

kubrick

G-Cloud 15

Cloud Finance & Security Management Service Definition

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
5	Service Snapshot	8
5	Value Proposition	9
5	What the Service Provides	10
6	Service Scope: What's included	12
	Service Scope:What's Not Included	14
	Typical Use Cases	16
	Outcomes & Deliverables	18
	Technical Approach & Methodology	20
	Associated Services	21
	Case Studies	22



Part C: Standard Information	23		
Social Value	24	Service Levels	36
Data Protection & Information Assurance	25	Outage & Maintenance Procedures	37
Business Continuity Statement	26	Financial Recompense Model	38
Privacy by Design	27	Provision of the Service	39
Using the Service	28	Customer Responsibilities	40
Ordering & Invoicing	29	Technical Requirements	41
Trial Service Availability	30	Account Management & Consultant Success	42
Onboarding, Offboarding & Service Migration	31	Termination Process	43
Training & Knowledge Transfer	33	Experience	44
Service Management	34	Client List	45
Service Constraints	35	Contant Details	46

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: Service Specific Information



Service Snapshot

Kubrick's Cloud Finance & Security service helps public sector organisations gain control over cloud spending and strengthen their security posture. As cloud adoption increases and budgets come under pressure, many organisations face rising costs, limited visibility of their usage, and growing security risks. This service provides practical support to understand where money is being spent, how environments are secured, and what steps are needed to make cloud operations more efficient, sustainable, and resilient.

We help clients build reliable cost-management practices using FinOps methods, including identifying cost drivers, improving tagging and reporting, and optimising workloads to reduce unnecessary spend. These insights support better forecasting, more informed budgeting, and clearer governance over cloud resources. We also incorporate sustainability metrics such as

energy use and carbon impact where required.

On the security side, we assess risks, design proportionate controls, and apply industry-recognised patterns such as Zero Trust, Defence in Depth, and least-privilege access. This strengthens the organisation's overall security posture – meaning how well its cloud environments are protected, monitored, and prepared to respond to threats. We support clients with encryption, identity and access management, monitoring, and automated compliance assessments, ensuring environments are built and managed in line with regulatory and policy requirements.

By combining FinOps, sustainability reporting, and cloud security engineering, this service helps organisations manage their cloud environments more effectively, reduce waste, improve protection against cyber threats, and maintain compliance across their workloads.

Finance & Security

Value Proposition

Kubrick's Cloud Finance & Security service gives public sector organisations a practical and structured way to understand where money is being spent in the cloud, how securely their environments are configured, and what actions will make those environments safer, more efficient, and more compliant. As cloud usage grows, many teams find that costs rise faster than expected, visibility becomes harder to maintain, and security gaps emerge across services. This service directly addresses those challenges.

On the financial side, we apply FinOps practices to help organisations gain clear visibility of their cloud spend, understand the drivers behind it, and identify opportunities to reduce unnecessary cost. This includes improving tagging, reporting, and forecasting, analysing workload behaviour, and assessing whether resources are appropriately sized. These insights support better budgeting, improved governance, and more predictable long-term planning. Where required, we also help organisations measure the

environmental impact of their cloud usage by incorporating sustainability metrics such as energy consumption and carbon footprint.

On the security side, we assess risks and strengthen the organisation's security posture – meaning how well its cloud environments are protected, monitored, and prepared to respond to threats. Our work covers identity and access management, encryption, network controls, configuration reviews, monitoring, and automated policy checks. We draw on recognised patterns such as Zero Trust, Defence in Depth, and least-privilege access to help ensure that cloud environments are aligned to required standards and regulatory obligations (e.g. GDPR, NIST, PCI, HIPAA).

By combining cost management, sustainability insights, and security engineering, this service gives organisations a balanced and actionable view of their cloud environments. It provides the clarity needed to manage budgets, reduce waste, strengthen protection against cyber threats, and build the governance structures that support long-term cloud maturity.

