



AI Safety, Compliance & Governance for Microsoft Business Applications

Service Definition Document

G-Cloud 15

Status: Definitive

Security Commercial – In Confidence

Version no.1/0

THINKING
BEYOND
LIMITATIONS

We're Kainos

Formed in 1986, we set about finding the best people to tackle the most difficult digital work. We fostered a culture where people truly care for each other and the world around them.

Our reputation for software engineering and problem-solving was quickly established, and our customers started to view us more as their colleagues

We're much bigger now, helping organisations across the globe to navigate change in more ways than ever. But some things never change, like our commitment to our people, delighting our customers, and our technical ability

Some say we're leading a quiet revolution in digital, but if you ask us, we're just doing our bit to make the world a little bit better.



3,132 amazing
people



13 consecutive
years of growth



40 years
of innovation



£382m revenue
(FY2024)



13 locations
globally



FTSE 250 listed
tech company



Our core expertise

The digital revolution is already happening. We're leading from the front to help our clients **seize every digital opportunity** and be future-ready.



Cloud



Business Applications



Data and AI



Managed services



Engineering



Service and
experience design



Workday services
and products

- Test
- Audit
- Shield
- Deployment
- Optimisation
- Spark & Grow

AI Safety, Compliance & Governance for Microsoft Business Applications

The AI Safety, Compliance & Governance service provides organisations with a structured approach to evaluating, defining and strengthening the governance and compliance controls required to adopt Microsoft AI capabilities safely. As AI becomes integrated into Dynamics 365, Power Platform and Microsoft 365, organisations require clarity around data protection, ethical use, risk boundaries, user permissions and operational oversight. The service supports organisations in building a robust governance framework, defining responsible AI policies, and establishing processes to manage AI usage across business applications.

The engagement includes discovery, risk evaluation, policy and standards definition, governance design, operational process development and recommendations for future improvements. The aim is to provide a clear, adoptable and maintainable framework that ensures AI features are used in a safe and compliant manner while supporting business value.

Discovery & Risk Assessment

A discovery process is conducted to assess existing governance controls and AI-related risks. Activities include:

- Reviewing organisational policies related to data protection, information management and technology governance

- Identifying current and planned AI usage across Dynamics 365, Power Platform and Microsoft 365

- Assessing identity, security and permissions models relevant to AI functionality

- Reviewing data sensitivity, classification, DLP rules and applicable compliance policies

- Understanding regulatory obligations (e.g., GDPR, FOI, industry-specific requirements)

- Identifying integration points where AI may access external or legacy systems

- Assessing operational maturity related to monitoring, incident management and auditing

A risk summary is produced outlining key AI-specific risks and mitigation considerations.

AI Governance Framework Review

The service includes a review of the organisation's ability to govern AI usage within Microsoft Business Applications. This includes:

- Assessing existing Power Platform, Dynamics and Microsoft 365 governance models

- Reviewing alignment with Responsible AI principles

- Identifying gaps in oversight, approval processes or role responsibilities

- Reviewing existing controls related to prompt management, agent behaviour, content generation and data access

- Evaluating the suitability of current environment strategy for hosting AI functionality

- Reviewing monitoring and reporting capabilities

Outputs include defined governance gaps and recommended enhancements.

Policy & Guardrail Definition

To support safe AI usage, a set of policy recommendations is developed based on organisational needs. This includes:

- Acceptable-use guidelines for generative AI

- Guardrails for prompt design, content handling and data exposure

- Standards for user access, administrative activities and approvals

- Requirements for data classification and protection when accessed by AI

- Controls to prevent unauthorised data extraction or sensitive content exposure

- Guidance for internal and external use of AI-generated content

- Escalation paths and incident management approaches

These policies ensure AI is used within appropriate boundaries and in alignment with organisational risk tolerance.

Technical & Security Controls Assessment

The service includes reviewing technical controls across Microsoft tenant services to determine whether adjustments are required to support AI safety. This involves:

- Reviewing Conditional Access, MFA and identity protection controls

- Assessing Microsoft Purview policies including sensitivity labels, DLP and records management

- Reviewing Dataverse access models and role configuration

- Evaluating Power Platform connectors, data policies and isolation requirements

- Assessing content access patterns affecting Copilot and AI Agents

- Validating logging, monitoring and audit capabilities for AI actions

Recommendations are provided for strengthening controls to reduce operational and compliance risks.

Training & Awareness Planning

Training requirements are identified to support safe usage and ongoing adoption. Activities include:

Defining training needs for users, administrators and governance teams

Recommending materials for safe-use guidance and internal communications

Identifying responsibilities for maintaining governance documents and policies

Outlining communication pathways to ensure users understand AI boundaries and expectations

This ensures users and administrators have confidence in the governance framework.

Strategic Governance Roadmap

A roadmap is created outlining steps to strengthen governance over time. This includes:

Phased introduction of enhanced governance controls

Prioritised improvements across security, compliance and monitoring

Responsibilities for governance

updates and periodic reviews

Recommendations for future tooling enhancements or automation

Long-term alignment with Microsoft AI platform evolution

The roadmap provides a structured, sustainable approach to maintaining governance for AI usage.

