SUPER CHARGE

G-Cloud 15 (RM1557.15)
Supercharge London Ltd.

# Cloud-Native Application Modernisation Services

## Service Definition

# Table of contents

# 1 Introduction

This Service Definition document provides information about the Cloud-Native Application Modernisation Services offered by Supercharge London Ltd (Supercharge) under the G-Cloud 15 Framework. We have designed this to provide clarity regarding key aspects of our company and services, including functionality, data and security, on/offboarding and pricing, management and support.

The document comprises **3 core sections**:

1. **Service description:** Provides an overview of our Cloud-Native Application Modernisation Services, outlining highlights, key features and benefits, delivery methodology and support measures
2. **G-Cloud alignment information:** Details how our services are delivered under the G-Cloud 15 framework, covering purchasing, onboarding/offboarding, data and security concerns and governance
3. **Supplier information:** Summarises our company background and how to procure our services through G-Cloud

To quickly locate the information most relevant to your stage in the procurement process, use the clickable table of contents provided on the previous page.

# 2 Service description

## 2.1 About our service

Through our Cloud-Native Application Modernisation Services, we help public sector organisations replace ageing, high-risk legacy systems or introduce new systems. We design, build, and launch new systems and support transitions to secure, cloud-native solutions that are accessible, adoptable, and cost-effective. Modernising critical applications without disrupting live services, our transformations reduce operational risk while improving productivity, resilience and long-term value for money.

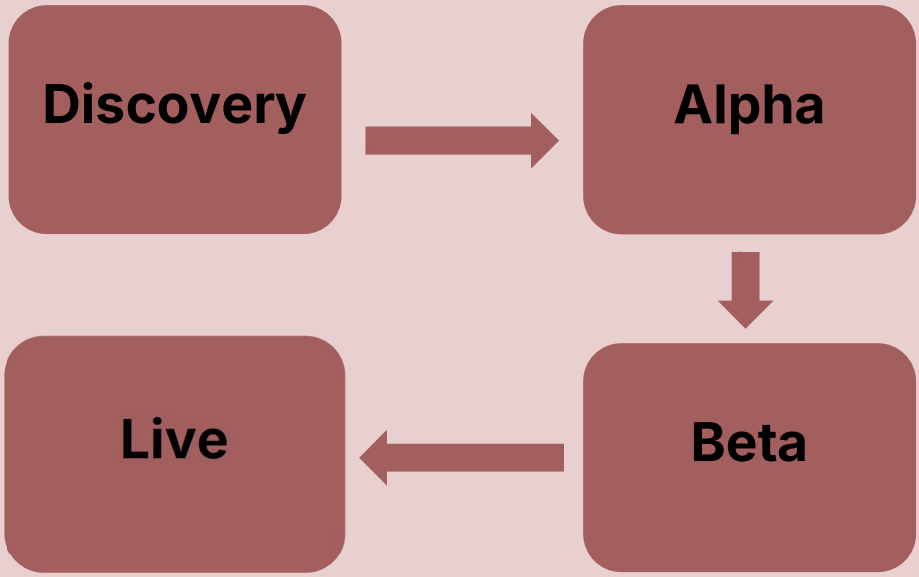
Drawing on **15+ years of experience** across cloud engineering, product design and managed support, we deliver end-to-end modernisation and ongoing support for Amazon Web Services (AWS), Microsoft Azure and Google Cloud platforms. We specialise in high-complexity platforms for regulated environments, where security, governance and performance must work together. Rather than layering controls on top of outdated systems, we design and engineer modern services aligned to Government Digital Service (GDS) standards with security, accessibility and user experience built in.

We are part of **Siili Solutions**, a National Association of Securities Dealers Automated Quotations (NASDAQ)-traded Scandinavian group focused on digital innovation. We are proud to be working with ambitious companies from Europe, the US and Asia and helping them realise their full potential. Providing confidence of security, quality and governance throughout, delivery is underpinned by recognised standards and assurance, including:

- ISO 27001
- ISO 9001
- ISO 14001
- ISO/IEC 20000-1
- Cyber Essentials Plus
- SOC 2 Type I

## 2.2 Delivery framework

We deliver our modernisation services through a phased, user-centred, Agile lifecycle that moves legacy systems to cloud platforms with minimal disruption. Providing end-to-end support, our tailored design and engineering services build early risk reduction, quality and continuous improvement into this framework. Our delivery lifecycle is outlined below:




### Discovery

To establish the current environment, desired result and steps to get from one to the other, we begin with the **Discovery phase**. Working collaboratively with our client, this begins following the agreement of initial project scope, constraints and clear project outcomes during our initial kick off call.