Finance & Security

What the Service Provides

Kubrick's Cloud Finance & Security service provides the practical analysis, engineering work, and governance support needed to help public sector organisations manage cloud spending and strengthen the security of their cloud environments. The service brings together FinOps techniques, sustainability reporting, and cloud security engineering to deliver clear visibility, meaningful insight, and actionable improvements.

Insight into cloud use and spending

We analyse cloud bills, usage patterns, and resource configurations to identify where money is being spent and whether workloads are sized appropriately. This includes improving tagging and reporting, mapping cost drivers to business services, and helping clients understand the link between architecture decisions and financial outcomes. These insights form the basis for more predictable budgeting, clearer accountability, and more informed decision-making.

Sustainability metrics and environmental impact analysis

Where organisations need to measure the environmental footprint of their cloud usage, we incorporate sustainability metrics such as energy consumption and carbon emissions into our reporting. This helps clients understand the environmental impact of their cloud workloads and supports internal or statutory reporting requirements.

Assessment of cloud security controls

We review how securely cloud environments are configured, including identity and access management, encryption, network policies, monitoring, alerting, and configuration baselines. This provides clients with a clear understanding of risks, gaps, or misconfigurations that could affect the confidentiality, integrity, or availability of their systems.

Practical cost optimisation recommendations

Kubrick identifies waste – such as idle resources, over-provisioned workloads, unused storage, or unnecessary duplication – and provides clear, evidence-based recommendations for reducing spend. Where appropriate, we also help clients design or adjust workloads to improve efficiency, using both architectural guidance and configuration changes grounded in best practice.

Finance & Security

What the Service Provides

Reporting, dashboards, and governance support

Kubrick provides clear, accessible reports and dashboards that summarise cloud spending, optimisation opportunities, sustainability impacts, and security risks. We also help clients structure their cloud governance processes – including cost reviews, risk assessments, or approval workflows – to improve long-term maturity and accountability.

Automated compliance and policy validation

We help clients adopt automated approaches for validating compliance against internal or regulatory standards, using tools that can check configuration drift, detect policy violations, or flag non-compliant resources. This supports better governance and reduces manual effort in managing complex environments.

Design and implementation of proportionate security improvements

Where improvements are needed, Kubrick designs and implements cloud-native security controls using recognised patterns such as Zero Trust, Defence in Depth, and least-privilege access. This may include tightening role-based access controls, enabling encryption, introducing automated configuration checks, improving log visibility, or applying guardrails that prevent accidental misconfiguration.

Finance & Security

Service Scope: What's included

Kubrick's Cloud Finance & Security service includes the analysis, engineering work, and governance support needed to help organisations gain clearer financial visibility, improve cost control, and strengthen the security of their cloud environments. The service brings together FinOps practices, sustainability metrics, and cloud security engineering to deliver practical improvements that organisations can build on over time.

Cloud cost analysis and financial visibility

The service includes detailed analysis of cloud bills, usage patterns, workload behaviour, and resource configurations. Kubrick helps clients understand where money is being spent, how costs map to business services, and which architectural or operational decisions are driving that spend. This provides a clear financial picture that supports better budgeting, forecasting, and cost governance.

Sustainability and environmental impact reporting

For organisations that need to measure the environmental footprint of their cloud usage, we incorporate sustainability metrics such as energy consumption and carbon emissions into our reporting. This helps clients understand the impact of their workloads and supports compliance with internal or statutory sustainability reporting requirements.

Cost optimisation and efficiency recommendations

Kubrick identifies unnecessary or avoidable spend – such as idle or oversized resources, unused storage, poorly tagged services, or inefficient architectural choices – and provides practical recommendations for reducing costs. Where appropriate, we also advise on configuration or architectural changes that improve workload efficiency, helping clients establish long-term cost-management practices.

Assessment of cloud security configuration and controls

The service includes a thorough review of how securely cloud environments are configured. Kubrick assesses identity and access management, encryption, network policies, monitoring, alerting, logging, and configuration baselines. This provides a clear understanding of risks, gaps, and misconfigurations that could affect the confidentiality, integrity, or availability of cloud systems.

