

Date: November 25, 2025

To: Brian Sargent

From: Chuck Nicholas

Subject: Sole Source Request: C015148 Kainos Smart Audit

Amount: \$79,800 per year x 3-year contract = \$239,400

Dept. Statement: The product is Kainos Smart Audit, an automated, specialized monitoring and compliance system that works exclusively with our Workday platform.

Department Requirements: UCF-IT desires to automate many manually performed Workday security audits, thereby increasing the security of sensitive data and reduce exposure to financial loss or data breach, while reducing IT staff workload performing manual reactive audits. Systems specifications require full compatibility with Workday; therefore, any solution considered will require certification by Workday of full compatibility with Workday's platform. Functional requirements include automated monitoring of segregation of duty compliance; a full suite of ready to deploy Service Organization Controls (SOC); AI-driven security group permission assessments; and monitoring of business process changes for risk.

Research Conducted: UCF-IT constructed a comparison matrix with these four required specifications and compared the Kainos system to competitive products from Pathlock and SailPoint. Only the Kainos system meets all four critical requirements. Kainos also has "built on Workday" certification, meaning that Workday has certified the platform, which was built on the Workday system architecture, as fully compatible with the Workday suite of products as used at UCF.

Proposal Analysis: Kainos has offered a three-year flat rate Smart Audit subscription service at \$79,800 per year (\$239,400 3-year term) based on 7600 FSE¹ which works out to \$10.50 per FSE. By comparison, Florida Gulf Coast University confirmed they are paying \$58,000 per year to Kainos for 1800 FSE, or \$32.22 per FSE. Kainos also charged FGCU a \$10,000 onboarding fee but waived this fee for UCF.

Searching GovSpend produced several orders for Kainos from The Ohio State University for the testing software, but not the Smart Audit package. UC-San Diego also purchased the testing software. The Hillsborough County Sheriff's Office purchased the Smart Audit service via a waiver in 2024. Source documents were not available for review.

Recommendation: It is clear the Kainos product is uniquely positioned as a Workday-approved software package that meets the critical requirements set forth by UCF-IT. UCF is also receiving favorable pricing compared to other SUS entities. I recommend we approve this sole source as requested.

¹ Full-Service Equivalent; a Workday metric for users

Re: Kainos Smart Audit - Sole Source Approval

From Albert Francis <Bert.Francis.III@ucf.edu>

Date Thu 12/4/2025 9:29 AM

To Joel Levenson <Joel.Levenson@ucf.edu>

Cc Brian Sargent <Brian.Sargent@ucf.edu>; Chuck Nicholas <charles.nicholas@ucf.edu>

I agree!

Bert

Bert Francis, CPA

Acting Chief Financial Officer
University Treasurer
Administration and Finance
University of Central Florida
4635 Andromeda Loop N
MH384
Orlando, FL 32816
Tel: (407) 882-1075
Email: Albert.Francis@UCF.Edu

From: Joel Levenson <Joel.Levenson@ucf.edu>

Sent: Thursday, December 4, 2025 8:39 AM

To: Albert Francis <Bert.Francis.III@ucf.edu>

Cc: Brian Sargent <Brian.Sargent@ucf.edu>; Chuck Nicholas <charles.nicholas@ucf.edu>

Subject: FW: Kainos Smart Audit - Sole Source Approval

Good morning Bert,

I also support this sole source. Research into other suppliers shows that they can not provide the required specifications, especially WD certification.

If you agree, reply all and indicate as such. If you have additional questions, let me know.

Thank you,

From: Brian Sargent <Brian.Sargent@ucf.edu>

Sent: Wednesday, December 3, 2025 12:04 PM

To: Joel Levenson <Joel.Levenson@ucf.edu>

Cc: Chuck Nicholas <charles.nicholas@ucf.edu>

Subject: Kainos Smart Audit - Sole Source Approval

Hi Joel,

I also support this sole source for Kainos Smart Audit submitted by David Canova. Attached are the relevant documents and Chuck's initial write up.

Supplier: Kainos Smart Audit

Department: Enterprise Applications and Data Systems

Amount: \$239,400 over 3-years

Description: Kainos Smart Audit is a proprietary, Workday-certified automated audit and testing solution that integrates directly with our Workday tenant. It provides real-time monitoring, configuration audits, and automated testing capabilities that no other vendor offers with the same level of Workday certification or compatibility. Smart Audit is required to ensure compliance, reduce risk during Workday updates, and maintain continuous oversight of our Workday configuration

Research into other products: Research was conducted into other known products but only Kainos meets all the requirements including:

1. Only product that works exclusively with our Workday platform as a "Built on Workday" Certified Application"
2. Out-of-the-Box SOC-Certified Control Library (150+ Workday-specific)
3. AI-Driven Anomaly and Privileged Access Detection

Price Reasonableness: David benchmarked with FGCU to ensure our pricing is fair and reasonable, and we are getting a much better deal per FSE and onboarding at no cost.

Please approve/disapprove and let me know if you have any questions.

Regards,

Brian



SOLE SOURCE CERTIFICATE AND POSTING NOTICE

(Greater than \$150,000)

A sole source procurement is when you make a request to purchase product(s) and/or service(s) without competition when competition is otherwise required. This means that product/service is unique and that the supplier is the only supplier that can provide the product or service. In accordance with the authority granted under applicable Florida law and UCF Regulation 7.130, the following documentation is submitted in support of this request.

