiva.com/en-us) for customers to browse or search reports, templates, connectors and services representing the effective uses of the Workiva platform. Workiva has pulled together listings from around the company and from our top partners. Reports and templates range from process checklists to carefully organized and linked reports. Users have the option to edit these templates if desired.

Sample dashboards, reports and templates images are included in the attachment titled '2.4.1 Appendix - Sample Reports and Dashboards'.

3	What standardized reporting templates are available with the application? Please provide a list of your company's standardized reporting templates, including examples, as an attachment to your RFP response.

The standard dashboards, reports and templates that are available using the Workiva platform for internal audit management and internal controls management are noted in technical question #2 (above) and sample images are provided in the attachment titled '2.4.1 Appendix - Sample Reports and Dashboards'.

4	Please elaborate on your application's document management capabilities, including the ability to link critical information across multiple documents such as narratives and process flows, version history capture, and audit plan creation.

The Workiva platform uses a *Graph Database* to link information together in a more efficient way compared to traditional relational databases used by most solutions on the market today. The *Graph Database* uses the same data points across the entire platform. For example, if the DOR updates the control language in a report, the test sheet updates as well. . Workiva calls this *dynamic linking*. *Dynamic linking* is a patented technology that confirms the user's documentation, such as flowcharts, narratives, Audit Committee Presentations is accurate and consistent. *Dynamic linking* eliminates manual copy-paste processes and manual updating by automatically updating linked content, minimizing human error and saving staff time.

In addition, the *Graph Database* links information (e.g., risks, audits, and objectives) together in one-to-one and one-to-many relationships, allowing teams to highlight interconnectivities. The Graph Database empowers organizations to view and connect data in more meaningful and efficient ways in comparison to traditional relational databases used by most solutions on the market today.

Audit, control and risk data, evidence, procedures task, template reports and workflows are maintained and completed within the Workiva platform, making the solution a central repository. The DOR creates workpapers, names audits, adds descriptions, assigns appropriate staff and process owners, links audits to related controls and risks, triggers review-approval workflows, requests evidence, marks up evidence, tracks status and writes conclusions. Information captured during the audit and control processes is readily available for reporting, and the Evidence Testing experience with a drag-and-drop feature makes the evidence markup process simplified.
The Workiva platform includes Audit Forms and Procedure Forms (i.e. electronic workpapers) that act as a summary page for documentation. The user ties these related workpapers in various formats (e.g., to one another, to a cover sheet, to a summary page, etc.) for maximum flexibility. For example, a DOR user can leverage the Evidence Testing experience to enable a tester to drag and drop specific attributes onto supporting documentation while cross-referencing the test matrix and other related documentation. Similarly a DOR user can embed spreadsheets and the preparer inputs figures for comparison, performs calculations, supports testing, and ties the information back to Procedure Forms.

Real-time collaboration is a core function of the platform. Users access and work in the platform at the same time with real-time updating, supporting collaboration and eliminating version control issues. Workiva offers a complete audit trail feature logging activity, changes, deletions, edits and updates by user with a date/time stamp. Audit trail information is granular (i.e., tracked down to the individual cell level), and readily available within the platform. The audit trail includes data and time stamps related to workpaper edits and signoffs. Lastly, Workiva offers granular control/permissions to enable controlled collaboration and to support varied levels of control within sections and components of the platform. For example, the administrator can restrict a single user's access to a single cell in a spreadsheet or single section within a document. Workiva supports user- and role-based security. The account administrator sets different levels of permissions for users and roles, controlling users' ability to modify and/or view content.

5	Please describe in detail the application's capabilities as it relates to facilitating scheduling to manage audit plans, reminders to business owners of upcoming tasks associated with internal control documentation review, and notification to Internal Control and Internal Audit administrators of completion and status of tasks.

Audit Planning

The Workiva platform offers user-friendly project management capabilities and makes it easy to track and report progress and resource utilization. Managers use the *Planning* experience to plan what audits to perform for a specific period of time (e.g., year), and easily assign staff and budgeted hours to projects. Gantt chart and table views are available for a high-level view of audit projects and assignments. Staff enter project time which links to budgeted verse actual hour reports and dashboards.

Reporting on resource utilization and project metrics can be done within the Workiva platform because project activity and data is maintained and stored within Workiva. Client creates customized dashboards and reports for activity like budgeted vs. actual hours, outstanding tasks and project completion. In addition, Workiva's *dynamic linking* function means client saves time maintaining accurate dashboard and reports because information is updated in real-time (e.g., as work is completed and/or entered by contributors), and one-click drill down capabilities from dashboards and reports provides quick access to more detailed information.

