

kubrick

G-Cloud 15

Kubrick – AWS Services

Lot 3 - Cloud Support



Contents



Part A: Company Profile

About Kubrick

About us

What we do

Our Approach

Why us?



4 Part B: Service Specific Information

7



<u>Part C: Standard Information</u>	<u>20</u>	
<u>Social Value</u>	<u>21</u>	<u>Service Levels</u> 33
<u>Data Protection & Information Assurance</u>	<u>22</u>	<u>Outage & Maintenance Procedures</u> 34
<u>Business Continuity Statement</u>	<u>23</u>	<u>Financial Recompense Model</u> 35
<u>Privacy by Design</u>	<u>24</u>	<u>Provision of the Service</u> 36
<u>Using the Service</u>	<u>25</u>	<u>Customer Responsibilities</u> 37
<u>Ordering & Invoicing</u>	<u>26</u>	<u>Technical Requirements</u> 38
<u>Trial Service Availability</u>	<u>27</u>	<u>Account Management & Consultant Success</u> 39
<u>Onboarding, Offboarding & Service Migration</u>	<u>28</u>	<u>Termination Process</u> 40
<u>Training & Knowledge Transfer</u>	<u>30</u>	<u>Experience</u> 41
<u>Service Management</u>	<u>31</u>	<u>Client List</u> 42
<u>Service Constraints</u>	<u>32</u>	<u>Contant Details</u> 43

kubrick

Part A: Company Profile



About Kubrick



About us

Kubrick is a technology services company that helps organisations build the cloud, data, and digital engineering capability they need to modernise and operate effectively. We were founded to address the growing digital skills gap by providing an alternative to traditional consultancy and contractor models. Our mission is to give organisations access to adaptable, well-trained engineering talent while creating meaningful career pathways for people from a wide range of backgrounds.

We recruit high-potential individuals and train them intensively through practitioner-led programmes in cloud engineering, data, DevOps, SRE, and modern analytics. After training, our consultants join client teams as embedded contributors, supported throughout by Kubrick's senior practitioners. This ensures that organisations gain the capacity to accelerate key programmes while developing long-term internal capability.

Kubrick is committed to:

- ✚ Expanding access to digital careers
- ✚ Practitioner-led technical oversight
- ✚ Focus on sustainable capability, not dependency



What we do

Kubrick provides organisations with trained consultants who work directly within their teams to deliver cloud, data, and modern engineering outcomes. Our consultants combine up-to-date technical training with practical problem-solving and a strong grounding in engineering practices such as agile delivery, automation, CI/CD, observability, and secure-by-design thinking.

We support a wide range of transformation and operational improvement initiatives. This includes cloud migration and platform development, modernising or optimising cloud environments, improving operational maturity through DevOps and SRE practices, enhancing CI/CD pipelines and automation, and strengthening data engineering, analytics, and governance. Consultants integrate quickly into client teams, contributing to active projects while helping embed sustainable engineering practices.

Throughout the engagement, consultants are supported by Kubrick's senior practitioners, who provide technical oversight, guidance, and coaching. This blended model allows organisations to scale capacity rapidly, introduce modern skills, and develop stronger internal teams without relying on long-term managed services or expensive contractor-based approaches.

About Kubrick



Our Approach

Kubrick's approach is collaborative, practical, and focused on building sustainable capability. We work alongside client teams rather than as an external, arms-length consultancy. Our consultants join delivery teams directly, learning organisational context and sharing modern engineering methods through hands-on contribution. They are supported throughout their placement by Kubrick's senior practitioners, ensuring high-quality delivery and continuous development.

We emphasise transparency, incremental improvement, and modern engineering practices such as automation, observability, secure-by-design thinking, and SRE-influenced operational readiness. Every engagement includes structured documentation, handover, and knowledge transfer so improvements are maintained after we leave.

Our approach emphasises:

- ✦ Embedded delivery supported by experienced practitioners
- ✦ Incremental, transparent improvement aligned to client priorities
- ✦ Automation, observability, and secure-by-design practices
- ✦ Clear documentation and knowledge transfer to support long-term capability



Why us?

People choose Kubrick because of our distinctive combination of engineering capability, structured training, and a sustainable approach to capability development. Our consultants bring technical knowledge, hands-on engineering skills, and a grounding in cloud-native, DevOps, and SRE practices. Our senior practitioners ensure consistency, quality and access to deeper expertise when required.

We accelerate transformation while strengthening internal capability. By working within client teams, we reduce reliance on external suppliers and help organisations adopt modern engineering methods that deliver value after the engagement ends.

We play a leading role in widening access to technology careers—recruiting from diverse backgrounds, training them intensively, and supporting them to become high-performing engineers. Clients gain technically capable teams who bring fresh perspectives, adaptability, and a strong motivation to learn.

This blend of delivery support, knowledge transfer, and social impact sets Kubrick apart and offers a scalable, flexible alternative to conventional consultancy or contractor models.