This form and related documentation shall be submitted through Workday Help using case type Waivers and Sole Source. Please do not attach to a requisition or send via email for review and approval.

WD case subject title should have common structure for easy tracking, to include:

- Exemption type (Sole Source)
- Supplier name
- Purchase amount

The completed sole source must be approved in the following order. **Please be sure to obtain all required signatures before submitting the form to Procurement Services.**

- PI/Researcher/Director/Chair
- President/Vice President/Dean
- Procurement Specialist
- Procurement Services Manager or Associate Director
- Assistant Vice President for Tax, Payables & Procurement, who will review and provide a recommendation to approve or disapprove the sole source to:
- Chief Financial Officer, who will either directly approve or disapprove the sole source, or forward it to the Provost and Executive Vice President for goods/services related to academia for input prior to making the final decision.

Once the completed sole source is received, Procurement Services in collaboration with kNEXT reviews the documentation provided and determines whether the sole source is valid or if there are additional suppliers that may be able to provide the requested product or service. The sole source review and approval process varies based on the nature of the product/service being requested and the information provided in the requestor's justification, among other factors, so please keep this in mind when submitting the form.

Contingent upon the approval of all the officers/individuals listed, the sole source shall be posted on the UCF Procurement Services website for seventy-two (72) hours. Upon expiration of said posting period, Procurement Services will process a purchase order upon receipt of the requisition.

The usual bidding process shall be conducted if sole source approval is not granted.

PART I: DEPARTMENT AND SUPPLIER INFORMATION

Department Name: UCF IT Contact & Phone: David Canova 4078235065

Product/Service Cost: 239400

☐ One Time Purchase ☐ Term Contract: _____

☒ Multiple Purchases ☒ Duration: 3 years

Company Name: Kainos Email: b.armstrong@kainos.com

Contact Person: Bradley Armstrong Title: Account Executive

Product and/or Service: Kainos Smart Audit

PART II: SOLE SOURCE JUSTIFICATION (see pages 4-5)

Only justifications submitted on this form and in the below format will be reviewed for approval. All the listed points **MUST** be fully answered on the following pages and any additional attached pages as needed. Failure to submit justification as outlined in the format below will **result in the form being returned without review.**

PART III: SOLE SOURCE CERTIFICATIONS

- A. In my professional opinion, this is the only product or service that can reasonably meet my requirement(s)/specification(s), and this is the only supplier who can provide the product or service. I further certify that the information contained herein is true and correct to the best of my knowledge and belief and would withstand any audit or supplier protest.
- B. I, the undersigned, certify that I and/or the user do not have a financial interest in the above named supplier or contractor, and that I am unaware of any conflict of interest related to this purchase.

dcanova
Digitally signed by dcanova
Date: 2025.11.07 11:00:58
+05'00'

Signature

David Canova

Printed Name and Title (PI/Researcher/Director/Chair)

11/7/2025

Date

Bill Poirier
Digitally signed by Bill Poirier
Date: 2025.11.12 17:18:26
+05'00'

Signature

William Poirier Chief Information Officer

Printed Name and Title (President/Vice President/Dean)

(Delegations not allowed; emails from absent approvers are acceptable)

11/12/2025

Date

I, the undersigned, hereby concur with the above justification and support a sole source approval for the above product(s) and/or service(s). Approvals may be documented and supported via email.

Charles D. Nicholas
Digitally signed by Charles D. Nicholas
Date: 2025.11.25 11:41:19
+05'00'

Signature

Charles D. Nicholas

Printed Name and Title (Procurement Specialist)

11/25/2025

Date

See attached email

Signature

**Printed Name and Title
(Procurement Services Manager or Associate Director)**

Date

See attached email

Signature

**Printed Name and Title
(Asst. Vice President for Tax, Payables & Procurement)**

Date

Signature

Printed Name and Title (Chief Financial Officer)

Date

POSTING NOTICE

12/4/2025 1:00pm

Date/Time Posted

12/8/2025

Posting End Date

2604

UCF Control No.

Chuck Nicholas

Procurement Specialist

SOLE SOURCE JUSTIFICATION

Please answer the questions below and attach additional documentation if needed.

1. Describe the product(s) and/or service(s) and anticipated use thereof in layman's language.

See Attached

2. Describe the required specifications or requirements and why are they essential to the accomplishment of your work.

See Attached

Provide the names of other suppliers, products and/or services that you have investigated and explain why they do not meet the required specifications or requirements. It may be helpful to present your information in a table like the one below.

Required Specifications	Supplier 1	Supplier 2	Supplier 3	Supplier 4
	Y/N	Y/N	Y/N	Y/N
	Y/N	Y/N	Y/N	Y/N
	Y/N	Y/N	Y/N	Y/N
	Y/N	Y/N	Y/N	Y/N

See Attached.

3. State in detail why only this and no other product(s)/service(s) will satisfy the department's requirements. Description may include unique features, compatibility, specifications, availability, delivery time frame etc. (For example, please list the features or special conditions that are unique and only available from one supplier. Note: Price is not a valid reason.)

See Attached.