- **Create a Plan and Project:** The manager adds a project using the *Add Project Entry* function. From the *Add Project Entry* screen, the manager selects the specific project (e.g., Payroll Audit), the associated activities for the project (e.g., Planning, Fieldwork, Reporting), and assigns staff, budget and duration to the respected project. The information entered automatically populates the Gantt chart view of the audit plan.
- **Track Time:** As staff completes work, they enter hours accordingly using the *Time Entry* function. After the time is entered, associated dashboards and reports are automatically updated. The manager has the flexibility to track and report budgeted versus actual hours in a variety of ways (e.g., by total, by auditor, by specific audit project).
- **Reporting**: Since audit, control and risk data is entered, maintained, and stored within Workiva, the manager easily reports budgeted hours verse actual hours to Management and the Audit Committee, without undue effort. Linked dashboards and reports update in real-time as information is updated. In addition, Management and Audit Committee members create customized dashboards and reports to view the information as needed or desired.

Communication, Task and Reminders

The Workiva platform includes several task assignment and notifications functions to streamline communication and remind users to complete tasks (e.g., complete audit survey, review workpapers, upload evidence, etc.). The primary notification tools are *Certifications*, *Comments*, *Evidence Request*, *Review and Approval Workflow*, and *Tasks* and each tool includes an email notification feature. In addition, users have personalized landing pages that resemble a "to do" list, providing a complete view of notifications and tasks to address in one spot.

- **Certifications**: The *Certifications* function (i.e. risk surveys) enables SCS to create surveys with applicable questions, store surveys as templates in a library for future use, and send surveys to the appropriate users. The auditees receive email notifications alerting them to respond to the survey, provide additional context, and attach documentation as needed. The auditees also receive reminder emails on a scheduled basis until the survey is completed. SCS tracks the status of surveys with dashboards and reports that update in real time.
- **Comments**: The Workiva platform supports coaching notes throughout the audit project lifecycle using the *Comments* function. The *Comments* function: maintains coaching and review notes within the platform; enables reviewers and preparers to direct coaching notes to specific users as well as associate notes with

specific content (e.g., section within in document, sentence within a paragraph, single cell within a spreadsheet); **sends automatic email alerts** to the respected user as a note is posted; clears notes as they are marked resolved; stores resolved notes and makes them accessible for reference or evaluation at a later time; enables reviewers and preparers to filter notes according to status (e.g., open, resolved), user, date and content; and, appears on the user's landing page as well for easy access. Using *Comments,* reviewers and preparers maintain communication within the platform, eliminate the need to use other tools to communicate and save past communications if need for reference at a later date. In addition, preparers and reviewers design customized home/landing pages for a snapshot view of any direct comments/coaching notes.

- **Evidence Request**: The Workiva platform offers an Evidence Testing experience function that is compatible with numerous file types, including Microsoft Office file types and PDF. Auditors markup workpapers with drag-and-drop annotations, electronic tick marks, and footnotes that are linked automatically to the testing matrix. Reviewers provide coaching and review notes directly on the workpapers, and the platform maintains a complete audit trail of all changes made and communication between users.
- **Review and Approval Workflow**: Client uses the review and approval workflow feature within the Audit experience for workpapers, and the workflow process captures user, date and time stamps. A Client user prepares workpapers and then assigns a reviewer upon completion, which triggers an automated email notification to the assigned reviewer. The auditor assigns any number of reviewers to the workpapers, and reviewers leave directed coaching notes using the Comments function. A directed comment triggers an automated email notification to the preparer of the workpaper. Client locks workpapers, as needed, to prevent further changes, and tracks the status of all reviews using real-time dashboards. In addition, the Workiva platform supports a PBC Request workflow that includes automatic notifications and a tracking dashboard providing a quick snapshot view of requests and status.
- **Task:** The Tasks function allow users to create and assign tasks to other users. A user adds a task detailing title, due date, description, assignee(s) and location (i.e., specific section of document or entire document). Once the task is created, the assignee receives an automatic email alert. Reminder emails are automatically sent and the assigner can send reminders at any time.

6	Please describe in detail the application's capabilities as it relates to user roles, document access security, and ability to integrate and coordinate internal controls activities with audit functionality.