Deliverables

- AI risk and governance assessment report
- Data protection, security and compliance review
- Responsible AI and acceptable-use guidance
- AI guardrail and policy recommendations
- Technical controls enhancement recommendations
- Operational governance and lifecycle processes
- Training and awareness guidance
- Strategic governance roadmap
- Executive summary for senior stakeholders

Methodology

Phase 1: Mobilisation

Kick-off session, planning and stakeholder alignment.

Phase 2: Discovery & Risk Assessment

Review current governance, data, security and AI usage.

Phase 3: Governance Framework Review

Evaluate existing governance structures and identify gaps.

Phase 4: Policy & Guardrail Definition

Define required governance policies and responsible AI controls.

Phase 5: Technical Controls Assessment

Assess tenant, environment and application-level controls.

Phase 6: Operational Governance Design

Define lifecycle processes, responsibilities and operational structures.

Phase 7: Roadmap Development

Create the roadmap for long-term governance improvements.

Phase 8: Handover

Deliver documentation and supporting materials to the organisation.

Roles & Responsibilities

Supplier Team

- Governance & Compliance Specialist
- Security Architect
- Microsoft Business Applications Consultant
- Business Analyst
- Project Manager

Customer Team

- Data Protection Officer
- IT Security Representatives
- Application Owners
- Governance and Risk Teams
- Business Stakeholders

Estimated Duration

Typically 4–8 weeks, depending on organisational size and breadth of AI capabilities in scope.



Where we are

The Americas

Buenos Aires
Indianapolis
Nova Scotia
Toronto

UK and Ireland

London
Birmingham
Belfast
Derry
Dublin

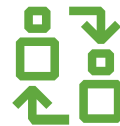
Central Europe

Gdansk
Helsinki
Paris
Wommelgem

What makes us stand out



Our people



True collaboration



Innovation



Digital know-how



Common goals



Trust



Digital Services

We are **engineers**, specialists. We **overcome big challenges** for our clients, through delivery of **intelligent** digital services that use the best in **talent and technology**.



55 million UK citizens

positively impacted by
services we've delivered



**892
customers**



13 locations

And growing



99% of customers

rate our service as good,
great or excellent



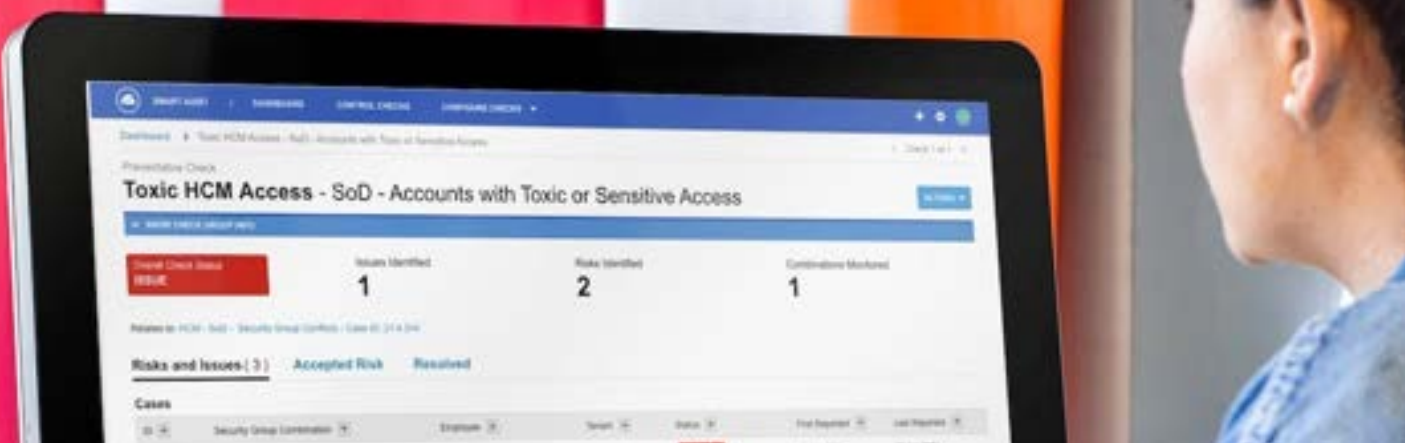
Key partners

Working closely with
Microsoft and AWS to
deliver results



Award-winning

90+ industry awards



Workday

Kainos is a Workday **phase one prime status partner** in all European, North American and Asia Pacific markets. We have worked with many public and private sector customers of various sizes and scale in over **40 countries worldwide**.



Partner Since 2011

We are the only certified Workday Services, Technology and Extend partner globally.



Workday Services

Full range provider from pre-deployment consulting, implementation and support.



650+ Customers

We have deployed to over 650 customers and are a proud Workday customer also, using HCM, Financials, Recruitment, Planning and PSA to run our business.



