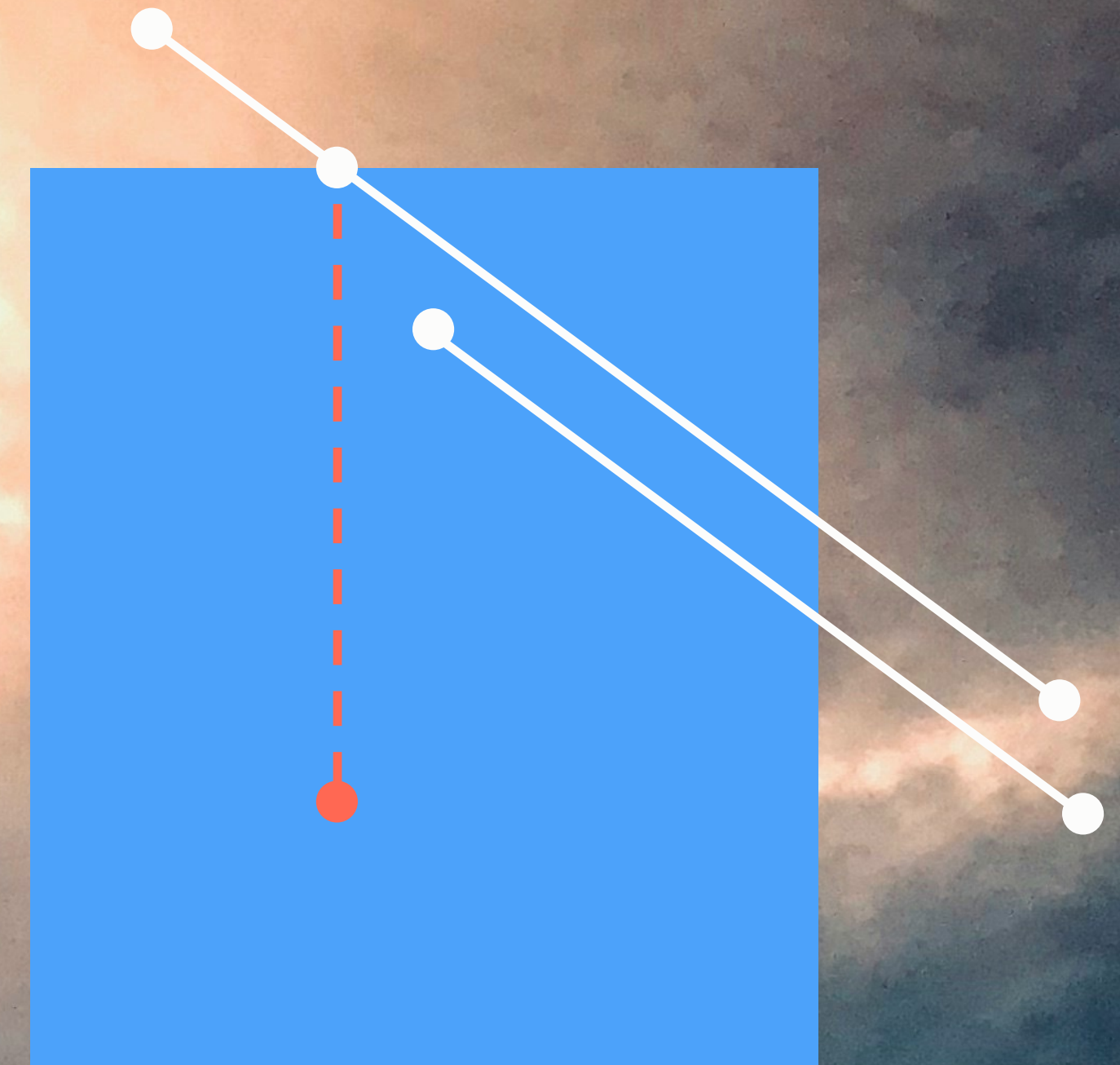




AI Safety & Security Advisory

G-Cloud 15 Services

Service overview

AI Safety & Security Advisory

Designed for organisations designing, building, or operating AI systems, this service helps you understand and manage the safety, security, and compliance risks that come with adopting AI.

The focus is on providing a structured, holistic assessment of risk, covering technical security controls, model robustness and safety, and the governance and regulatory considerations needed for responsible use. Delivery is collaborative and evidence-led, using interactive workshops and technical assessments to build a clear picture of your current position.