Part B: AWS Service Specific Information



Data Mesh and Data Product Development Service on AWS

Service Snapshot

Service Description

Kubrick's Data Mesh and Data Product Development Service supports public sector organisations in designing and implementing decentralised, domain-oriented data architectures on AWS.

The service enables a transition from centralised data platforms to a data mesh approach, supported by AWS-native lakehouse patterns. Data products are built to be discoverable, secure, interoperable, and reusable across domains, while federated governance ensures consistency and compliance.

Service Features

- Definition of data mesh principles, domain boundaries, and operating model
- Design and implementation of AWS lakehouse architectures using Amazon S3, AWS Glue, and analytics engines
- Creation of domain-owned data products with clear data contracts and quality rules
- Metadata management and data discovery using Amazon DataZone
- Secure data collaboration and sharing patterns, including AWS Clean Rooms where appropriate
- Federated governance models using AWS Lake Formation and IAM
- Data lineage, observability, and quality monitoring
- Enablement of domain teams through templates, patterns, and documentation

Service Benefits

- Improved data ownership and accountability across domains
- Increased trust and usability of shared data assets
- Reduced dependency on central data engineering teams
- Faster delivery of analytics and operational insights
- Scalable lakehouse-based data foundations

Data Mesh and Data Product Development Service on AWS

Service Snapshot

Pricing

Pricing is provided on a time-and-materials, fixed-price, or subscription basis depending on scope and delivery model. Final pricing is confirmed following an initial discovery or service definition phase.

Security and Compliance

The service aligns with UK government security principles and UK GDPR. AWS-native security controls such as IAM, encryption using AWS KMS, network isolation, logging, and auditing using Amazon CloudWatch and AWS CloudTrail are applied in line with agreed security requirements.

Exit Management

At contract end, all documentation, configurations, and deliverables are handed over. Kubrick provides reasonable assistance to support transition to another supplier or an internal team.

AWS-Native Data & Analytics Solutions as a Service

Service Snapshot

Service Description

Kubrick's AWS-Native Data & Analytics Solutions as a Service provides managed, scalable data and analytics capabilities using AWS-native services.

The service is built around modern AWS lakehouse and streaming architectures, enabling reliable data ingestion, transformation, storage, and analytics without customers needing to operate complex data platforms themselves.

Service Features

- Managed data ingestion using AWS Glue, Amazon Kinesis, and batch and streaming pipelines
- Lakehouse-based data storage and analytics using Amazon S3 and AWS-native analytics services
- Data transformation, cataloguing, and schema management using AWS Glue
- Near-real-time data processing and event streaming using Amazon Kinesis
- Analytics, reporting, and data access enablement for downstream tools
- Operational monitoring, reliability, and performance management
- Security, access control, and governance using AWS IAM and Lake Formation
- Cost monitoring and optimisation for data and analytics workloads

Service Benefits

- Reduced operational burden on internal teams
- Faster access to trusted, well-governed data
- Support for both batch and real-time analytics use cases
- Predictable, scalable analytics capability
- Improved reliability and platform resilience

AWS-Native Data & Analytics Solutions as a Service

Service Snapshot

Pricing

Pricing is provided on a time-and-materials, fixed-price, or subscription basis depending on scope and delivery model. Final pricing is confirmed following an initial discovery or service definition phase.

Security and Compliance

The service aligns with UK government security principles and UK GDPR. AWS-native security controls such as IAM, encryption using AWS KMS, network isolation, logging, and auditing using Amazon CloudWatch and AWS CloudTrail are applied in line with agreed security requirements.

Exit Management

At contract end, all documentation, configurations, and deliverables are handed over. Kubrick provides reasonable assistance to support transition to another supplier or an internal team.

MLOps and LLMOps Accelerator

Productionisation of AI and GenAI on AWS

Service Snapshot

Kubrick's MLOps and LLMOps Accelerator supports public sector organisations in moving artificial intelligence (AI), machine learning (ML), and generative AI (GenAI) solutions from proof-of-concept into secure, scalable, and operational production environments on Amazon Web Services (AWS).

The service establishes repeatable engineering practices, pipelines, and governance required to deploy, operate, and improve models over time. For GenAI and LLM-based solutions, the service supports retrieval-augmented generation (RAG) patterns, prompt and chain management, evaluation, safety controls, and operational monitoring to ensure solutions are maintainable and aligned to organisational requirements.

The service can be delivered as an accelerator to establish foundational capabilities, or as a targeted engagement to operationalise a specific model or GenAI use case. Delivery approach and outcomes are agreed during discovery.