4. Are there resellers or distributors? If yes, please list names and contact information.

SHI

5. Will this purchase obligate UCF to this vendor for future purchases such as maintenance, licensing, or continuing need? ☒ Yes ☐ No

If yes, please provide details regarding future obligations and/or needs to include number of years and total spending amount of obligations:

3 year Subscription Service Charge (Annual) at \$79,800

6. What efforts have been made to obtain the best pricing available? Please provide an explanation to support the belief that the price is fair and reasonable.

Peer Institution Price Benchmarking: The university actively compared the proposed subscription price against contractual rates paid by other higher education institutions utilizing Kainos Smart Audit. This benchmark confirmed that our pricing aligns with or is better than the industry standard for a public university of our size and complexity.

1. Describe the product(s) and/or service(s) and anticipated use thereof in layman's language.

The product is Kainos Smart Audit, an automated, specialized monitoring and compliance system that works exclusively with our Workday platform.

Description: Workday is the central system that manages the university's human resources, payroll, and financial processes. It holds our most sensitive employee and financial data. Due to its complexity, we must continuously monitor Workday to prevent fraud, fix security flaws, and ensure we comply with legal requirements like SOX (financial reporting) and data privacy laws.

Kainos Smart Audit acts as our dedicated, electronic security and compliance officer living inside Workday. Instead of our staff spending weeks manually pulling reports to check security, this automated tool performs four essential, continuous checks:

1. Stops Bad Combinations (Segregation of Duties - SoD): It constantly watches to prevent any single person from gaining too much power—for example, the ability to both create a vendor payment and approve that payment. This is key to preventing internal fraud.
2. Validates User Access: It automatically checks every user's security permissions against their current job duties, using AI to instantly flag any access that looks inappropriate, especially as staff roles change.
3. Monitors System Changes: It tracks all high-risk changes made to Workday's configuration (its "rules"). This ensures our security and financial controls are not accidentally or maliciously disabled during system maintenance or updates.
4. Detects Risky Behavior: It constantly monitors for suspicious user activity, such as unauthorized attempts to view sensitive employee data, which helps us proactively prevent data breaches.

Anticipated Use: The university will use this product to move away from slow, reactive audits to continuous, automated compliance. This process is crucial for maintaining our Workday operational governance framework, significantly reduces our risk of financial loss and data exposure, and frees up our technical and Business Subject Matter Expert staff to focus on strategic work rather than manual compliance checks.

2. Describe the required specifications or requirements and why are they essential to the accomplishment of your work.

The required specifications are mandatory technical controls necessary to manage risk, ensure continuous compliance, and maintain the integrity of the university's Workday system in line with our operational governance framework. These cannot be met through manual processes or non-native solutions.

Required Specification 2.1: Native Integration and Certification as "Built on Workday." Essential Rationale: Workday is a highly specialized enterprise system that undergoes complex, bi-annual updates. We require a solution certified by Workday that is built on the Workday platform. This is essential to guarantee seamless, non-breaking integration with Workday's proprietary security model and data structures. Without this native certification, any third-party tool is at high risk of failure or data incompatibility, which would immediately halt compliance monitoring and expose the university to significant risk.

Required Specification 2.2: Automated, Continuous Monitoring for Segregation of Duties (SoD). Essential Rationale: This is a non-negotiable requirement for IT General Controls (ITGC) and SOX compliance. We must have an always-on, automated system that instantly identifies and prevents toxic permission combinations—such as a user who can create a fraudulent

payment and then approve it. Manual checks are too slow and resource-intensive to provide this continuous level of financial protection.

Required Specification 2.3: Comprehensive Out-of-the-Box SOC-Certified Control Library. Essential Rationale: To achieve immediate audit readiness and compliance, we require a vendor-supplied library of at least 150 pre-built, SOC-certified controls that are pre-mapped to the complexities of Workday's security and business processes. Custom-building this specialized library would cost hundreds of thousands of dollars and take years of effort by technical Business Subject Matter Experts, which would delay our compliance efforts unacceptably.

Required Specification 2.4: AI-Driven Anomaly and Privileged Access Detection. Essential Rationale: Simple rule-based auditing is insufficient. We require advanced, specialized AI technology that can analyze complex access data in Workday to proactively flag subtle, anomalous security group permissions. This is essential for identifying and mitigating high-risk vulnerabilities, protecting sensitive PII, and preventing sophisticated access abuses that standard Workday reporting cannot detect.

Required Specification 2.5: Automated Configuration Change Control Monitoring. Essential Rationale: Workday's configuration is highly dynamic. We require continuous monitoring that instantly flags any high-risk changes to business processes or system settings. This ensures the university maintains system stability, prevents disruptions to critical operations, and guarantees that our compliance controls remain intact despite ongoing system maintenance and updates.

Provide the names of other suppliers, products and/or services that you have investigated and explain why they do not meet the required specifications or requirements. It may be helpful to present your information in a table like the one below.

Required Specifications	Kainos Smart Audit (Proposed Solution)	Supplier 1: Pathlock (GRC/SoD Platform)	Supplier 2: SailPoint (Identity Governance)
1. Native Integration as "Built on Workday" Certified Application	Y	N	N
2. Automated, Continuous Segregation of Duties (SoD) Monitoring	Y	Y (Via Connector)	N (Focus on Access Cert)
3. Out-of-the-Box SOC-Certified Control Library (150+ Workday-specific)	Y	N	N
4. AI-Driven Anomaly and Privileged Access Detection	Y	N (Rule-based)	N (General Access AI)

3. State in detail why only this and no other product(s)/service(s) will satisfy the department's requirements. Description may include unique features, compatibility, specifications, availability, delivery time frame etc. (For example, please list the features or special conditions that are unique and only available from one supplier. Note: Price is not a valid reason.)