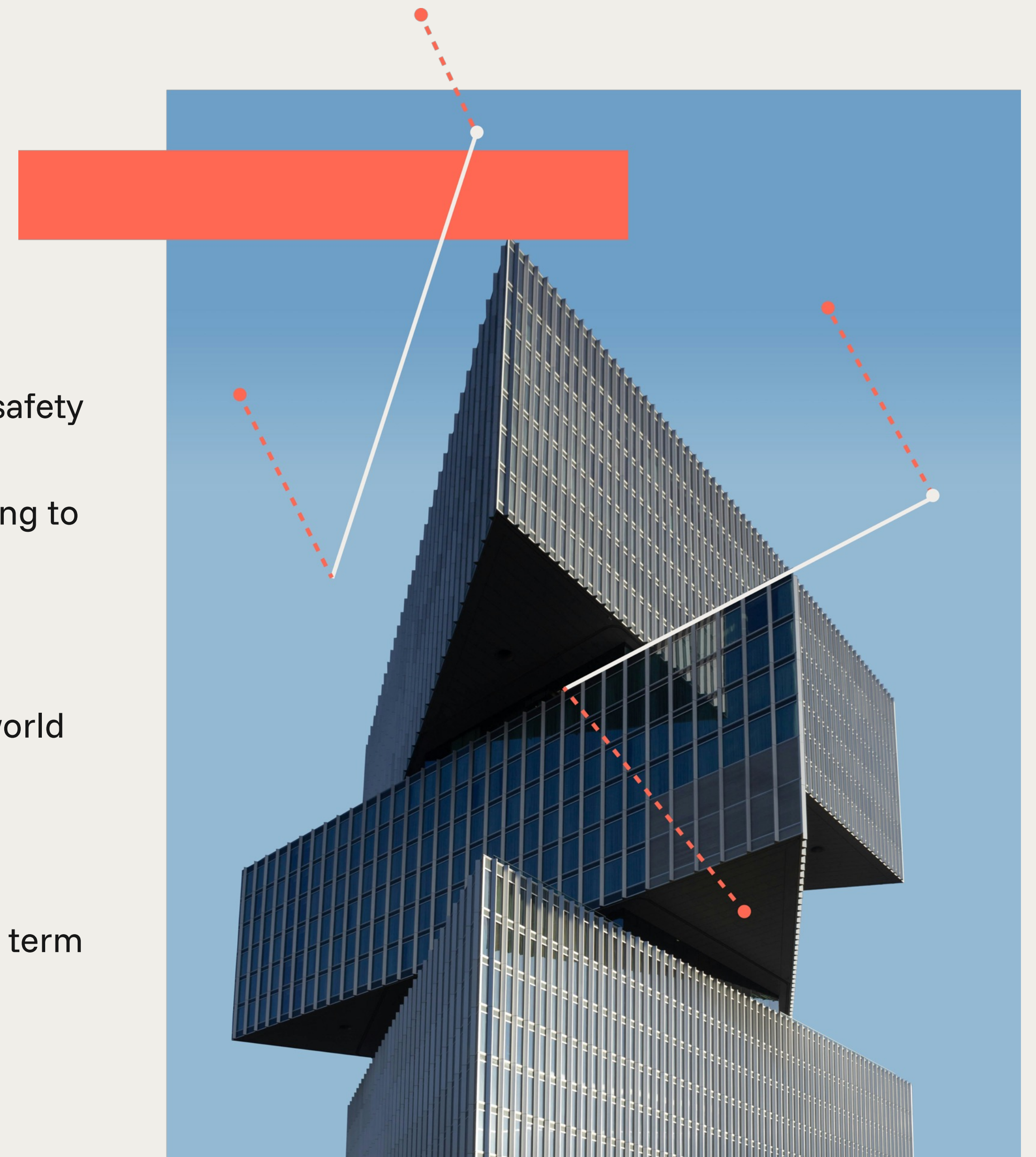
It is particularly useful where teams need confidence that AI systems can be deployed safely, withstand scrutiny, and be operated reliably over time.