MLOps and LLMOps Accelerator

Productionisation of AI and GenAI on AWS

Service Features and Benefits

Service Features (MLOps)

- Assessment of current ML delivery lifecycle, tooling, and operational readiness
- Target-state MLOps architecture design aligned to AWS reference patterns
- CI/CD pipelines for training, testing, packaging, and deployment of ML models
- Model registry and versioning, including promotion workflows across environments
- Automated validation and approval gates (unit, integration, data and model checks)
- Monitoring for model performance, drift, data quality signals, and service reliability
- Incident, change, and release management processes for model updates
- Documentation and knowledge transfer to internal engineering and operations teams

Service Features (LLMOps / GenAI)

- Design and implementation of GenAI application delivery pipelines (including prompt/chain updates)
- RAG architecture and implementation patterns for enterprise knowledge use cases
- Integration with Amazon Bedrock for foundation model access and orchestration
- Use of common orchestration frameworks (for example LangChain) where appropriate
- Vector search and retrieval design (including indexing, chunking strategy, and relevance tuning)
- Prompt, chain, and policy management with version control and deployment controls
- LLM evaluation approaches (quality, safety, bias, latency, and cost) and regression testing
- Guardrails and safety controls (e.g., policy enforcement, content filtering, PII handling)
- Observability for GenAI apps: tracing, token usage, latency, failure modes, and user feedback loops

Service Benefits

- Reduced risk when moving ML and GenAI solutions into live environments
- Repeatable and auditable deployment processes for models and GenAI applications
- Improved reliability and observability, including drift and performance management
- Better control of GenAI cost, latency, and quality through measurement and governance
- Foundations that enable scaling AI/GenAI delivery across multiple teams and use cases

MLOps and LLMOps Accelerator

Productionisation of AI and GenAI on AWS

Overview

Who the Service Is For

This service is intended for public sector organisations that have developed (or are developing) ML or GenAI solutions and require support to operationalise them. It is suitable for organisations at different stages of maturity, from early pilots to established AI programmes, including teams adopting Amazon Bedrock for GenAI use cases.

Typical stakeholders include data science teams, platform/DevOps teams, security and governance functions, and product owners responsible for deploying AI-enabled services.

What's Included

Discovery and assessment to confirm scope, architecture, and delivery plan
Design of target operating model and technical patterns for MLOps/LLMOps
Implementation of agreed pipelines, controls, and monitoring capabilities
Documentation, runbooks, and knowledge transfer sessions

What's Not Included

Ongoing managed service unless explicitly agreed. Cloud consumption and software licensing costs are not included unless stated. Data preparation, large-scale model training, or extensive data remediation is included only where explicitly in scope.

Pricing

Pricing is provided on a time-and-materials, fixed-price, or subscription basis depending on the nature, scope, and duration of the engagement. An initial discovery or assessment phase is typically used to confirm requirements, delivery approach, and commercials before work begins.

MLOps and LLMOps Accelerator

Productionisation of AI and GenAI on AWS

Overview

Who the Service Is For

This service is intended for public sector organisations that have developed (or are developing) ML or GenAI solutions and require support to operationalise them. It is suitable for organisations at different stages of maturity, from early pilots to established AI programmes, including teams adopting Amazon Bedrock for GenAI use cases.

Typical stakeholders include data science teams, platform/DevOps teams, security and governance functions, and product owners responsible for deploying AI-enabled services.

What's Included

Discovery and assessment to confirm scope, architecture, and delivery plan
Design of target operating model and technical patterns for MLOps/LLMOps
Implementation of agreed pipelines, controls, and monitoring capabilities
Documentation, runbooks, and knowledge transfer sessions

What's Not Included

Ongoing managed service unless explicitly agreed. Cloud consumption and software licensing costs are not included unless stated. Data preparation, large-scale model training, or extensive data remediation is included only where explicitly in scope.

Pricing

Pricing is provided on a time-and-materials, fixed-price, or subscription basis depending on the nature, scope, and duration of the engagement. An initial discovery or assessment phase is typically used to confirm requirements, delivery approach, and commercials before work begins.

MLOps and LLMOps Accelerator

Productionisation of AI and GenAI on AWS

Overview

Security and Compliance

The service is designed to align with UK government security principles and relevant public sector security standards. Data protection and privacy requirements, including UK GDPR obligations, are supported throughout delivery.

Where AWS is used, native capabilities such as AWS Identity and Access Management (IAM), encryption at rest and in transit (for example using AWS KMS), logging and monitoring (for example using Amazon CloudWatch and AWS CloudTrail), and network controls are configured in line with agreed security policies. Controls for secrets management, key rotation, and least-privilege access are implemented where applicable.

Support

Support is provided during agreed delivery hours for the duration of the engagement. Incident and issue management processes are defined at project initiation, including escalation routes and responsibilities.

If ongoing support or a transition to a managed service is required, this can be defined as a separate scoped arrangement.

Service Constraints

Delivery is dependent on access to required AWS environments, data sources, and relevant stakeholders. Timelines may be impacted by security approvals, data access provisioning, and third-party dependencies. Any material scope change may affect delivery timeframes and cost.