Only Kainos Smart Audit can satisfy the university's requirements because it is the only continuous, automated audit and compliance product natively certified by Workday. This grants it a unique technical and operational advantage that no other vendor or service can replicate, ensuring uninterrupted security and compliance for our mission-critical platform.

The core necessity is a system that can continuously maintain our Workday operational governance framework. No other product or service delivers the following mandatory, unique features:

1. Unique Feature: Guaranteed Compatibility ("Built on Workday" Certification)

- Unique Condition: Kainos Smart Audit is the only solution in this domain that holds the prestigious "Built on Workday" certification. This status means the application is built using Workday's proprietary framework, guaranteeing the deepest level of technical integration with Workday's security model, data structures, and bi-annual update cycle.
- Why Others Fail: General Identity Governance (e.g., SailPoint) and GRC tools (e.g., Pathlock) connect to Workday via standard, external connectors. These external connections are highly vulnerable to breaking after Workday's mandated updates, leading to compliance outages. The university cannot risk a disruption in audit monitoring that would leave us exposed to fraud and regulatory non-compliance.

2. Unique Feature: Productized, SOC-Certified Control Library

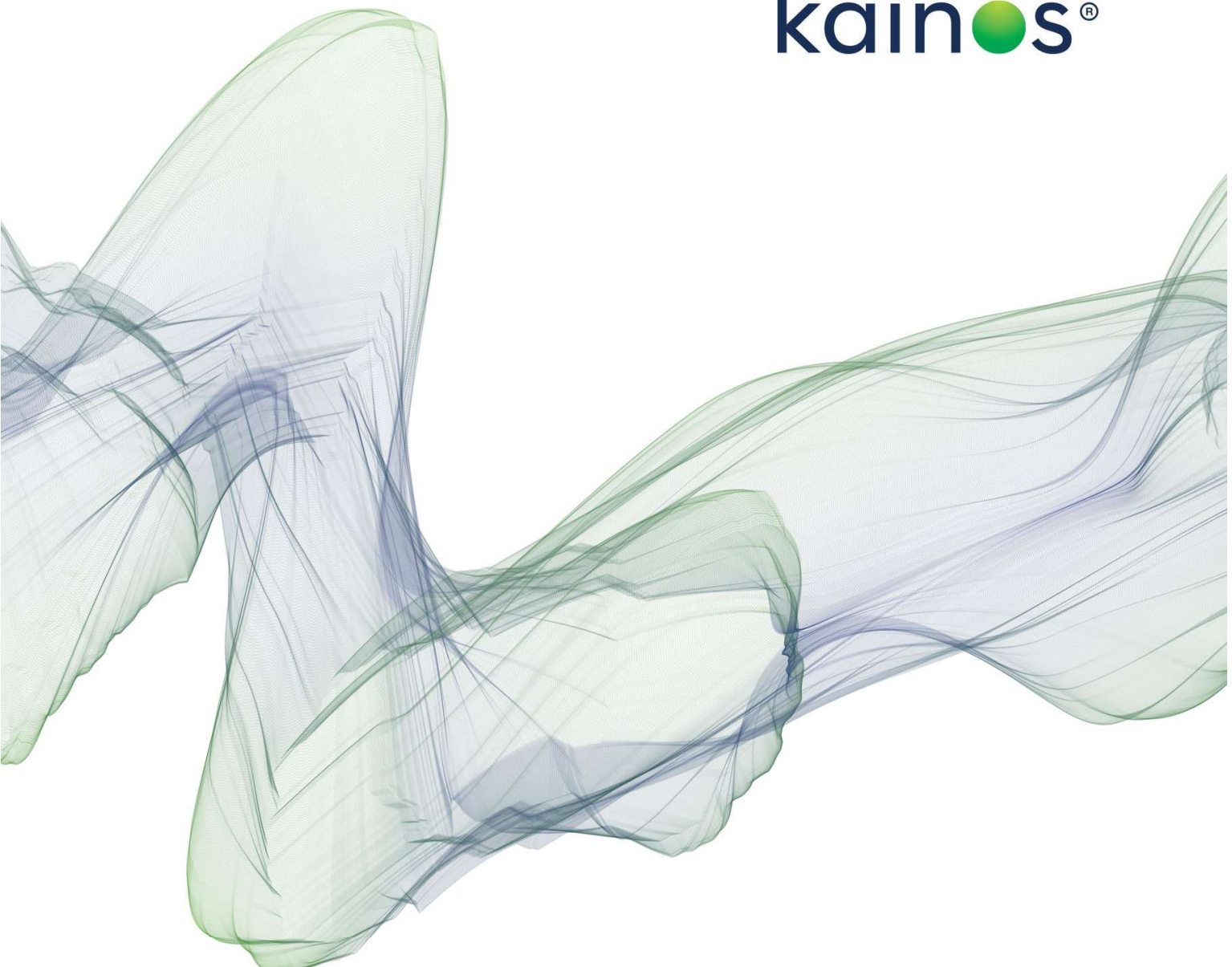
- Unique Condition: The product comes with a ready-to-deploy library of over 150 SOC-Certified controls that are pre-mapped to the specific complexities of Workday's Financials and HCM modules, including all key Segregation of Duties (SoD) scenarios.
- Why Others Fail: Competing GRC platforms offer generic rulesets that require thousands of hours of customization and consulting work by Business Subject Matter Experts to accurately translate into Workday-specific controls. Services like manual consulting would require starting from scratch every year. This pre-built, certified library ensures immediate audit readiness, cutting implementation time from years to minutes, and is not offered by any alternative.