Who this service is for

This service works well for organisations that:

- Are developing or deploying AI systems and need assurance on safety and security
- Need to reduce security, privacy, or compliance risk before moving to production
- Want clearer governance for how AI is approved, monitored, and improved
- Need to evaluate model quality, robustness, and safety for real-world use
- Are working with sensitive data or high-impact decision-making contexts
- Want to build internal capability to manage AI risks over the long term

It is commonly used by digital, data, security, risk, assurance, and governance teams responsible for safe adoption of AI.



What the service includes & excludes

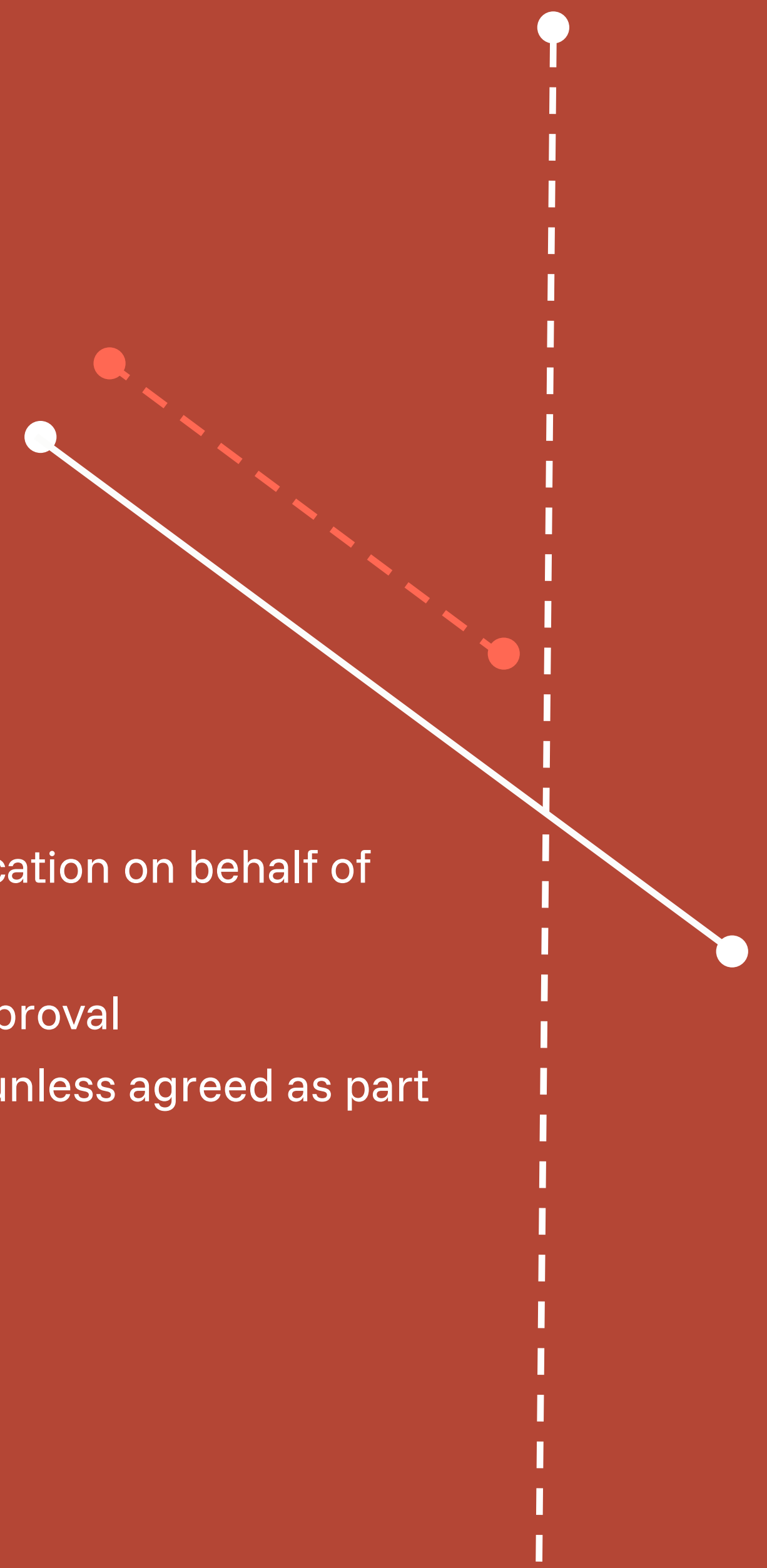
G-Cloud 15 Services

In Scope

- AI safety, security, and compliance briefing
- Holistic AI risk and security assessment
- Stakeholder workshops to understand risks and operating context
- Governance, ethics, and regulatory advisory
- Model robustness and safety evaluation (where appropriate)
- Actionable recommendations and enablement support