Exit Management

Exit management is supported to ensure continuity and minimal disruption at contract end. All documentation, configurations, design artefacts, and agreed deliverables are handed over to the customer. Reasonable assistance is provided to support transition to an alternative supplier or an internal team where required.

kubrick

Part C: Standard Information



Standard Information

Social Value

Kubrick creates social value by developing diverse early-career talent and helping individuals build long-term digital and data careers. We combine intensive training with paid employment, giving people from a wide range of backgrounds the opportunity to enter technical roles that may otherwise be inaccessible to them.

We actively seek applicants from underrepresented groups and communities, using outreach programmes, partnerships, and inclusive recruitment practices to widen participation. Successful candidates receive structured training in cloud, data, and digital disciplines, followed by real project experience with clients. This approach helps individuals build professional confidence while contributing meaningful work to public sector digital programmes.

Kubrick's commitment to social value continues beyond the initial placement. We provide ongoing learning and development support,

leadership pathways, and coaching, helping our consultants progress in their careers and sustain long-term employment in the digital and technology sectors. Many consultants move into permanent roles within client organisations, supporting local capability building and reducing reliance on external contractors.

We also contribute to the wider community by working with educational institutions, community groups, and outreach partners to raise awareness of digital careers. These activities support local skills pipelines and help address the UK-wide shortage of cloud and data talent.

By developing new talent and helping organisations build sustainable internal capability, Kubrick delivers social value that extends beyond the duration of individual projects and contributes to stronger, more diverse digital workforces across the public sector.

Data Protection & Information Assurance

Kubrick takes data protection and information security seriously and ensures that all work complies with UK data protection law, including the UK GDPR and the Data Protection Act 2018. Our consultants operate solely within the client's cloud environments, systems, and networks; Kubrick does not host, store, or process client data on Kubrick infrastructure.

All data access is governed by the client's own security and access controls. Consultants receive only the permissions required to undertake the agreed work, follow the client's security and change-control processes, and have all access removed at the end of the engagement.

Kubrick provides regular data protection and information security training to all staff, covering secure handling, incident reporting, phishing awareness, and good security practice. Internal policies, including our Information Security and Data Protection Policies, define the standards expected of all employees.

Where personal data is accessed within client systems, Kubrick acts as a data processor and handles that data strictly under the client's documented instructions. We do not copy personal data outside client-managed environments or transfer it to third parties without explicit client authorisation.

Kubrick maintains appropriate organisational and technical safeguards, including secure corporate devices, multi-factor authentication, access logging, and encryption within Kubrick systems. As client data is never stored on Kubrick infrastructure, these safeguards apply only to our internal systems.

By working within the client's security framework and maintaining robust internal controls, Kubrick ensures that cloud engineering activities are delivered securely, transparently, and in line with recognised information assurance expectations.

Business Continuity Statement

Kubrick maintains business continuity arrangements to ensure that consultancy services can continue with minimal disruption in the event of an incident affecting our people, systems, or offices. Our consultants carry out their work using secure corporate devices, cloud-based collaboration tools, and remote access methods, which allows delivery to continue from any suitable location with internet connectivity.

In the event of a disruption affecting a consultant, Kubrick can provide alternative resources where required, subject to the skills and knowledge needed for the engagement. All active work is supported by internal documentation and oversight, allowing another consultant to pick up tasks where necessary. Managers review project progress regularly to ensure continuity is maintained throughout each engagement.

If an incident affects Kubrick's internal systems

or office facilities, we can continue operating through our remote-working capabilities. Core functions — including communication, project coordination, and file management — use cloud services that have their own resilience measures, ensuring that Kubrick staff can maintain contact with clients and continue work without depending on a single physical site.

Kubrick follows the client's own continuity and disaster recovery processes when working within client environments. Where the service involves deploying or configuring cloud resources, any recovery or restoration of the client's systems is managed under the client's established procedures, and Kubrick will provide support within the scope of the engagement.

By combining flexible working practices, resilient internal systems, and clear oversight of active engagements, Kubrick is able to maintain continuity of service and respond effectively to operational disruptions.

Privacy by Design

Kubrick applies the principles of Privacy by Design to all work delivered under this service. Personal data is handled securely, minimised where possible, and processed only within the controls defined by the client. Our consultants work entirely within the client's cloud environments and systems, always following the client's data protection requirements and technical standards.

At the start of each engagement, we work with the client to understand whether personal data is present in the systems or workloads being designed or prepared for cloud deployment. Where relevant, Kubrick ensures that access is limited to what is necessary for the agreed tasks and that all consultants understand the specific handling requirements.

Kubrick does not copy or store personal data within Kubrick systems. All work takes place on client-managed devices, cloud accounts, and collaboration tools, ensuring data remains

under the client's control. Any logs, notes, or artefacts we create are kept free of personal data unless explicitly required and authorised.