The Workiva platform supports role- and user-based security and is granular to achieve varied levels of control within the platform. For example, the administrator can limit a user's access to a single cell within a spreadsheet or section within a document. Permissions includes the following features: distribute role-based document access and privileges for administrators, contributors and reviewers; set permissions at the cell, document or section level; approve and reject proposed changes; and four (4) permission levels.
The four (4) Permissions levels are:

- Owner: A user with owner permissions can edit text, lock and unlock data cells, accept and reject track changes, adjust user permissions, and adjust style guides to lock down formatting.
- Editor: A user with editor permissions can edit text and data within a document, spreadsheet, and presentation.
- Viewer: A user with viewer permissions can view content within a document, spreadsheet, and presentation, and apply comments but not edit.
- No Access: A viewer with no access cannot view, edit, or access a document, spreadsheet, and presentation

2.4.2 Training and Support

1	Please describe in detail your company's proposed initial training and support. What is your company's standard process for implementation and training of administrators and various role-based users?

Indiana Department of Revenue will be supported during and after implementation with end user-based training by Deloitte as well as direct on-call support from Workiva. Deloitte's end user-based training will be held across multiple days specifically for key users of the platform. The training will be taught using a hands-on approach within the platform meant to prepare end users for completing their tasks in the platform. End users will also be prepared to teach others within the organization on how to utilize the platform in the future through Deloitte's "train the trainer" approach. In addition to this formal live training, Workiva will also provide a customer service manager (CSM) to Indiana during and after implementation. This professional is available on call as needed to help provide additional support and typically provides more support as needed after implementation. Workiva also provides a full 24/7 help line should immediate technical support be needed during or after implementation. Please see more detail on these various roles below and/or at the following links:
https://www.workiva.com/legal/premiumsupport
https://www.workiva.com/legal/service-level-commitment

Customer Success Manager: The CSM is a single person dedicated to the State of Indiana - DOR for the life of the contract. The CSM is the strategic partner, and helps the DOR identify opportunities, shares use case leading practices, coordinates user training and adoption, and schedules recurring strategic meetings.

Support Team: In addition to the CSM, the DOR has access to Workiva's 24/7, world-class Support team, as well as the Success Center, which includes The Learning Hub (online courses), a Help site (hundreds of articles and video tutorials on the platform) and Community (where you can converse with other Workiva customers, ask questions, post answers, etc.). Lastly, Workiva hosts an annual user conference called Amplify. Amplify brings together thousands of users and provides training, professional development sessions, CPE credits.

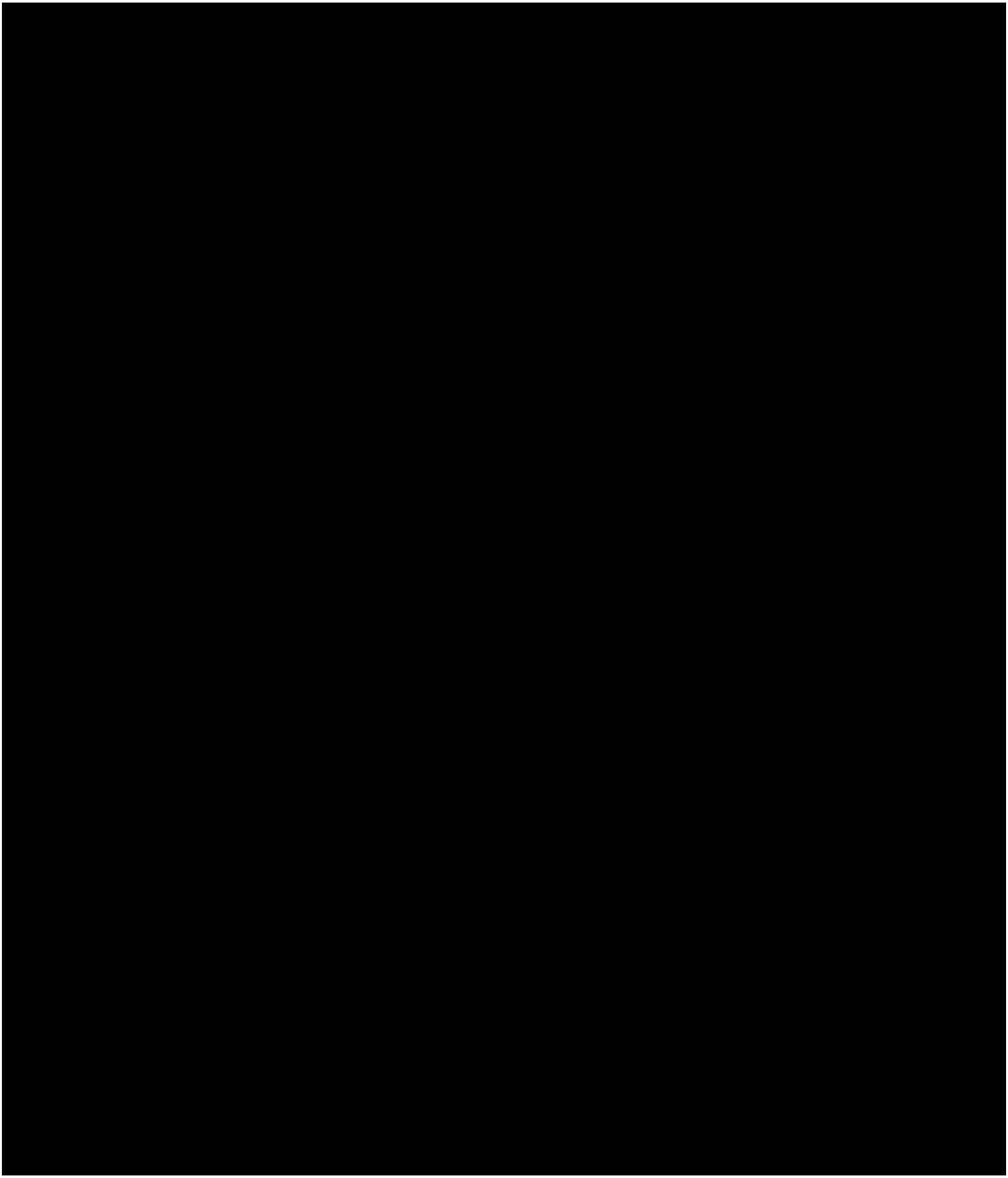
Hosting and Platform Maintenance: Workiva manages all enhancements and optimizations as well as all upgrades