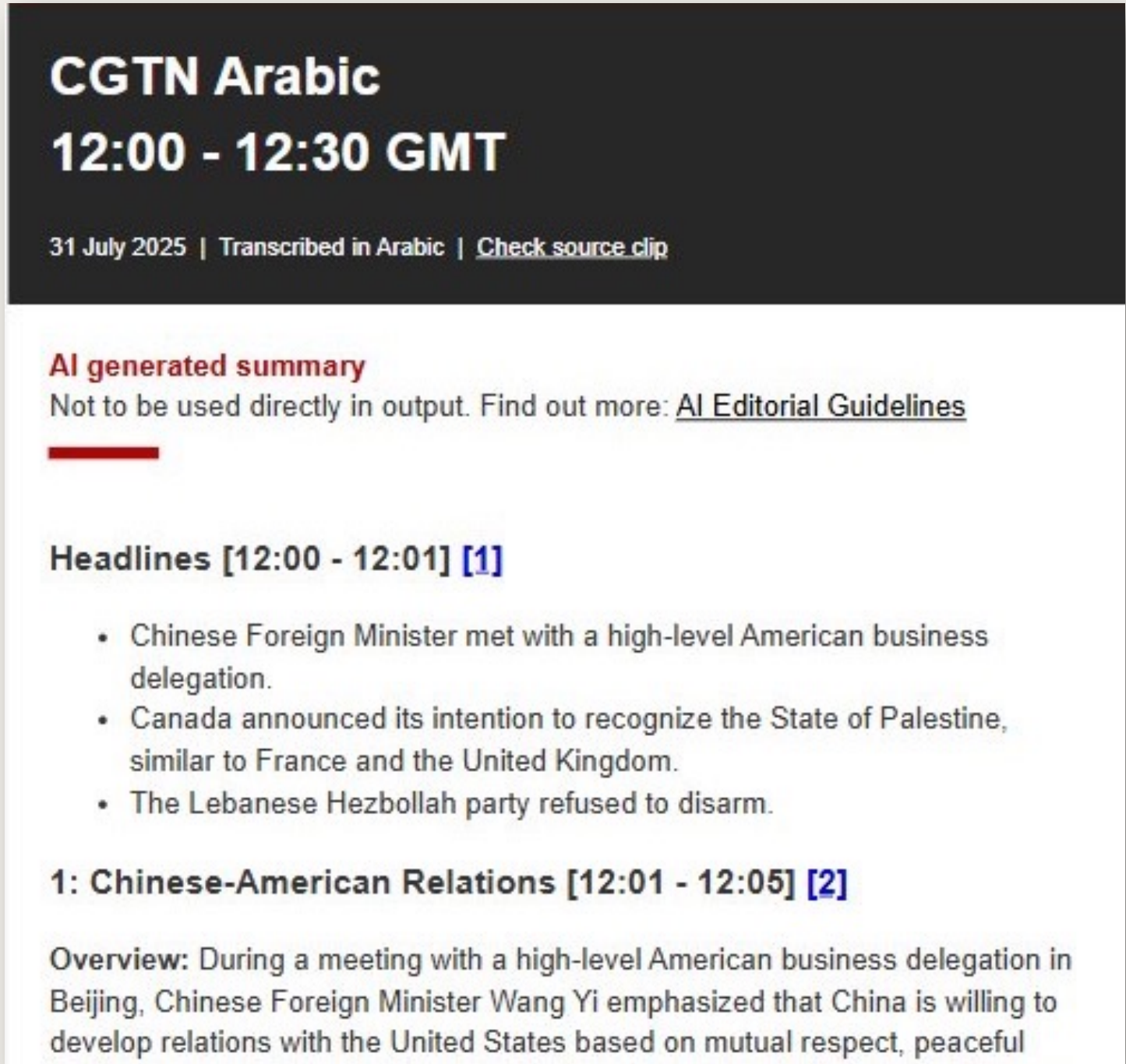
Out of Scope

- Ownership of live services
- Formal accreditation or certification on behalf of the organisation
- Legal sign-off or regulatory approval
- Business-as-usual operations unless agreed as part of the scope





Case Study: BBC
GenAI



Solutions Delivered

Softwire helped bring GenAI, responsibly and securely, to BBC News journalists.