We incorporate secure engineering practices when designing cloud environments, including appropriate identity and access controls, monitoring and logging, and adherence to the client's change management and security review processes. These measures help maintain visibility and control over how personal data is accessed within client systems.

All consultants receive regular training in data protection and cyber security. If a data protection concern arises, Kubrick will notify the client immediately and follow the client's incident response procedures.

By keeping processing within client systems, limiting access, and embedding secure engineering practices, Kubrick ensures privacy considerations are integrated from the outset.

Standard Information

Using the Service

Kubrick delivers this service through consultants who work directly with the client's teams, using the client's cloud environments, systems, and collaboration tools. Consultants follow the client's working practices and security requirements, and all activity is carried out under the direction of the client's product owners, technical leads, or project managers.

Engagements begin with a short onboarding period where Kubrick and the client agree ways of working, communication routes, and the tasks defined in the Statement of Work. During delivery, consultants attend stand-ups, planning sessions, retrospectives, and other ceremonies used by the client's teams to ensure work is fully integrated.

Progress is shared through the client's preferred channels, such as project boards, ticketing systems, or scheduled update meetings. Kubrick

can also provide written updates or participate in governance forums where required.

Consultants use client devices or secure remote access, and rely on the client to provide the credentials, approvals, and tools needed. All development, testing, and deployment activities take place within the client's environment so that changes remain visible and governed by the client.

If priorities change, Kubrick will work with the client to revise tasks or sequencing within the agreed scope. Where additional skills or capacity are needed, Kubrick can discuss options for bringing in further consultants.

By working within the client's teams and systems, Kubrick provides a transparent and collaborative approach that makes it easy to manage work, monitor progress, and maintain control over cloud transformation activities.

Standard Information

Ordering & Invoicing

Clients can order this service through the G-Cloud framework by raising a purchase order and agreeing a Statement of Work (SoW) that outlines the objectives, tasks, and commercial terms for the engagement. Each SoW sets out the duration of the work, the number and type of consultants required, and the day rates that apply. Kubrick does not require a minimum commitment or minimum spend to begin an engagement.

Work is delivered on a time-and-materials basis, with consultants charging for the days spent completing the activities described in the SoW. Any changes to scope, timelines, or consultant requirements can be agreed with the client and reflected in an updated SoW where needed.

Invoices are issued monthly in arrears and reflect the time delivered during that period. Timesheets or activity logs can be provided in line with the client's preferred reporting process. Payment terms follow the agreement set out in the SoW or the client's purchase order.

If the client chooses to extend the engagement or bring in additional consultants, this can be arranged quickly through an amendment to the existing SoW or the issue of a new one, ensuring continuity of delivery without disrupting ongoing work.

Kubrick aims to keep ordering and invoicing straightforward and transparent so that clients can monitor costs easily and adjust capacity when project needs change.

Standard Information

Trial Service Availability

A trial version of this service is not available. Cloud Transformation & Deployment is delivered through consultants working directly with the client's teams and systems, and therefore cannot be meaningfully offered as a standalone trial.

Clients can, however, begin with a short initial engagement under a Statement of Work if they wish to explore ways of working, confirm the fit of the service, or complete a defined piece of discovery or design activity before committing to a longer programme of work.

Standard Information

Onboarding, Offboarding & Service Migration

Onboarding

Onboarding is designed to be straightforward and adaptable to the client's ways of working. Before delivery begins, Kubrick and the client agree a Statement of Work (SoW) that outlines the tasks, timelines, and governance arrangements for the engagement. During the onboarding phase, Kubrick works with the client to confirm access requirements, communication routes, and any technical or security prerequisites.

Clients provide the devices, accounts, permissions, and tools needed for Kubrick consultants to carry out their work inside the client's cloud environments and internal systems. Consultants then join the relevant delivery teams, attend existing ceremonies such as stand-ups or planning sessions, and follow the client's established change control and security procedures.

This approach ensures that Kubrick integrates smoothly into the client's delivery model and that all work is carried out under the client's direction and governance framework.

Offboarding

At the end of the engagement, Kubrick provides a clear and orderly offboarding process to ensure that client teams are fully equipped to continue work without disruption. This includes transferring documentation, reviewing outstanding tasks, and ensuring that code, scripts, and configuration artefacts are correctly stored within the client's repositories.

All Kubrick access to client systems is removed at the conclusion of the SoW, and any temporary development or testing resources created by consultants are reviewed with the client before decommissioning. If requested, Kubrick can provide a final handover meeting to walk through the cloud setup, deployment processes, or migration steps completed during the engagement.

Where follow-on work or additional support is required, this can be arranged through an updated or new SoW so that delivery can continue without delay.