2	Please describe in detail your company's proposed management team structure including names and contact information where possible, and services each individual or group will perform.

Deloitte will be prime on this implementation with support from the Workiva CSM and account team as needed.

[redacted]

Figure 1. Team Structure



[redacted]

Please refer to '2.4.2 Appendix - Practitioner Resumes' for deeper insights into our qualified professionals.

Note: Please note that the profiles are representative and are provided to demonstrate the caliber of people currently available to assist you in this engagement. Proposed staffing is based on current projected availability and timing of the award. Staffing will be confirmed at the start of the engagement

3	**What is your company's standard process for problem resolution, including standard response times? What is the escalation process if the standard resolution process cannot resolve the issue?**

Workiva adheres to a detailed Service Level Commitment (SLC) that is provided as an attachment with the response. Workiva uses commercially reasonable effort to correct or provide reasonable workarounds to address all material errors that are identified in the platform. Any reported error or issue is classified (i.e., critical, urgent, standard) according to defined criteria and the classification corresponds with a detailed Workiva response timeframe (e.g., 30 minutes, 2 hours, etc.). For example, Workiva support responds to a critical error within 30 minutes and works to correct the issue or provide a reasonable workaround, providing status updates every two hours. Unresolved issues are escalated according to their initial error level (i.e., escalated from urgent to critical). In the event an urgent issue is not resolved, a reasonable workaround is not identified, a resolution has no estimated delivery time, or is determined unresolvable within four business days, the issue is escalated to critical. And critical issues that are not resolved or for which a reasonable workaround is not provided, the issue is escalated to a member of Workiva's Executive Management who is personally involved in overseeing the resolution

Workiva shall maintain a customer support team staffed with personnel to receive inquiries by telephone and e-mail 24 hours a day, year round (excluding limited holidays). Please refer to '2.4.2 Appendix - Workiva Service Level Commitment' for detailed service level commitment.

4	**What reference materials are available that users might access for content/support on the application?**

The DOR has access to reference materials using Workiva's Success Center that includes The Learning Hub (online courses), a Help site (hundreds of articles and video tutorials on the platform) and Community (where you can converse with other Workiva customers, ask questions, post answers, etc.)

5	**Where are your support personnel located?**

The Support Team is US based, has a greater than 95% customer satisfaction rate, and handles all technical questions. Workiva provides a support phone number and email. Basic support hours are from 9:00 AM to 5:00 PM, Monday through Friday based on the time zone of the nearest Workiva support center. Support center locations are in Eastern (ET), Central (CT), Mountain (MT) and Pacific (PT) Time Zones. In addition, Workiva provides customer support by telephone and e-mail 24 hours a day, year-round (excluding limited holidays). The 24/7 support includes a two hour maximum response time.