Finance & Security

Service Scope: What's included

Design and implementation of security improvements

Where opportunities to strengthen security are identified, Kubrick designs and implements cloud-native controls using patterns such as Zero Trust, Defence in Depth, and least-privilege access. This may include refining access policies, improving encryption, tightening network controls, or setting guardrails that prevent configuration drift or accidental misconfiguration.

Reporting, dashboards, and governance guidance

Kubrick provides clear reporting and dashboards that help clients interpret cloud financial data, optimisation opportunities, sustainability metrics, and security risks. We also support clients in shaping governance processes – such as cost reviews, risk assessments, or approval workflows – so that the improvements delivered through the service can be embedded in long-term organisational practice.

Automated compliance assessments and policy validation

To help organisations maintain visibility and reduce manual effort, the service includes the introduction of automated methods for checking compliance against required standards. This may involve tooling that detects policy violations, flags misconfigurations, evaluates resources against internally defined policies, or identifies departures from expected configuration baselines.

Service Scope: What's Not Included

For clarity, the following items are not included within the scope of this service:

Managed security operations or live monitoring

Kubrick does not operate a Security Operations Centre (SOC), provide threat monitoring, triage alerts, or respond to live security incidents. All operational security responsibilities – including incident response, remediation, and ongoing monitoring of logs or alerts – remain with the client or their managed-service provider.

Operation, hosting, or administration of cloud environments

Kubrick does not host, run, or administer cloud platforms or applications. All cloud accounts, subscriptions, operational access, and platform-level responsibilities remain with the client.

Financial guarantees, cost savings, or budget accountability

Kubrick provides analysis and recommendations but does not guarantee specific cost reductions, forecast accuracy, financial outcomes, or ongoing savings. Cloud spend remains the responsibility of the client and is influenced by consumption decisions under their control.

Continuous compliance monitoring or operational enforcement

Although the service includes the design or configuration of automated policy checks, Kubrick does not run continuous compliance tooling, investigate alerts, or enforce compliance on an ongoing basis. Automated checks are introduced as part of uplift work; the client owns day-to-day operation.

Procurement or licensing of tools, platforms, or cloud services

Kubrick does not buy or license FinOps platforms, monitoring tools, security scanners, cloud optimisation tools, or cloud services on behalf of the client. We work with technologies the client selects and provides access to.

Finance & Security

Service Scope: What's Not Included

Penetration testing or adversarial security activities

The service does not include penetration testing, red teaming, offensive security activities, or certification-driven testing. Kubrick focuses on configuration reviews, cloud-native security controls, and policy alignment – not regulated security testing.

Out-of-hours support, emergency response, or 24/7 availability

The service is delivered during standard business hours unless otherwise agreed in the Statement of Work. Kubrick does not provide out-of-hours security support, on-call services, or urgent incident response.

Security accreditation sign-off or regulatory certification

Kubrick can help clients align with frameworks (e.g., GDPR, NIST, CIS benchmarks), but we do not issue certifications, provide data protection officer services, or act as an accredited assessor for regulated standards.

Long-term operation of FinOps or security governance processes

While Kubrick can help establish cost reviews, risk assessments, tagging standards, and approval workflows, we do not operate these processes on behalf of the client. Ongoing governance ownership rests with the client.

Finance & Security

Typical Use Cases

This service is suited to organisations that need greater clarity, control, and assurance across their cloud spending and cloud security. The following non-exhaustive list of use cases shows how Kubrick's capability directly supports common public-sector challenges.

Rising or unpredictable cloud costs

Cloud bills can grow faster than expected, making it difficult to forecast or plan budgets. Kubrick helps identify which workloads, architectural choices, or operational practices are driving these increases and provides recommendations to reduce avoidable spend.

How Kubrick's capability applies: Kubrick analyses detailed cost and usage data, evaluates workload sizing and performance behaviour, checks tagging quality, and identifies inefficiencies such as idle or oversized resources. These insights support budget planning and cost reduction.