Standard Information

Onboarding, Offboarding & Service Migration

Service Migration

Kubrick does not operate client systems or manage ongoing service delivery, but we support clients in preparing their applications, data, and cloud setups for transition into live service. As part of transformation activities, Kubrick helps clients:

- ✦ Plan and rehearse migration steps
- ✦ Validate that workloads behave as expected in the cloud environment
- ✦ Document key processes such as deployment, rollback, and recovery
- ✦ Confirm the readiness of the cloud setup for handover to operational teams

Any formal service transition into live operations is managed under the client's own processes and governance structures. Kubrick supports these activities within the scope of the SoW by providing documentation, answering technical questions, and ensuring the work completed during the engagement is ready for operational ownership.

Training & Knowledge Transfer

Kubrick's approach places a strong emphasis on knowledge transfer so that client teams are able to understand, operate, and extend the cloud setup once the engagement concludes. Throughout delivery, our consultants work alongside client developers, engineers, and technical leads, sharing the reasoning behind architectural decisions, build methods, and deployment processes as the work progresses.

Rather than providing standalone training courses or certification programmes, Kubrick embeds learning directly into day-to-day delivery. Consultants explain how cloud resources are structured, how infrastructure-as-code and CI/CD pipelines operate, and how migration or deployment steps should be carried out safely. This hands-on approach ensures that knowledge

is gained in context and can be applied immediately to the client's own systems.

Documentation is produced throughout the engagement, covering the cloud setup, migration steps, deployment processes, and any patterns or templates used. This gives client teams clear reference material once delivery is handed over. Where helpful, Kubrick can also provide walkthrough sessions at key stages of the engagement to explain completed work, address technical questions, and support the transition to internal ownership.

By combining close collaboration, transparent working practices, and clear documentation, Kubrick enables organisations to build sustainable in-house capability and reduce long-term reliance on external suppliers.

Standard Information

Service Management

Kubrick provides service management through regular communication, clear oversight of consultant activity, and close collaboration with the client's delivery and governance processes. While the client retains overall ownership and direction of the work, Kubrick ensures that consultants are supported, work is coordinated, and any issues are addressed promptly.

Each engagement has a designated Kubrick manager who oversees the consultants assigned to the project. This manager maintains regular contact with the client's delivery leads, reviews progress against the Statement of Work, and helps resolve any questions or adjustments required during the engagement. If priorities or timelines change, Kubrick will work with the client to agree revised plans and reflect them in an updated Statement of Work where needed.

Consultants participate in the client's existing ceremonies and reporting structures, such as stand-ups, planning sessions, show-and-tells, or governance meetings. This ensures

that work is visible, aligned, and integrated with the client's internal processes.

If the client requires additional service management reporting — such as written progress updates, dashboards, or risk summaries — Kubrick can provide these in the client's preferred format. Any concerns about delivery, access, or priorities can be raised through agreed points of contact and will be addressed promptly by Kubrick's management team.

Kubrick does not provide operational monitoring or managed-service oversight of the client's live systems. Service management relates to coordinating the work of Kubrick consultants and ensuring that delivery proceeds as agreed under the Statement of Work.

By combining clear lines of communication, experienced oversight, and integration with the client's governance processes, Kubrick provides reliable and transparent service management throughout the engagement.

Standard Information

Service Constraints

Delivery of this service depends on the client providing the access, tools, and governance structures required for Kubrick consultants to work effectively within the client's cloud environments and internal systems. As Kubrick does not host or manage client data or infrastructure, all work must take place inside client-managed platforms.

Consultants require suitable devices, user accounts, permissions, and security approvals to carry out the tasks agreed under the Statement of Work. Any delays in obtaining access, licences, or technical approvals may affect delivery timelines. Work must follow the client's change control processes and security policies, which may determine how and when deployments or configuration changes can be made.

The service is delivered during standard business hours unless otherwise agreed in the Statement of Work. Out-of-hours work, emergency support, or activities

requiring extended coverage are not included by default and would need to be discussed and agreed in advance.

Kubrick does not provide managed-service monitoring, live incident response, or operational support for client systems. Any restoration of live services, resolution of production incidents, or ongoing platform management remains the responsibility of the client's operational teams.

Where third-party tools or cloud services are required, the client is responsible for selecting, procuring, and configuring licences or subscriptions. Kubrick can work with the client's chosen technologies but does not procure tools or cloud accounts on behalf of clients.

These constraints ensure our service is delivered securely, consistently, and within governance frameworks established by the client.

Standard Information

Service Levels

This service is delivered on a time-and-materials basis and does not include operational service levels, uptime guarantees, or incident response commitments. Kubrick does not operate the client's cloud environment or provide managed-service monitoring; instead, we supply consultants who work under the client's direction to design, build, and prepare cloud systems.

Service levels for this engagement relate to the coordination and progress of consultancy work rather than the performance of live services. Kubrick ensures that consultants are available during agreed working hours, attend the client's ceremonies and governance meetings, and provide regular progress updates in line with the client's delivery processes. Any issues affecting delivery—such as access delays, tool availability, or changes to priorities—are raised promptly through agreed communication routes.