3. Unique Feature: Proprietary AI-Driven Risk Analysis

- Unique Condition: Kainos Smart Audit uses proprietary Artificial Intelligence (AI) specifically trained on the Workday security model to perform AI-Driven Anomaly Detection. This capability goes beyond simple rule-based checking (which competitors primarily use) to proactively identify subtle, high-risk access combinations and privileged user behaviors that are technically compliant with the rules but pose a severe security vulnerability.
- Why Others Fail: Neither general IGA platforms nor manual services possess this specialized, built-in AI intelligence to detect *anomalous* risks within Workday's complex security group structure. This advanced detection capability is crucial for protecting sensitive data (PII) and preventing insider threats.

4. Unique Condition: Availability and Delivery Time Frame

- Unique Condition: As a cloud-native, specialized product, Kainos Smart Audit can be provisioned and activated in less than two hours (as per vendor specifications), providing immediate value and continuous risk detection.
- Why Others Fail: Implementing or integrating a non-native GRC tool (like Pathlock or SailPoint) to achieve comparable depth of control requires a custom, multi-phase IT project typically lasting 6 to 18 months, which is a delay the university cannot afford given its continuous regulatory and compliance obligations.



Kainos Subscription Service Order Form

Status
Security
Version No.

Definitive
Confidential
5.0

KAINOS SUBSCRIPTION SERVICE ORDER FORM

Customer Details					
Customer Name	University of Central Florida				
Registered Office Address	4000 Central Florida Blvd, Orlando, FL 32816				
Customer Contact, Phone, Email	David Canova, 407.823.5065, David.Canova@ucf.edu				
Invoice Contact, Phone, Email	TBC				
Hosting Platform	USA				
Kainos Details					
Kainos Name	Kainos WorkSmart Inc				
Registered Office Address	Suite 4300, 111 Monument Circle Indianapolis, Indiana 46204, USA				
Kainos Contact, Phone, Email	Bradley Armstrong, +447885667488, b.armstrong@kainos.com				
Contract Reference (PID)	P216486				
Subscription Term					
Start Date	Day	01	Month	01	Year 2026
End Date	Day	31	Month	12	Year 2028
Subscription Service	Modules	Selected	Built on Workday		
Smart Audit Subscription Service	Segregation of Duties	✓	✓		
	Privileged Access & Security Design Validation	✓			
	User Activity Monitoring	✓			
	Configuration Change Detection	✓			
Smart Shield Subscription Service	N/A	☐			
Smart Test Subscription Service	Advanced Compensation	☐			
	Financials	☐			
	HCM	☐			
	Payroll	☐			
	Recruitment	☐			
	Security	☐			
	Talent and Performance	☐			
	Learning	☐			
Kainos EDM	N/A	☐			
Charging Band(s)					
Staff Number (FSE)	Subscription Service Charge (Annual)				
Up to 8,000	\$79,800				☒
8,001 – 10,000	\$91,800				☐
10,001 – 15,000	\$97,800				☐
Summary of Charges					
Services	Invoice Amount	Frequency	Duration	Total	
Choose an item - Audit	\$79,800 per annum	Annually in advance	3 years	\$239,400	
Total Charges				\$239,400	
Customer			Kainos		
Signature			Signature		
Print Name		Print Name			
Title		Title			
Date		Date			
The Order Form and the Terms of Use are accepted on signature.					

SUBSCRIPTION SERVICE DESCRIPTION

Smart Audit is a “Software as a Service” (SaaS) solution designed to enhance IT compliance, security, and operational efficiency within Workday environments. Smart Audit addresses critical pain points related to security, compliance, and efficiency by offering robust tools for internal control, compliance, and fraud prevention.

- Smart Audit is designed to highlight potential risks in Customer’s Workday configuration by identifying instances of specific, pre-defined scenarios in one or more Workday tenant(s). The following features are available to all Smart Audit subscribers.
- Using Workday integrations and “Reports as a Service” (RaaS), Smart Audit evaluates a Customer’s Workday Tenant configurations and identifies potential risks via our proprietary **“audit checks”** functionality and raises **“cases”** if configuration scenarios arise that meet audit check criteria.
- Smart Audit includes **preventive audit checks** that analyze and report on configuration(s) and Smart Audit includes **detective audit checks** which analyze and report on activity that has occurred in the customer’s tenant. Additionally, audit checks available within Smart Audit are defined as follows:



Fixed Scope Checks

These checks are specific non-modifiable audit checks designed to detect specific configuration(s) that exist in a Customer’s Workday tenant. Fixed scope checks are included as a part of the basic Smart Audit subscription but can be deactivated by the customer. The customer only has access to the fixed scope checks for each module subscribed to.



Customized Check Capability

Customers can configure custom audit checks within each module they subscribe to.