2.4.3 Security

1	It is the intent of the Department of Revenue to contract with a respondent that has a quality cloud based application. Is your application cloud based, and if so, does the company have the capability of allowing the application to reside on the State's Indiana Office of Technology (IOT) cloud?

The Workiva Platform is a cloud-based software as a service (SaaS) solution. Workiva does not support deploying the platform to the State's cloud.

2	Please detail your company's structure and management of the application as it pertains to the following: 1. Network Management 2. Storage Management 3. Database Management 4. Project Management

Workiva manages Information Security in several areas

- Internal Information Security - internal Information Security who manages security policy, standards, procedures, exceptions, security awareness training, code reviews, vulnerability assessments, log monitoring, cybersecurity, incident management. This team reports up through the Senior Director of Information Security to the VP of IT/Security.
- Cyber Security Compliance - This team is the customer facing team for Sales who works with prospects/customers on their compliance and risk needs. This team reports up through to the VP of Solution Engineering
- Platform Support (Tier II Support) - This team manages customers on the support of the Workiva Platform for security, authentication, browsers and API integration. This teams works with customers on setting up their security requirements within Wdesk. (SSO)This team reports up through tot the VP of Customer Success
- Compliance - this team manages internal and external audits along with special initiatives This team reports up though to the VP of IT/Security
- Infrastructure and Reliability - this team has security architects for the design of our platform security and reports us to the VP of Infrastructure and Reliability
- The Chief Compliance Officer oversees the information security function and all other areas of compliance.

Admin roles with the State's instance are managed by the State within the account.

- The Organization Admin by default is split into User Admin, Workspace Admin, and Security Admin.
- Org User Admins can add, remove, update and view users in your organization, manage organization settings, and view all activity in the organization.
- Org Workspaces Admins can manage all workspaces, workspace settings, members, roles, and groups, create new workspaces, and view all activity in all workspaces
- Org Security Admins can view, update, and manage organization security settings, such as password settings, access restrictions, and SAML single sign-on.

Workspace & other Admins:

- Workspace Owner - appointed by Org Workspace Admin, can add and manage users to the Workspace (must exist on the organization), manage files, update settings, view activities, move files, and add and manage groups.
- Database Administrator - have access to view and edit all data records in the database.
- Certification Admin -can manage all things in Certifications no matter who created it.

3	Please verify the access capabilities of the company's application, including verification that the application will integrate with the State's existing technology, and adaptability to incorporate single sign on access.

The Workiva Platform provides an administration portal for security and organization settings. The settings include a configuration for single sign-on (SSO) using Security Assertion Markup Language (SAML) and a configuration for multi-factor authentication using a smartphone (e.g., Google Authenticator) or hardware security token.	
4	Confirm the company's level of compliance as it relates to FedRAMP certification level, and whether the company's solution is validated in the government cloud.
The Workiva Platform is FedRAMP authorized at the moderate security impact level for a broad range of connected reporting and compliance solutions. FedRAMP Authority to Operate (ATO) Details: Authorization Date: 10/9/2019; Service Model: SasS; Impact Level: Moderate; Status: FedRAMP Authorized Package ID: FR1726564822; Authorization Type: Agency; Independent Assessor: Coalfire System, Inc., The Federal Risk and Management Program Dashboard.	
5	Confirm the company's FedRAMP cloud is for government and if not, whether there are plans for it to get on the GCC and when.
The Workiva platform uses the Amazon Web Services (AWS) and Google Cloud Platform (GCP) cloud infrastructure and services. The AWS and GCP infrastructure are authorized at a FedRAMP moderate level.	
6	DOR has adopted a FISMA-based security requirement for its operations and systems due to the high need to keep DOR's data confidential, available, and with high integrity. DOR uses the highest intolerance for risk in its assessment of the system. DOR classifies its systems as moderate impact systems under the FIPS Publication 199. DOR requires that the Contractor be compliant with such a security scheme for its system and operations because DOR will be transmitting its data to the Contractor. Please describe the security scheme adopted by the company. Verify the company is compliant with the following: a. NIST and IRS Publication 1075 (PUB 1075) security controls and requirements to which DOR subscribes. Contractor must be familiar with the requirements of NIST 800-53 to certify that their software conforms to NIST 800-53 and to assist DOR with installing its software in a manner that complies with NIST 800-53. Contractor must also comply with all aspects of NIST 800-53 during support activities when they attach to the State's data network to perform support tasks. Any Contractor who possesses DOR data in their facilities must comply with all aspects of NIST 800-53 pertaining to safeguarding that data. Contractor should also note that in some instances NIST 800-53 references other federal standards, such as the FIPS 140-2 Encryption Standard, with which they must also comply. DOR must comply with IRS PUB 1075 governing federal, state, and local entities' use of federal tax information (FTI). As a result, Contractor must also comply with IRS PUB 1075 when handling FTI and the systems on which it resides. Contractor should note that PUB 1075 is a subset of the standards and controls identified in NIST 800-53. b. Contractor shall provide evidence of compliance with NIST 800-53 and IRS PUB 1075. Evidence shall include the report of Contractor's self assessment of information technology (IT) assets, processes, practices, and facilities against security criteria from aforementioned documents. The first of these self-assessments shall be provided with the RFP response. c. Contractor must certify to compliance with DOR's reading of FISMA, NIST SP800-53, and security best practices. d. Contractor must describe how its proposed solution provides its own data security. e. Contractor will be required to evaluate its proposed system against a set of security technology implementation guidelines (STIGs). The STIGs are available on the Defense Information Security Agency (http://iase.disa.mil/stigs) website.
Compliance: Workiva maintains an authorization to operate (ATO) at a FedRAMP moderate level. The FedRAMP authorization verifies that the Workiva platform implements the relevant controls in NIST SP 800-53. Encryption for data at rest and data in transit following NIST standards including FIPS 140-2 is included in the security	