Where clients require additional structure

around reporting or oversight, Kubrick can provide written updates, risk summaries, or delivery plans that show progress against the Statement of Work. These management activities support transparency and alignment but do not constitute operational SLAs or system-level service commitments.

Any service levels relating to the operation, monitoring, uptime, or recovery of the client's cloud environment remain the responsibility of the client's internal teams or their managed-service providers. Kubrick supports these teams by designing and preparing cloud systems that are stable, secure, and maintainable, but we do not take ownership of live operations.

By focusing on clear communication, reliable consultant availability, and alignment with the client's governance processes, Kubrick provides a stable and predictable level of service throughout the engagement without assuming operational control over client systems.

Outage & Maintenance Procedures

As this is a consultancy service, Kubrick does not operate or manage the client's cloud environment and therefore does not provide outage management, maintenance windows, or system-level recovery services. All responsibility for the availability, maintenance, and operational continuity of the client's cloud platforms remains with the client's internal teams or their managed-service providers.

During delivery, Kubrick consultants follow the client's established change control and release processes, including any required scheduling for deployments, maintenance windows, or freeze periods. If planned changes depend on specific timing — such as the availability of test environments, data refreshes, or scheduled releases — Kubrick will coordinate work within the client's governance and maintenance timetable.

If an outage or service disruption occurs within the client's environment, Kubrick will pause

relevant work and resume it once the client has restored access or confirmed that it is safe to continue. Kubrick does not provide incident response or operational support for live services but will cooperate with client teams when needed, for example by explaining recent changes or sharing relevant documentation.

Any temporary development or testing resources created as part of the engagement are reviewed with the client before decommissioning, and consultants work within the client's procedures to ensure that changes are made safely and in line with operational standards.

By aligning our work to the client's maintenance and change control framework, Kubrick ensures that cloud transformation activities are delivered safely without affecting the client's operational service responsibilities.

Standard Information

Financial Recompense Model

This service is delivered on a time-and-materials basis and does not include financial recompense for service interruptions, delays, or unmet operational service levels. Kubrick does not operate or manage the client's cloud environment, and therefore does not provide compensation related to system availability, performance, or incident response.

All work carried out under this service is governed by the agreed Statement of Work, which sets out the tasks, timelines, and commercial terms for the engagement. If circumstances arise that affect delivery — such as access delays, changes in client priorities, or unexpected technical constraints — Kubrick will work with the client to adjust plans and agree any amendments required to the Statement of Work.

Because Kubrick's role is limited to providing consultancy and engineering expertise within the client's systems, and not to running those systems, no financial penalties or service credits form part of this service.

Standard Information

Provision of the Service

Kubrick provides this service through consultants who work directly with the client's teams, either on site or remotely, depending on the client's requirements and the nature of the engagement. Consultants work using client-provided devices, access credentials, and cloud environments, ensuring that all activity is carried out within the client's security and governance framework.

The service is delivered during standard business hours unless otherwise agreed in the Statement of Work. Consultants participate in the client's delivery processes, attend scheduled ceremonies or meetings, and follow the client's change control, security, and operational procedures when carrying out design and engineering activities.

Consultants are supported by Kubrick's internal management team, who oversee delivery quality, resolve issues raised by either

party, and ensure that consultants have the guidance and resources needed to complete their work. Where additional expertise is required — for example, to address a specific architectural question or support a complex migration step — Kubrick can provide access to subject-matter specialists as part of normal delivery oversight.

The service does not include the operation or monitoring of the client's production environment, or any form of managed-service activity. All work relates to the design, build, preparation, and documentation of the cloud setup, carried out within client systems and under the client's direction.

By embedding consultants into client teams and aligning to existing workflows, Kubrick provides a transparent and flexible service that integrates smoothly into the client's wider technology and delivery landscape.

Standard Information

Customer Responsibilities

Successful delivery of this service relies on the client providing the access, resources, and governance structures needed for Kubrick consultants to work effectively within client-managed cloud environments and systems. As all work takes place on client platforms, the client must supply the equipment, tools, and permissions required for the engagement.

Clients must provide suitable devices or secure remote access, along with user accounts, role-based permissions, and any approvals needed to work within cloud environments, code repositories, and ticketing systems. Delays in granting access or provisioning accounts may affect project timelines.

The client is responsible for selecting and procuring any cloud services, licences, monitoring tools, or third-party products required for delivery. Kubrick can advise on configuration but does not obtain or manage subscriptions.

All work must follow the client's governance processes, including change control, security reviews, architectural approvals, and release procedures. The client is responsible for coordinating these processes, scheduling maintenance windows, and ensuring relevant internal teams are available to review or approve changes.

Where work involves applications or data containing personal or sensitive information, the client must provide clear handling instructions and ensure appropriate controls are in place. Any data sets required for migration, testing, or deployment must be prepared by the client.

The client retains responsibility for operating and supporting their cloud platforms once changes are deployed. Kubrick does not provide monitoring, incident response, or managed-service support for live systems.