Need to strengthen security in response to growing threats

Cloud environments often accumulate security gaps over time – such as overly broad access, unencrypted resources, missing monitoring, or inconsistent network controls.

How Kubrick's capability applies: Kubrick reviews IAM configuration, network policies, logging, encryption settings, and monitoring coverage. We then design and implement improvements using cloud-native controls and recognised security patterns such as Zero Trust and Defence in Depth.

Limited visibility of cloud resources and ownership

As cloud estates grow, it becomes harder to understand which teams own which resources, whether tagging is consistent, and how spend maps to business outcomes.

How Kubrick's capability applies: Kubrick improves tagging structures, cost allocation rules, and reporting quality so that stakeholders can clearly see ownership, consumption, and cost drivers. We also help clients build dashboards and governance processes that keep visibility high as the environment evolves.

Preparing for audits, compliance reviews, or regulatory scrutiny

Public-sector teams often need to demonstrate adherence to standards, but manual checks are difficult to maintain and can be incomplete.

How Kubrick's capability applies: Kubrick assesses the environment against required frameworks (e.g., GDPR, NIST, CIS benchmarks) and introduces automated compliance checks that detect misconfigurations or policy violations. This reduces manual effort and provides clearer audit evidence.

Finance & Security

Typical Use Cases

Improving forecasting, budgeting, and internal governance

Inconsistent cost reporting or unclear review processes make it hard for organisations to manage cloud finances effectively.

How Kubrick's capability applies: Kubrick shapes governance structures such as cost reviews, tagging standards, and approval workflows. We also provide clear reporting and financial insights that support better forecasting, budgeting, and accountability.

Understanding and reducing environmental impact

Many organisations now need to show how their cloud workloads contribute to energy use or emissions.

How Kubrick's capability applies: Kubrick incorporates sustainability metrics such as energy consumption and carbon impact into reports and dashboards, helping clients understand environmental footprints and identify opportunities to reduce them.

Needing a clearer security baseline before scaling cloud adoption

Teams often expand cloud usage before establishing consistent standards for identity, encryption, monitoring, or configuration.

How Kubrick's capability applies: Kubrick helps define baseline policies, implement identity and access controls, apply encryption consistently, and introduce monitoring and guardrails that provide a secure foundation for future growth.

Finance & Security

Outcomes & Deliverables

Kubrick's Cloud Finance & Security service provides organisations with clear financial insight, practical cost optimisation guidance, strengthened cloud security controls, and the governance structures needed to manage cloud environments more effectively. The following outcomes and deliverables are included as part of the service.

Clear visibility of cloud spend and usage

Organisations receive a detailed breakdown of their cloud spending, including cost drivers, workload behaviour, and usage patterns. This includes improved tagging structures, cost allocation rules, and reporting that makes financial data easier to interpret and act upon.

Deliverables may include:

- Cloud spend analysis and cost-driver reports
- Improved tagging or cost allocation models
- Dashboards summarising usage, spend, and ownership

Evidence-based cost optimisation recommendations

Kubrick identifies unnecessary spend such as idle or oversized resources, inefficient storage, underutilised compute, and poorly aligned architectural choices. Organisations receive clear, prioritised recommendations for reducing waste and improving efficiency.

Deliverables may include:

- Cost optimisation recommendations with supporting evidence
- Workload right-sizing assessments
- Proposed architectural or configuration changes to reduce spend

Sustainability reporting for cloud workloads

Where required, Kubrick provides sustainability metrics such as energy consumption and carbon impact, helping organisations understand the environmental footprint of their cloud environments and align with internal or statutory reporting requirements.

Deliverables may include:

- Environmental impact dashboards
- Carbon and energy-use estimates linked to workloads

Governance guidance and improved decision-making structures

Organisations receive practical guidance on how to embed ongoing cost reviews, risk assessments, approval workflows, and reporting rhythms. This helps ensure that the benefits of the service are sustained beyond the engagement.