Core/Expansion Risk and Control Matrix (RACM)

This proprietary bank of audit checks is designed and maintained by Kainos’ Workday Smart Audit product, audit advisory and services team. Customers can choose which checks from the RACM to deploy within their tenant(s). This artefact is provided to the customer at the time of onboarding. The use of Kainos’ risk and control matrix is optional.

- **Customers decide which audit checks to run, which Workday tenants (including Production tenants) to run checks against, and how often to run audit checks.**
- Scheduling and audit check configuration can be performed by the Customer.
- Kainos Smart Audit includes a **case workflow** to help customers manage the cases that arise, and document actions taken or link to external systems.
- Kainos Smart Audit features **.csv export** functionality and a **report generation engine**, enabling the execution of predefined reports and the export of these reports in Excel or JSON format.
- Kainos Smart Audit includes a **re-certification** feature which allows Customers to create flexible, time-bound recertification **schedules for preventive checks**.

Smart Audit is divided into several modules, each targeting specific aspects of IT compliance and security. Customers may purchase and deploy a single **Smart Audit module, all modules, or a bundle.**



Smart Audit Modules

Segregation of Duties (SOD)

Smart Audit enables customers to identify potential SoD violations and accept, remediate, and/or maintain oversight of which users hold such access via case workflow. Accepted SOD cases can be periodically re-certified in alignment with the Customer's policies/controls. Smart Audit automates essential SOD checks, eliminating manual processes and providing a library of ready-to-run controls. This module helps minimize fraud and errors, ensures compliance with regulatory requirements, and improves operational efficiency. By streamlining audit processes, it reduces the time and effort required to diagnose and resolve risks.

If subscribed to this module, Customers can create custom checks in this module, have access to all SOD RACM checks, and access to this fixed scope check:

- **SoD - Business Process Definitions with No Approval Steps**
 - This check will identify any Business Process Definitions in the tenant which have no approval steps within them.

Privileged Access & Security Design Validation

This module helps the customer report on and evaluate the appropriateness of privileged access in Workday via Smart Audit's case workflow. Smart Audit dynamically identifies which security groups enable workers to perform privileged actions or to see privileged data per the Customer's defined scope. Smart Audit provides review capabilities for Security Group membership, which enables Customers to view and evaluate a list of all workday accounts with access to any Workday Security Groups (including up to 5 combinations of groups), per the Customer's Security Group scope. Accepted privileged access cases can be periodically re-certified in alignment with the Customers' policies/controls.

If subscribed to this module, Customers can create custom checks in this module, have access to all privilege access RACM checks, and access to these fixed scope checks:

- **Super User Access - Active Implementers**
 - This check returns every active implementer account to the target tenant and enables monitoring and control of implementer access.
- **General Access Control – Inactive Accounts with User Based Access**
 - This check strengthens offboarding processes by identifying inactive workday accounts which are currently assigned to User Based security groups.
- **General Access Control - Workers who are their own Manager**
 - This check will identify any workers who are their own manager, or who appear somewhere within their own management chain.
- **General Access Control - Integration Accounts with UI Access**
 - This check returns all ISU accounts within the tenant with the permission to login via UI, providing control and visibility of these permissions.

User Activity Monitoring

Checks in this module are designed to detect and flag events that could indicate an abuse of privileged access when a Workday account views sensitive worker profile data such as Personally Identifiable Information (PII). Sensitive worker profile information is defined by the customer. These checks provide detailed information on who performed the activity, what was viewed, when it occurred, where it happened, and how the activity was carried out via case workflow. If subscribed to this module, Customers can create custom checks in this module, have access to all data privacy RACM checks, and access to these fixed scope checks:

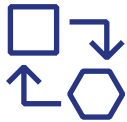
- **Sensitive Activity - Integration Account UI Logins**
 - This check detects any occurrence of an integration user account logging into a workday tenant via the UI.
- **Sensitive Activity - WD-Support and WD-Developer Logins**
 - This check detects and returns every instance of wd-support and wd-developer account logins on the tenant.

Configuration Change Detection

Checks in this module monitor key objects within Workday and alert customers when changes to those objects occur or when tasks are executed that which could enact configuration changes in Workday. This enables customers to detect when key changes happen across their Workday configuration and core Workday objects such as Business Processes. Customers can assess those changes for appropriateness and tie them back to authorized change activities (i.e., change tickets) via case workflow.

These checks provide visibility into who performed the change and the attributes of what was changed.

If subscribed to, Customers can create custom checks in this module and have access to all RACM checks.



Customer's Use of Kainos Smart Audit

Each module of Smart Audit is designed to streamline IT general control processes, provide on-demand compliance, and build confidence and trust in Workday environments. By leveraging automation, AI, and continuous monitoring capabilities, Smart Audit ensures organizations can effectively manage their IT compliance and security needs.

The Customer will:

- Directly configure and run Kainos Smart Audit including and pre-requisite configuration to connect to Customer's Workday tenant/s as outlined in the Kainos Smart Audit User Guide.
- Log into Kainos Smart Audit and take responsibility for interpreting results and deciding what action is appropriate in response to such results.
- Maintain and update Kainos Smart Audit configuration to meet organisation's requirements.
- Create and maintain User access to Kainos Smart Audit.
- Be responsible for all other activities which would be associated with day-to-day use of the product.
- Ensure that relevant employees participate any training provided by Kainos, to assist with the set-up and use of Kainos Smart Audit.