BBC VOLT aids journalists in monitoring television channels from around the world. It ingests ~1500 clips/day, transcribes ~3000 hours/week, and processes ~50TB/month of TV clips. Users can search through transcripts, and in multiple languages.

We have used generative AI to deliver product outcomes that were previously not feasible:

- Summarising long transcripts into clear, digestible bullets
- Generating daily digests and sending key highlights to users
- Allowing natural language search across transcript content to find semantically similar topics
- Improving the accuracy of video transcriptions with the Whisper model

We worked directly with BBC editors and journalists to co-design grading criteria to benchmark AI output on coherence, factual accuracy, completeness, and trustworthiness, ensuring editorial standards were met. Summaries included verifiable references with timestamps, ensuring trust and transparency.

Results & ROI

VOLT has evolved from a search-and-transcribe tool into an intelligence platform, empowering BBC journalists with near real-time analysis, cross-channel comparisons, and digestible daily tailored insights. This has saved their time wading through 3,000+ hours of weekly content and manual searching.

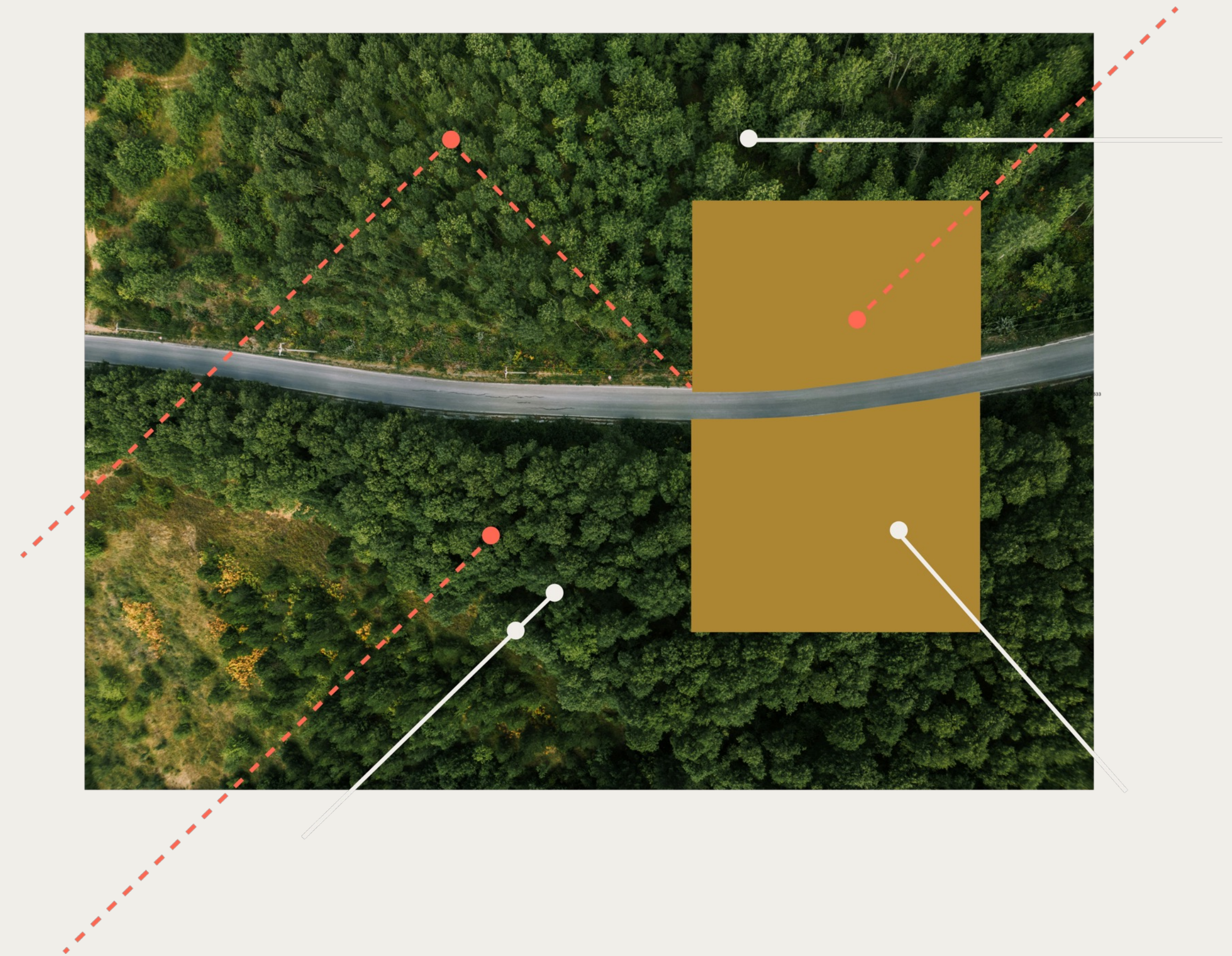
The project established BBC best practices for AI evaluation, validation, and deployment, feeding into wider organisational efforts to adopt generative AI responsibly.