controls. The DOR owns the data input in the Workiva platform, and Workiva does not monitor the specific data. The security and privacy controls maintained by Workiva do cover the moderate data classification.
Workiva's FedRAMP Authorized Package (ID: FR1726564822) is maintained in the FedRAMP Marketplace (https://marketplace.fedramp.gov/#!/product/wdesk?sort=productName&productNameSearch=workiva). With a non-disclosure agreement, Workiva will supply FedRAMP System Security Plan (SSP), SOC 2 Type 2 report, and InfoSec Policies and Approvals to certify compliance with FISMA, NIST SP 800-53, and security leading practices.

IRS 1075:
The systems which the Platform resides (AWS and GCP) work to meet Pub 1075 requirements (see below) and as part of the FedRAMP authorization, Workiva implements controls in NIST SP 800-53 under the moderate level.

Workiva partners with Amazon Web Services (AWS) and Google Cloud Platform (GCP) for infrastructure and platform services. AWS and GCP work closely with the IRS to ensure the environments meet Pub 1075 requirements for storing and processing FTI.

https://aws.amazon.com/compliance/irs-1075/#:~:text=1075%20security%20requirements.-,AWS%20has%20worked%20closely%20with%20the%20IRS%20to%20ensure%20that,for%20storing%20and%20processing%20FTI
https://cloud.google.com/security/compliance/irs1075

The IN DOR owns the data input to the Platform so the DOR would be responsible for any reporting and deletion of data based on IRS 1075 (e.g., 45-day notification). The Workiva Platform is FedRAMP authorized, located in the US, encrypts data in transit with FIPS 140-2 compliant encryption, and encrypts data at rest with FIPS 140-2 compliant encryption. The Workiva Platform is a multi-tenant solution and uses logical data separation.

Data Protection:
Workiva provides protection of the data including NIST standard encryption for data at rest and data in transit, granular access, connected platform (eliminating the need to share data outside the platform), and detailed audit trail. Workiva also provides continuous monitoring of the platform.
The DOR owns the data in the platform. All data is encrypted at rest and in transit, and Workiva does not monitor the DOR's data. The DOR may save, export, or delete data at any time. The DOR may export data in docx, xlsx, and pdf formats for archival purposes. The Workiva platform also provides the option to export in XML format for later use in the platform. The security and privacy controls maintained by Workiva apply to the moderate data classification and the controls apply to active data and data marked for deletion.

STIGS: As part of the FedRAMP authorization and overall security posture, Workiva maintains up to date configurations, software updates, and vulnerability patching matching configuration standards outlined in STIGs.

Data Purging:
Secure destruction of the data is performed by the secure deletion of all files and file pointers to data fragments. Workiva partners with Amazon Web Services (AWS) and Google Cloud Platform (GCP) for infrastructure and platform services. AWS and GCP follow NIST SP 800-88 for media sanitization.