Kainos Smart Audit is intended to be used to supplement Customer's existing risk and compliance controls. Customer acknowledges that the configuration of Kainos Smart Audit will determine the results that it produces for the Customer, within the remit of its Workday system. Kainos will not review, or be responsible for, results or actions taken using Kainos Smart Audit modules.

Kainos reserves the right to audit Smart Audit customer tenants to ensure compliance with the Service Description.

Kainos Smart Audit Onboarding

Kainos and Customer will assume the following roles and responsibilities during the onboarding of Kainos Smart Audit:

Smart Audit Onboarding	Responsible	Accountable	Consulted	Informed
Programme & Value Management				
Management of the rollout of Smart Audit across the customer organization	Customer	Customer	Kainos	Kainos
Defining goals and success Metrics for Audit	Customer/ Kainos	Customer	Kainos	Kainos
Planning				
Determine Customer project team/ primary contacts	Customer	Customer	Kainos	Kainos
Define deployment plan and timelines in collaboration with the Customer	Customer/ Kainos	Customer	Customer/ Kainos	Customer/ Kainos
Set up weekly calls and weekly project status reports	Kainos	Kainos	Customer	Customer
Appointing Customer Audit Admins, who will be responsible for managing the accounts in Smart Audit	Customer	Customer	N/A	Kainos
Defining scope - risk posture and controls	Customer	Customer	Kainos	Kainos
Configure				
Apply relevant risk posture and control monitored items to Smart Audit	Kainos & Customer	Kainos & Customer	N/A	N/A
Training & Assisted Review				
Establishing training sessions & assisted review	Kainos	Kainos/ Customer	Customer	Customer
Attendance training sessions & assisted reviews	Customer	Customer	N/A	Kainos
Deployment and management of cases				
Management of Smart Audit cases	Customer	Customer	N/A	Kainos
Changes to Workday environment	Customer	Customer	N/A	Kainos
Additional User Creation	Customer	Customer	Kainos	Kainos
Additional check scope during Implementation	Customer	Customer	Kainos	Kainos
Support				
Raising support tickets	Customer	Customer	N/A	Kainos
Fixing defects/issues identified and raised in Kainos Smart Audit, in line with defined Kainos Smart Audit SLA	Kainos	Kainos	N/A	Customer

Smart Audit Post-Onboarding

Smart Audit Onboarding	Responsible	Accountable	Consulted	Informed
Programme & Value Management				
Management of Smart Audit across the customer organization	Customer	Customer	Kainos	Kainos
Defining goals and success metrics	Customer/ Kainos	Customer	Kainos	Kainos
Support				
Raising support tickets	Customer	Customer	N/A	Kainos
Defined SLA's	Kainos	Kainos	N/A	Customer
Fixing defects/issues identified and raised in Kainos Smart Audit, in line with defined Kainos Smart Audit SLA	Kainos	Kainos	N/A	Customer
Regular value meetings	Kainos / Customer	Kainos / Customer	N/A	Customer
Tenant Management activities, including the below: - Provisioning new tenants - Scope updates and refinement - User Creation	Customer	Customer	Kainos	Kainos



Built On Workday

The following sections apply if the customer is agreeing to purchase a Built on Workday application or enabled module of Smart Audit. All apps and modules using the Built on Workday framework are subject to limitations of Workday, Built on Workday, and/or Extend. This may mean that certain feature requests are not possible.

The Built on Workday framework automatically updates customer app versions with new versions as they are released. This applies to all module and application instances listed below in customer's Implementation, Sandbox and Production environments.

Additional details of specific applications or modules are specified below.

Kainos Smart User Access Review (Kainos UAR)

Kainos UAR is an extension of the Smart Audit product which is designed to facilitate privileged access reviews, certification, and recertification directly within Workday via the Built on Workday framework.

Smart Audit enables users to identify and gain oversight of privileged security groups within their Workday tenant/s based on their Smart Audit configuration. Kainos UAR allows for review, certification and recertification of privileged access held by Workday users directly within the native Workday interface. This includes dashboarding and reporting on the review progress and historical detail.

Functionality Included:

- Kainos UAR provides administration functionality within the application, to configure the scope of Security Groups in your access review and to specify which Workday users perform the access review.
- Kainos UAR enables customers to specify additional Workday users (or groups of users) to perform approval steps through a Workday Business Process.
- Kainos UAR prompts the appropriate specified Workday users during an access review event, from within their Workday inbox to review or approve access.
- Kainos UAR gives dashboarding and reporting for current and preview review events which can be accessed inside Workday.
- Kainos UAR provides customers the ability to trigger an ad-hoc access review event in Workday, in whole or in part.
- Kainos UAR allows authorized users, such as Security Administrators, to trigger the access review cycles.
- A UAR review cycle can be configured to automatically launch the UAR based on customer's defined schedules. (Expected calendar Q1 2026)
- Access to the UAR business process, Dashboards & Reporting, UAR Scope and UAR execution functionality is fully configurable.

Auditability

Any changes made through the Kainos UAR application is available for users to query in Workday and in Smart Audit records an audit trail of changes that are indicated by the access review. This includes the user, the date, the time, actions suggested by the reviewer or notes left by the reviewer.