Standard Information

Technical Requirements

This service is delivered within the client's cloud environments and internal systems, so certain technical requirements must be in place before work can begin. The client must provide Kubrick consultants with appropriate devices or secure remote access, along with the accounts, permissions, and tools needed to carry out the tasks agreed in the Statement of Work.

Consultants require access to the client's cloud platforms — such as AWS, Azure, or Google Cloud — at the appropriate permission level to design, build, and configure resources. Access to supporting tooling, including code repositories, ticketing systems, CI/CD platforms, and logging or monitoring tools, should also be provided where these form part of the delivery process.

Where work depends on specific data sets, test environments, or integration points, the client is responsible for preparing these resources

and ensuring that they are available, stable, and accessible during the engagement. Any required data masking, redaction, or access restrictions should be completed in line with the client's own data protection policies.

Kubrick does not supply software licences, cloud accounts, or development tools. If third-party products or cloud services are required to support the engagement, the client must obtain and configure them before Kubrick can begin work. Any delays in the availability of these tools may affect delivery timelines.

Finally, because all changes are completed within the client's governance framework, clients must ensure that their change control, security approval, and release management processes are working effectively and that Kubrick consultants have the access and visibility required to participate in these processes.

Standard Information

Account Management & Consultant Success

Kubrick provides account management throughout the engagement to ensure that consultants are supported, delivery remains on track, and communication between Kubrick and the client is clear and consistent. A dedicated Kubrick manager oversees the consultants working on the engagement and acts as a point of contact for both operational matters and longer-term planning.

This manager reviews progress against the Statement of Work, meets with client stakeholders as required, and helps address any questions, risks, or changes in priorities. If adjustments to scope, timelines, or consultant allocation are needed, Kubrick will work with the client to agree the appropriate updates and ensure continuity of delivery.

Consultant success is supported through regular internal check-ins, access to Kubrick subject-matter specialists, and ongoing development

and coaching. This oversight ensures that consultants have the guidance, escalation routes, and resources required to deliver effectively within the client's environment.

If the client wishes to expand or extend the engagement, Kubrick can provide recommendations on consultant profiles, skill sets, or team structures that best support the next phase of work. Equally, if the client requires additional visibility on progress, Kubrick can provide tailored reporting or attend governance meetings to support alignment.

These account management and consultant success arrangements help ensure that delivery is well-coordinated, issues are resolved promptly, and the client remains informed and supported throughout the engagement — while retaining full control over the direction and priorities of the work.

Termination Process

When an engagement comes to an end, Kubrick follows a clear and orderly termination process to ensure a smooth transition for the client. All work completed under the Statement of Work is reviewed with the client, and any outstanding tasks or documentation are identified so that the client has full visibility of the current state of the cloud setup and any remaining activities.

Kubrick transfers all relevant artefacts — including code, scripts, infrastructure-as-code templates, documentation, and configuration details — into the client's repositories or designated storage locations before the engagement concludes. Where helpful, Kubrick can provide a final handover meeting to walk through completed work, answer questions, and highlight any considerations for future development or maintenance.

At the point of termination, all Kubrick access to the client's systems, cloud environments, tools, and collaboration platforms is removed in line with the client's security procedures. Any temporary resources created as part of development or testing activities are reviewed with the client before being decommissioned.

Kubrick does not retain client data or copies of artefacts once the engagement has ended. All material remains within client-controlled systems, consistent with Kubrick's data protection and information assurance commitments.

If the client wishes to restart work or begin a new phase of activity after termination, this can be arranged through a new Statement of Work or an amendment to the original agreement.

Standard Information

Experience

Kubrick has extensive experience helping organisations design, build, and modernise their cloud environments using secure, repeatable engineering practices. Our consultants have worked with a range of public and private sector clients to create well-structured cloud setups, introduce automation, prepare complex applications and data for migration, and support wider digital transformation programmes.

Across these engagements, Kubrick has delivered cloud architectures based on industry best practice, built environments using infrastructure-as-code, and implemented CI/CD pipelines that improve the speed and reliability of application delivery. We have supported teams moving from legacy systems to cloud-based platforms, carried out

detailed analysis and testing of migration steps, and introduced monitoring and configuration patterns that help organisations operate cloud services confidently.

Our experience spans multi-team programmes, focused discovery and design phases, and long-term transformation initiatives. Consultants work closely with client developers, architects, and product teams, contributing not only technical engineering capability but also clear documentation and knowledge transfer to support sustainable internal ownership.

By combining hands-on engineering with structured design and safe-change practices, Kubrick has built a strong track record of helping organisations establish reliable cloud foundations and modernise the systems they depend on.

Standard Information

Client List



Contant Details



Christopher Swann

Public Sector Partner

chrisswann@kubrickgroup.com

07710806932



Nick Allen

Head of Global Client Acquisition
and Tech Partnerships

nickallen@kubrickgroup.com

07971125836