Incident Response:
Workiva's standard agreement includes that Workiva maintains an incident response policy with procedures to provide the Customer with reasonable assurances that Workiva responds to any type of security event or breach, which includes:

1. Roles and responsibilities with a team and a dedicated leader which is tested annually;
2. Methods for investigation and escalation assessing the event to determine the risk the event poses including proper escalation;
3. Processes regarding internal communications, reporting and notification and external reporting and notification to customers within forty-eight (48) hours of unauthorized disclosure of or access to Customer Data. Workiva's standard is forty-eight (48) hours to allow for enough time to gather information and provide a coherent message, but willing to discuss twenty-four (24) hours if required.
4. Appropriate documentation of the event, incident and investigation of what was done and by whom with authorization for later analysis and possible legal action; and,
5. An audit of the incident conducting root cause analysis and remediation.

2.4.4	**Technical Support**
1	Explain any limitations that exist with your cloud solution. For example (**not** a complete list): • Number of concurrent users on the system • Storage restrictions and or limitations • Licensing restrictions • Realm of responsibility of your company vs. third-party cloud hosting vendor

The Workiva platform is designed to handle significant growth in an elastic manner, leveraging Google and Amazon's cloud services and providing a highly scalable and capable tool for customers and their data. In addition, Workiva's solution-based license (SBL) model includes unlimited users and data. The SBL model enables the DOR to easily expand and scale without having to revisit pricing or number of licenses.

2	Explain how your solution manages user identity, access, and permissions.

The Workiva platform provides a robust role-based authorization lattice. The platform provides four administrative roles: Org Security Admin, Org User Admin, Org Workspace Admin, and Workspace Owner. The platform enables the DOR to create workspaces. Workspaces provide separate places for entities, departments or teams to collaborate in secure, controlled spaces. Within a workspace, the platform provides additional roles and the ability to create groups to restrict access. The platform also provides advanced permissions within documents, spreadsheets, and presentations to limit access to specific sections, cells, and slides based on user or group. The Workiva platform only requires a modern web browser and an internet connection for users to securely connect and work together. Workiva is compatible with Internet Explorer, Firefox, Safari, and Chrome. Workiva recommends the latest browser versions Google Chrome and Microsoft Edge Chromium.

3	Describe your customer support model, including: a. Your company's standard process for problem resolution b. Standard response times c. Escalation process if the standard resolution process cannot resolve an issue d. Service Levels and how you report on your effectiveness in meeting those Service Levels e. Actions your company will take if the Service Levels are not met

Workiva offers a SBL model that includes support throughout the life of the contract. The SBL includes a dedicated CSM, premium support based in the continental United States, and access to a variety of training

resources. Lastly, Workiva adheres to a detailed Service Level Commitment (SLC) that is provided as an attachment with the response, and highlights of the SLC are noted below.

Support Response Times: Workiva uses commercially reasonable effort to correct or provide reasonable workarounds to address all material errors that are identified in the platform. Any reported error or issue is classified (i.e., critical, urgent, standard) according to defined criteria and the classification corresponds with a detailed Workiva response timeframe (e.g., 30 minutes, 2 hours, etc.). For example, Workiva support responds to a critical error within 30 minutes, and works to correct the issue or provide a reasonable workaround, providing status updates every two hours.

Workiva's **service availability commitment** is as follows: The Software will be available 99.5% of the time, measured on a quarterly basis. Availability shall be calculated for the measurement period by dividing (a) the Baseline Uptime less Unscheduled Downtime by (b) the Baseline Uptime for the same period. In the event that the availability of the Software for the applicable measurement period is below standards, the DOR is eligible for service credits. The SLC, included as an attachment with the response, details eligible service credits according to Software availability.

Customer Success Manager: The CSM is a single person dedicated to the DOR for the life of the contract. The CSM is the DOR's strategic partner, and helps the DOR identify opportunities, shares use case leading practices, coordinates user training and adoption, and schedules recurring strategic meetings.

Support Team: In addition to the CSM, the DOR has access to Workiva's 24/7, world-class Support team, as well as the Success Center, which includes The Learning Hub (online courses), a Help site (hundreds of articles and video tutorials on the platform) and Community (where you can converse with other Workiva customers, ask questions, post answers, etc.). Lastly, Workiva hosts an annual user conference called Amplify. Amplify brings together thousands of users and provides training, professional development sessions, CPE credits.