Time scales and effort

Engagements typically range from a few days to several weeks, depending on the breadth of service required and complexity of the domain.

The service is typically delivered as a health-check assessment conduct via workshops with our technical experts and follow-up exploration of outcomes.

G-Cloud 15 Services



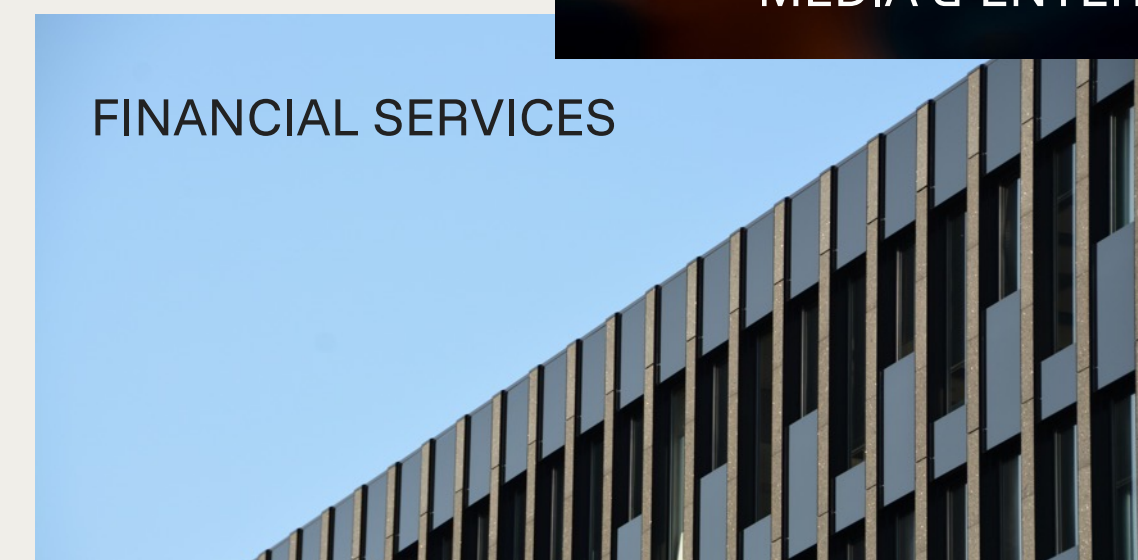
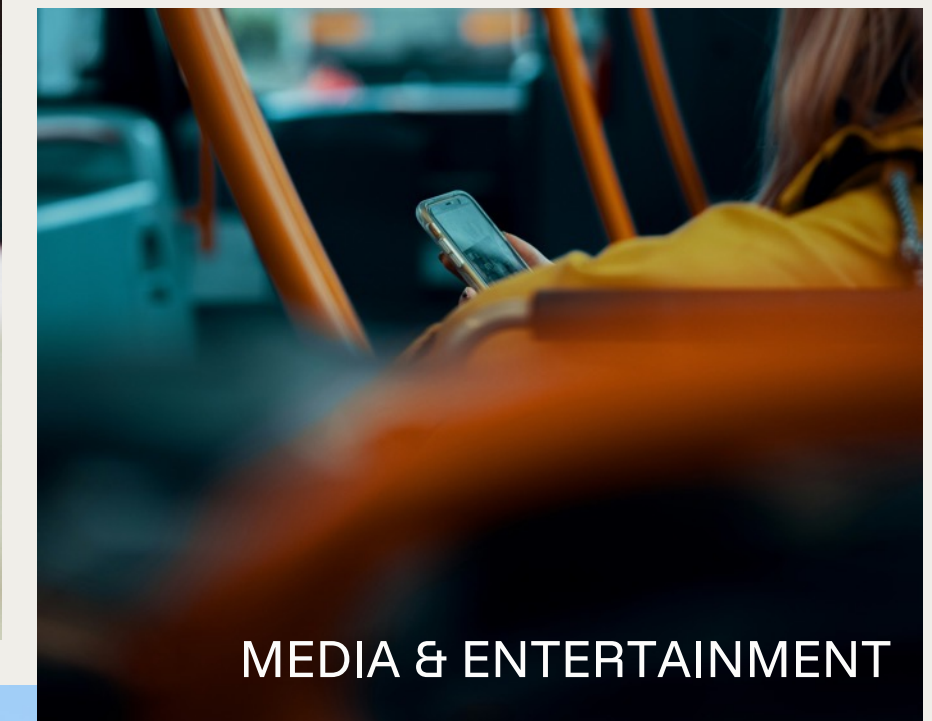
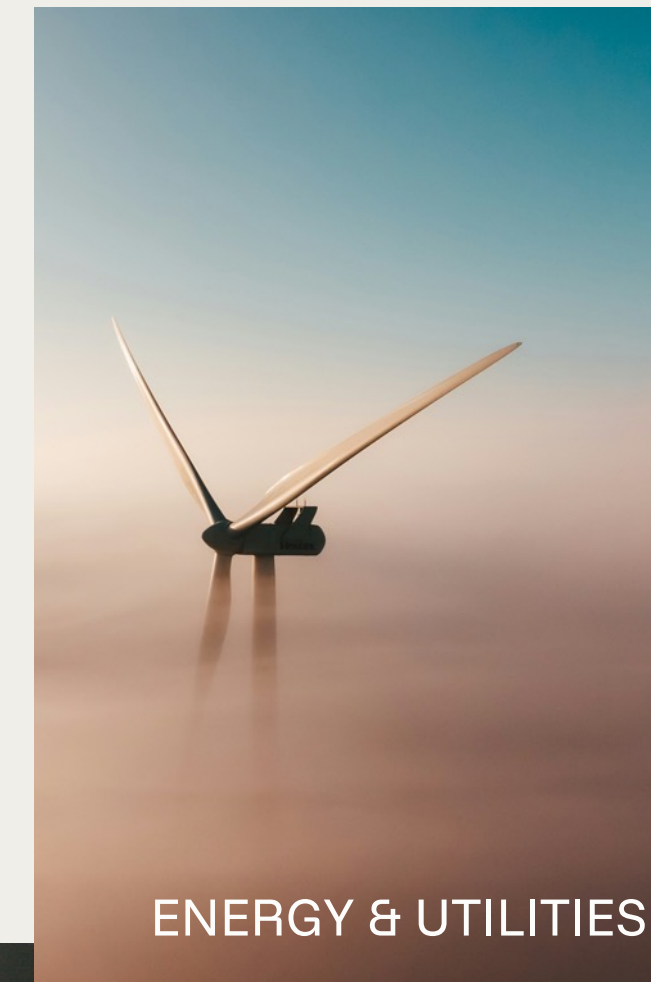
About Softwire

Softwire is a digital and technology consultancy that works with organisations to design, build, and improve digital services.

We support teams across the public sector with work ranging from discovery and delivery through to data, cloud, and AI-enabled services. Our focus is on solving real problems, working collaboratively, and delivering work that stands up to scrutiny.

We take a pragmatic approach to AI, helping organisations explore where it can add value, put appropriate controls in place, and integrate it safely into existing services and ways of working.