Deliverables may include:

- Governance process guidance
- Review cadence recommendations
- Decision-making and approval workflow models

Finance & Security

Outcomes & Deliverables

A clear picture of cloud security risks

Organisations receive a thorough review of how securely their cloud environments are configured. This covers identity and access management, encryption, network controls, monitoring, alerting, and configuration baselines, providing a practical assessment of risks and gaps.

Deliverables may include:

- Security configuration assessments
- IAM and access reviews
- Logging, monitoring, and alerting gap analysis

Designed and implemented cloud-native security improvements

Where improvements are needed, Kubrick implements changes using cloud-native controls and industry-recognised patterns such as Zero Trust, Defence in Depth, and least-privilege access. These improvements help strengthen protection against threats and reduce configuration drift.

Deliverables may include:

- Updated IAM roles and policies
- Encryption and network-control improvements
- Guardrails or automated policy checks

Automated compliance assessments and policy validation

Kubrick introduces automated methods for checking configuration compliance against internal standards or external frameworks. These reduce manual effort, improve visibility, and make it easier for organisations to maintain ongoing compliance.

Deliverables may include:

- Automated compliance rules or templates
- Reports highlighting non-compliant resources
- Recommendations for improving compliance coverage

Finance & Security

Technical Approach & Methodology

Our approach to Cloud Finance & Security combines structured financial analysis, detailed security assessment, and practical engineering techniques to help organisations manage cloud costs and strengthen their security posture. The methodology emphasises clarity, automation, and governance, ensuring that improvements can be sustained long after the engagement concludes.

We begin by developing a clear picture of how the organisation currently uses the cloud. This includes analysing billing data, usage patterns, tagging quality, workload behaviour, and the architectural choices that influence spend. At the same time, we review the configuration of cloud environments to understand how identity, access, encryption, network controls, monitoring, and logging are implemented. This provides clients with an evidence-based view of both financial drivers and security risks.

Using these insights, we identify opportunities to optimise spend and strengthen security controls. Cost optimisation work focuses on reducing waste, improving workload efficiency, and enhancing the visibility needed for more predictable budgeting and forecasting. On the security side, we design improvements that use cloud-native controls and recognised patterns such as Zero Trust, Defence in Depth, and least-privilege access, ensuring that enhancements are aligned to best practice and proportionate to the organisation's needs.

A core part of our methodology involves introducing automation wherever it adds value. This includes using policy-as-code to define expected configurations, enabling automated checks that identify non-compliant resources, and integrating these checks into existing CI/

CD pipelines where appropriate. By embedding governance activities directly into engineering workflows, organisations can reduce manual effort, improve consistency, and detect issues earlier in the development or deployment process.

We also incorporate sustainability analysis where required, using cloud-native metrics to estimate energy consumption or carbon impact. These insights can be combined with financial and security data to provide a more complete view of how cloud services are consumed and governed.

Throughout the engagement, we work alongside client teams so that knowledge is transferred naturally. We document cost insights, security recommendations, automated checks, tagging standards, and governance processes in clear and accessible formats. This ensures that teams understand not only the recommendations we provide but also the underlying reasoning and the steps needed to maintain controls over time.

By combining financial analysis, cloud security engineering, and automated governance techniques, this methodology helps public sector organisations build more efficient, more secure, and more sustainable cloud environments – with the structures in place to maintain progress long after the engagement has ended.

Finance & Security

Associated Services

Kubrick's Cloud Finance & Security service can be used on its own or alongside other Kubrick cloud services where organisations have wider transformation or operational goals. Each associated service is independent and optional; none is required in order to use this service, but they can complement the work depending on an organisation's needs.

Cloud Transformation & Deployment

Where organisations are designing new cloud environments or modernising existing workloads, Kubrick's Transformation & Deployment service provides the architectural design, automated environment build, and migration preparation work that can sit alongside cost and security improvements. This allows financial and security insights from this service to be incorporated into the design of new environments from the outset.