Hosting and Platform Maintenance: Workiva manages all maintenance, updates and upgrades in a manner that does not typically require downtime or disruption to the DOR. There are no additional costs for ongoing maintenance, updates or upgrades. Platform updates and upgrades are released regularly (e.g., daily, weekly).

Please refer to '2.4.2 Appendix - Workiva Service Level Commitment' for detailed service level commitment.

4	Describe your application's maintenance model, including common schedule for changes and new features, and how customers are notified.

Workiva uses a defined **Software Development Life Cycle (SDLC)** with an emphasis on functionality, quality, responsiveness, and security. This systematic approach includes a process to confirm that any changes to systems or applications are thoroughly reviewed, tested, approved, and well communicated.

The SDLC employs **Agile** software development practices designed to be nimble and responsive with customers and the market. Research & Development teams prioritize their work and maintain a queue of work that is planned and in-progress. Teams meet regularly to review their work with the larger organizations, hold planning meetings, and hold retrospectives to review how they are working as a team and identify performance improvements going forward. Many teams also hold stakeholder meetings where they invite stakeholders to provide their input on the future direction.

Updates to the Workiva platform are released on a regular basis as work is completed. Release Management verifies completion of all SDLC requirements for any code before it is used in the production environment.

Future Products and Services: Workiva has a history of reinvesting in the platform to keep pace with customer needs, industry trends and regulations. In 2020 Workiva reinvested 33% of revenue, approximately $90 million dollars into platform research and development. In addition, the dedicated CSM communicates new features, updates and upgrades to the DOR, and the information is available through the Support Center.

Platform Maintenance and Upgrades: Workiva manages all platform maintenance, updates and upgrades with no downtime or disruption to the DOR. This support is part of the annual subscription fee, and updates and upgrades are released regularly (e.g., daily, weekly).

Platform Requests and User Groups: Workiva's Support Center includes a component called Community. Community is where Workiva platform users can connect with other customers to ask and post questions and submit software feedback and requests. In addition, Workiva hosts an annual conference for customers to connect, collaborate and discuss industry leading practices. Lastly, Workiva uses a Customer Issue Resolution Process and has a team of Feedback Managers (FM). FM moderate all the feedback that comes in, ensuring customers feel their voice is heard, and their CSM is aware of their request. They also create and link up any tickets, establishing the connection that keeps the CSM and FM, and in the end, the customer up-to-date as their feedback progresses.

5	Describe your disaster recovery (DR) strategy.

The Workiva platform is a software as a service (SaaS) solution, and Workiva tests data recovery capabilities as part of an overall disaster recovery and business continuity plan. A copy of Workiva's Business Continuity and Disaster Recovery Plan and Annual Test for Business Continuity and Disaster Recovery 2020 are available upon request.
Workiva production databases are replicated in real-time to physically separate data center locations while binary logs record all database activity in order to provide point-in-time recovery. Backups are retained for thirty (30) days, and are always stored encrypted-at-rest (AES-256). Workiva platform editor provides detailed document history and revision control enabling a user to recover or compare against any past revisions. Workiva performs a fail-over test annually to test our defined Recovery Point Objective (RPO) 24 hours and Recovery Time Objective (RTO) 8 hours, and test results are available upon request. Restore testing of backups is completed annually.

Deloitte has a formal business continuity and disaster recovery plan. Deloitte's Disaster Recovery and Business Continuity plans are considered confidential and cannot be shared outside of Deloitte. Please refer to the next question below as well as 2.3.11 Attachment - Deloitte Approach to Confidentiality - An Overview for a high-level overview of our security program and controls

6	If awarded this RFP, describe the responsibilities, actions, and methods that your company would perform to return DOR's data, and the format of the data, if DOR chooses to disengage with your company later.

At any time the DOR can save/export data from the Workiva platform. Workiva enables the DOR to self-administer data and data governance requirements for all workspaces. The DOR is the owner of all DOR data within the platform. Workiva can assist the DOR with saving/exporting data to a local DOR drive, and the DOR would be able to migrate its data at any point it so chooses. The DOR can migrate its data out of the platform as needed or desired. The Workiva platform exports data as Microsoft files (e.g., Word, Excel, and PowerPoint), CSV (for spreadsheets), and PDF. The Wdata portion of the platform functions with CSV, JSON, XML, and connector specific data. Upon contract termination, Workiva offers the DOR 30-day access to save/export any data from the platform.