G-Cloud 15 Services



Our Capabilities

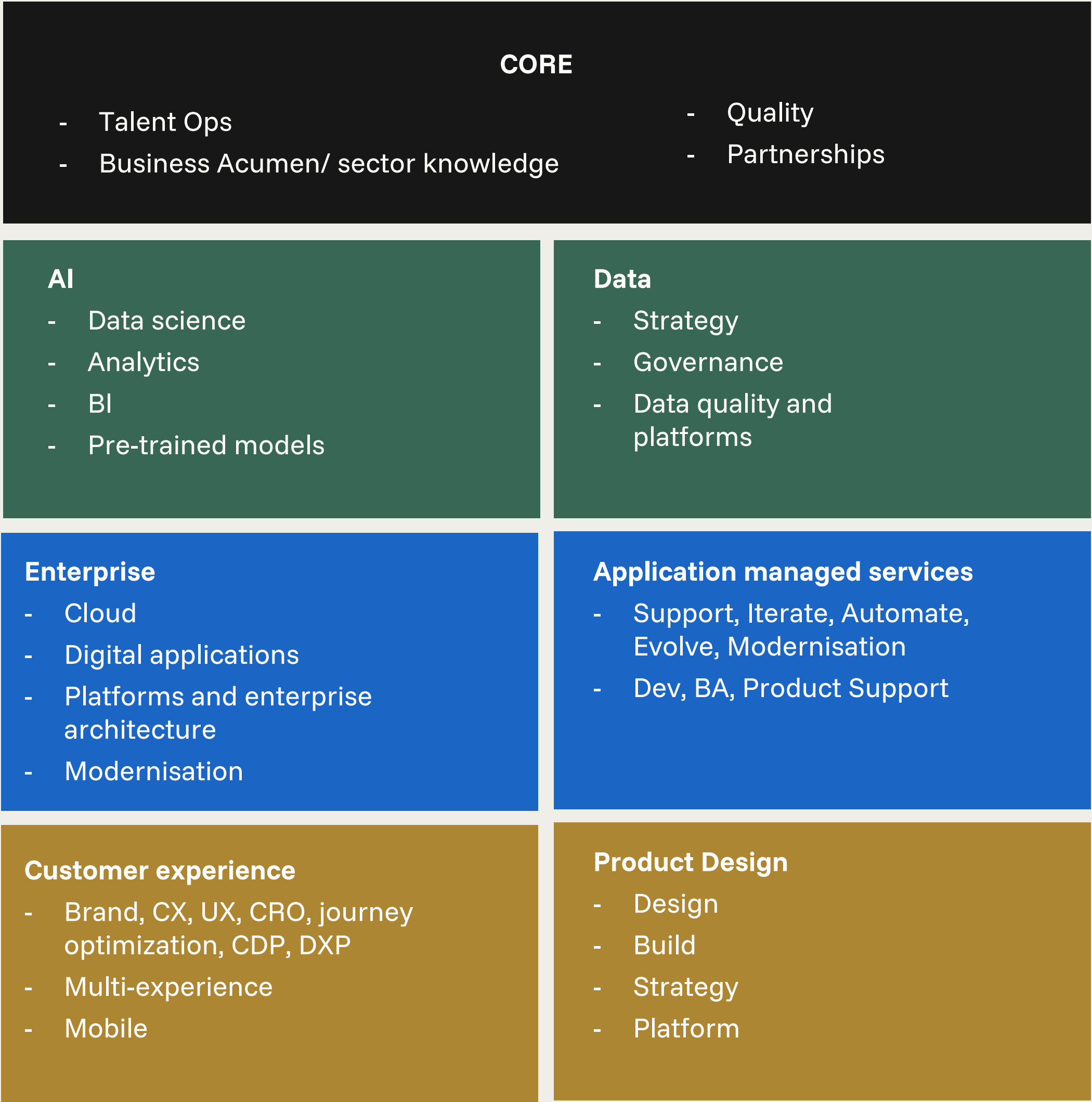
We have expertise across multiple sectors

Our multi-skilled cross-functional teams offer full-lifecycle management and ownership of outcomes across a range of domains, using a range of specialisms.

 Enablers

 Brand, Differentiated Experience, Engagement Revenue

 Optimisation, Modernisation, Continuous improvement



Working in the the public sector

We have experience delivering work across central government, arm's length bodies, and the wider public sector.

Our teams are used to working within public sector constraints, including governance, assurance, procurement, and delivery standards. This includes supporting the responsible use of data and AI, with appropriate oversight, transparency, and risk management.

We work closely with policy, operational, and delivery teams, adapting our approach to fit existing processes, capability, and levels of confidence with emerging technologies.

G-Cloud 15 Services



Thank you for reading

Contact us

Email: info@softwire.com

Phone number: +44(0)207 485 7500

Address: 315 Highgate Studios, 53-79 Highgate Road, London, NW5 1TL