Cloud Design and Architecture Services

Where broader architectural guidance is required – for example, defining cloud standards, landing zones, platform blueprints, or enterprise-wide guardrails – Kubrick can provide additional architectural support beyond the specific financial and security scope of this service.

These associated services provide organisations with flexible options for continuing their cloud modernisation journey, while ensuring that the Cloud Finance & Security service remains clearly focused on cost control, sustainability insight, and cloud security uplift.

Cloud Operational Excellence

For teams looking to enhance the reliability or operational maturity of their cloud services, Kubrick's Operational Excellence service focuses on observability, performance engineering, incident readiness, and improvements to day-to-day cloud operations. This can build on the security and governance enhancements delivered through Cloud Finance & Security.

Case Studies

1

Safety Stock Optimisation

The Challenge: A global pharmaceuticals organisation needed a controlled, efficient way to calculate safety stock across its supply network. Existing parameters were static, manual, and slow to reflect changes in demand or lead-time variability. This created financial risk: excess stock tied up capital, under-stocking increased chances of service shortfalls. A dynamic, transparent approach was required to balance cost, availability, and operational risk.

Our Approach: Kubrick helped develop a cloud-based optimisation model that produced statistically driven safety stock recommendations. Consultants processed historical demand and lead-time data across thousands of product–location combinations and built multiple modelling approaches – including Monte Carlo simulation, seasonality-adjusted formulas, and demand-driven methods. A decision framework selected appropriate recommendations, and a governed interface enabled planners to review or adjust outputs.

The Outcome: The solution delivered clear financial and operational benefits:

- Lower inventory holding costs
- Improved planner efficiency and accuracy
- Consistent safety-stock governance
- Scalable logic supporting thousands of recommendations

This data-driven approach improved financial visibility, reduced risk, and strengthened supply-chain resilience.

2

Data-Driven Purchasing Optimisation

The Challenge: A multinational manufacturer needed to improve financial control and reduce the manual effort in analysing supplier options. Data sat in silos across ERP systems, commodity feeds, and logistics sources, delaying response times to volatile pricing, shipping constraints, and availability risks. They required a governed, auditable, and scalable decision-support model to strengthen cost forecasting and purchasing accuracy.

Our Approach: We developed a cloud-based optimisation engine that consolidated large, disparate datasets and applied advanced analytics to model purchasing scenarios. Working with procurement teams, we incorporated variables such as price trends, lead times, storage constraints, and geopolitical factors. Buyers could adjust parameters through a controlled interface, enabling transparent, defensible financial decisions aligned with internal governance.

The Outcome: The tool reduced decision-making time by over 90% and delivered significant cost avoidance across key materials.

- Improved financial visibility and forecasting accuracy
- Reduced manual analysis time and operational cost
- Stronger governance through transparent, auditable modelling
- Multi-million-dollar annual savings projected across priority categories

3

Improving Data Ingestion Reliability

The Challenge: A global insurer struggled with unreliable, manually-intensive bordereaux ingestion workflows. Inconsistent formats, limited monitoring, and reactive error-handling created bottlenecks and compromised confidence in financial reporting. A more robust operational model with clearer observability, stronger process control, and reduced operational toil was needed.

Our Approach: We delivered a resilient ingestion solution using metadata-driven pipelines, automated validation, and structured error-handling patterns. Enhanced monitoring and logging provided end-to-end visibility of ingestion progress, failures, and data transformations. Configurable rules enabled teams to adjust processing logic without code changes, reducing turnaround time and improving operational consistency. The architecture also supported dynamic schema handling, improving reliability when source files changed unexpectedly.

The Outcome: The client achieved a more predictable, supportable ingestion process.

- Improved traceability and incident-readiness
- Reduced manual effort and operational delays
- More consistent, reliable ingestion cycles
- Clearer visibility and faster diagnosis of issues

The solution strengthened day-to-day performance while creating a foundation for long-term maturity.

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. Our Cloud Finance & Security service 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.

Standard Information

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