Additional Information

Post-deployment services relating to the configuration of Kainos UAR (e.g. relating to business process rules, security, triggering of review cycle events, and UAR retention policies, or re-deployment to new/additional implementation tenants) are out of scope for the purposes of Customer's subscription to Kainos UAR and will only be provided where Customer enters into a separate Order Form for the provision of Professional Services.

Customer Responsibilities within Kainos UAR

Kainos recommends that Customers have Implementation, Sandbox and Production environments to deploy the Kainos UAR app. Should a Customer decide to procure the Kainos UAR app and deploy additional tenants, the Customer is responsible for the provision and any costs associated with Workday tenants required for those additional tenants.

Customers are responsible for all activities associated with day-to-day use of the Kainos UAR application.

Customer's configuration of Smart Audit and the Kainos UAR application will determine which Security Groups, reviewers and approvers will be involved in reviews within Workday.

** If additional support or review is required post-deployment, a supplemental support agreement or additional delivery consultant hours can be purchased in packs of 20 hours at 75GBP/hour (1500), to be used over a specified time period.

User Access Review General Onboarding

BoW Support	Responsible	Accountable	Consulted	Informed
Programme & Value Management				
Management of the rollout of Built on Workday (BoW) application across the customer organization	Customer	Customer	Kainos	Kainos
Defining goals and success metrics for Built on Workday application	Customer/ Kainos	Customer	Kainos	Kainos
Planning & Discovery				
Determine customer project team/ primary contacts	Customer	Customer	Kainos	Kainos
Define deployment plan and timelines in collaboration with the Customer	Customer/ Kainos	Customer	Customer/ Kainos	Customer/ Kainos
Set up weekly workshop calls and weekly project status reports	Kainos	Kainos	Customer	Customer
Appointing Security Admins, who will be responsible for managing the BoW application in Workday	Customer	Customer	N/A	Kainos
Provide named Kainos staff timely access to tenants (IMPL, SBX and PRODUCTION) and any other relevant systems	Customer	Customer	Kainos	Kainos
Notify Kainos of critical processing activities, including activities that will impact the Workday system, and their associated timeframes as well as planned and unplanned system outages	Customer	Customer	Kainos	Kainos
Defining scope of requirements for BoW application & complete workbooks	Customer	Customer	Kainos	Kainos
Define knowledge transfer plan	Kainos & Customer	Kainos	Customer	Customer
Configure				
Configuration of initial scope within Smart product (if required)	Kainos & Customer	Kainos & Customer	N/A	N/A
Configuration of initial Workday functionality for BoW application - Domain - Business Processes	Kainos & Customer	Kainos & Customer	N/A	N/A

User Access Review General Onboarding (Continued)

BoW Support	Responsible	Accountable	Consulted	Informed
Testing				
Review and test BoW application functionality in lower tenant e.g. Smoke Testing	Kainos & Customer	Customer	Kainos	Kainos
Define and execute User Acceptance Testing strategy and plan	Customer	Customer	N/A	Kainos
Change Management				
Policy and procedure updates	Customer	Customer	N/A	N/A
Change management, communication and operational readiness planning and subsequent execution activities	Customer	Customer	N/A	Kainos
Deployment				
Functionality Sign Off	Customer	Customer	N/A	Kainos
Deployment to production	Kainos & Customer	Kainos & Customer	N/A	N/A
User training and communication	Customer	Customer	N/A	Kainos
Management of BoW application on Go Live	Customer	Customer	Kainos	Kainos
Support				
Raising support tickets	Customer	Customer	N/A	Kainos
Fixing defects/issues identified and raised in BoW application, in line with defined BoW application	Kainos	Kainos	N/A	Customer

User Access Review Post Deployment Services

BoW Support	Responsible	Accountable	Consulted	Informed
Programme & Value Management				
Management of Built on Workday (BoW) application across the customer organization	Customer	Customer	Kainos	Kainos
Defining Goals and Success Metrics for Built on Workday application	Customer/ Kainos	Customer	Kainos	Kainos
Planning				
Ensuring Kainos has access to Workday non-production and production tenants as required to facilitate ongoing support and for deploying maintenance releases and feature releases in line with Kainos release schedule.	Customer	Customer	Kainos	Kainos
Support (Core)				
Raising support tickets	Customer	Customer	N/A	Kainos
Fixing defects/issues identified and raised in BoW application, in line with defined BoW application	Kainos	Kainos	N/A	Customer
Core product support queries - 6 Office Hours per subscription agreement	Customer	Customer	Kainos	Kainos
Support (Specialist) – Optional**				
Raising support tickets	Customer	Customer	N/A	Kainos
Fixing defects/issues identified and raised in BoW application, in line with defined BoW application	Kainos	Kainos	N/A	Customer
Core product support queries - 20 Office Hours or other purchased amount	Customer	Customer	Kainos	Kainos
Additional Workday Configuration changes/enhancements to customer BoW application: - Business Process - Domain	Customer	Customer	Kainos	Kainos
Review and test BoW application functionality in lower tenant after changes	Customer	Customer	Kainos	Kainos
Additional knowledge transfer	Customer	Customer	Kainos	Kainos
General				
Liaise directly with Workday for resolution of any Workday issues	Customer	Customer	N/A	Kainos
Maintain appropriate licenses for Workday	Customer	Customer	N/A	N/A