Workday Public Sector

We have worked with many UK Public Sector customers with their initial deployment, post-deployment support and adoption of new modules.



Kainos Smart

Our product is deployed to 500+ customers globally saving them 1000s of testing hours.



900+ Consultants

Hold over 2,700+ Workday certifications covering all areas of the platform.

65 million

citizens positively impacted
by services **built by Kainos**
for the UK Government



Every driver & every car on the road
Every piece of work to fix roads
Every court case & every prisoner
Every home helped with help-to-buy
Every passport & renewal application
Every COVID test sent out
Every COVID test result
Every user of the NHS App

Every voter registered
Every company opened & closed
Every UK civil servant trained
Every piece of produce grown in the UK
Every thing imported & exported to the EU
Every benefit fraud prevented
Every body's pension details

Our Social Values and commitment to HM Government strategy



Education & Capability Building

We empower people through technical and behavioral learning programs, academies, and outreach projects, fostering skills development and inspiring future technology leaders across communities and organisations.

Social Responsibility

Tackling workforce inequality and ensuring equal access to technical and vocational education, through our Academies, Camps and Earn as you Learn schemes.

Innovation & Future Readiness

Driving continuous improvement through technology

Health, Wellbeing & Accessibility

We support colleagues' physical, emotional, and career wellbeing through initiatives, guidance, and inclusive design, ensuring equal access, experiences, and compliance for all users with diverse needs.

Climate Action & Sustainability

With a comprehensive sustainability strategy underway, we will be a Carbon Net Zero company by 2030.

Equality, Diversity & Inclusion

Maximising service experience for citizens and civil servants by delivering projects with diverse teams, underpinned by our BAME, LGBTQIA+ and female communities.



The Code of Ethics

We are guided by our 6 ethical principles.



Wellbeing

We protect the wellbeing of our staff, customers and communities.



Equality

We improve access and inclusion and minimise bias.



Transparency

Our decisions are traceable and accountable.



Integrity

We hold ourselves and others to ethical standards.



Environment

We act responsibly towards the Earth and its resources.



Initiative

We take initiative to deliver social value and positive impacts.

BCDR and Exit Plan

Business Continuity and Disaster Recovery (BCDR)

A Business Continuity Plan can be provided if required. This shall set out the arrangements to be invoked in the event of an actual or perceived threat to business continuity, to ensure continued operation of the system and continuity of the services provided by Kainos pursuant to the Prime Agreement and shall include: the alternative processes, options and responsibilities that may be adopted in the event of a failure or disruption to the system and/or services provided by Kainos pursuant to the Prime Agreement; and the steps to be taken by Kainos upon resumption of the system and services provided by Kainos pursuant to the Prime Agreement in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

Exit Plan

An Exit Plan can be provided if required to detail the steps that would be carried out to ensure smooth transition of Kainos services to a new supplier. The steps outlined in the Exit Plan will help mitigate against any disruption to the service during the transition period. It is assumed that any new supplier will themselves have a procedure they wish to follow during the transition period, and as such the steps in this Exit Plan will serve as a checklist for the new supplier to ensure all key areas of the transition have been covered. The Exit Plan will therefore be subject to refinement should it be exercised.

Commercial Statement

Confidentiality and copyright

© Kainos Software Limited 2026 ("Kainos")

The contents of this document are commercial and confidential in nature and the copyright of Kainos. This document must not be reproduced (in whole or in part) save in connection with the purpose for which it was issued and must not be shared with Generative AI systems without express consent.

Trademarks

Kainos® is a registered trademark of Kainos Software Limited. All rights reserved. You may not delete or change or modify any copyright or trademark notice.

Caveats

Kainos has used all reasonable endeavours to ensure that the contents of this document are accurate but is not responsible for any errors or omissions.

All information provided prior to execution of a contract is provided 'as is' and 'subject to contract' without warranty of any kind.

This document does not constitute an offer from Kainos. In the event that the parties elect to work together, they will only be contractually bound to each other upon signature of a contract.

Corporate information

"Kainos" is the trading name of the Kainos group of companies, further information on which can be found here: <https://www.kainos.com/corporate-information/>.

Kainos Software Limited/ Kainos WorkSmart Limited, will be the contracting entity under this tender / for the provision of the service and may be assisted from time to time by other Kainos group companies.

Freedom of information

Kainos considers that the following information provided in this document is exempt from disclosure under the Freedom of Information Act 2000 (FOI):

The CVs of staff qualify under the "Personal Information Exemption (s.40)" of the Freedom of Information Act and are exempt from disclosure under the Data Protection Act 1998. The Period for which this information should be confidential is the lifetime of the Data Subject.

Rate and pricing information is confidential and commercially sensitive and covered by the 'Commercial Interests' exemption (s.43) of the FOI, as the release of this information is likely to prejudice the commercial interests of Kainos and is likely to adversely affect its (and the Customer's) future negotiating position. The period that this information should be confidential for should be 5 years.