Identifying the main system issues to inform either an improvement plan for an existing application or a solution mapping for a brand-new system, our Design Team:

- Conducts user research
- Runs stakeholder interviews
- Reviews the existing application flows and pain points
- Maps critical user journeys, data flows and workflow gaps/bottlenecks
- Identifies security and compliance constraints together with our technical team

To clearly present findings, we produce our Discovery Outcomes. Bespoke to each project, these may include:

- User research key findings
- User interview outputs
- Existing application audit inputs
- Approved user journeys for the new/improved tool
- A functional breakdown of the target cloud-native architecture
- Design and development estimates with a project plan and timeline

### Alpha

Following Discovery, to reduce risk and validate our proposal, we recommend running a focused **Alpha stage**. In practice, this means prototyping the riskiest user journeys and validating them with users, while running technical sprints to confirm the approach for the final system architecture, the integrations needed and the potential migration if required.

Alpha enables us to prove feasibility, refine assumptions and agree the target architecture, user flows and delivery plan before committing to Beta.

### Beta

During the **Beta** phase, we build the system in iterative Agile cycles. This stage includes turning user-centred designs into working software with modernised application components, released incrementally.

In parallel, we set up delivery and operational foundations such as CI/CD pipelines, infrastructure-as-code and container deployment, enabling repeatability of releases. Building quality into the process, automated testing is conducted across functional, integration, performance, and accessibility checks.

Enabling us to learn and iterate with minimal disruption, we address legacy replacement and roll out fixes to users in a controlled way. Additionally, we proactively fix bugs within the cycle, instead of addressing them retroactively once live.

### Live

Once the product is **Live**, to drive continuous improvement, we refine the solution based on user feedback and operational data. For stability, accessibility and scalability, we prioritise the backlog, then turn to performance tuning, cloud cost management, security strengthening and other enhancements. This process is led by the client's Product Owner, customer feedback or suggestions our Product Leads put forward based on testing and research.

Adding value, we provide ongoing maintenance and L1-L2-L3 support at a level agreed with our client, enabling teams to operate and evolve the service continually.

## 2.3 Service highlights

**Designed to maximise productivity in complex, regulated environments**: Refusing to sacrifice user experience to meet governance requirements, our solutions are engineered for performance and accessibility alongside security.

**End-to-end delivery from a single, accountable partner:** Removing handover risk and simplifying governance, we act a single point of contact and responsibility across strategy, service, product design and ongoing live support.

**User adoption driven by behavioural insight:** Using our habit-forming design framework, we combine behavioural psychology with user-centred design to help public sector teams deliver services that citizens, service users and internal staff actually use.

**Long-term cost control and savings:** We work openly and efficiently, giving buyers control over roadmaps and outcomes. Clients retain IP ownership, and our end-to-end delivery approach reduces duplication when scaling, facilitating long-term total cost of ownership.

**Strong engineering and exceptional product design:** Our teams combine deep technical expertise with award-winning product and service design. Demonstrating how our solutions are not just technically robust, but genuinely usable and adopted, we have delivered over 200 digital products used by more than 20 million people globally.

**Provider-neutral engineering:** Selecting platforms based on security, compliance and cost requirements rather than vendor preference, we design and build services across AWS, Azure and Google Cloud.

**Dynamic solutions:** Our flexible delivery model supports complex constraints such as legacy systems, governance, security and data quality. With ongoing support and refinements post Go-Live, we help organisations launch confidently and continue evolving services safely as needs, policy and demand change.

## 2.4 Service features and benefits

### 1. Discovery-led capability review

Our Discovery phase includes a comprehensive capability review and assessment of legacy infrastructure, dependencies and objectives. Whether creating new products or transforming existing systems, we help clients to map out their desired solution and create a roadmap for turning this into reality. We build a clear picture of technical risk and improvement opportunities, with user and stakeholder feedback informing our understanding of the client's current vs desired features, user flows, systems and operations. This:

- Reduces uncertainty at the outset of delivery
- Identifies constraints, assumptions and risks early before they can impact timelines or outcomes
- Enables more accurate planning, clearer prioritisation
- Ensures informed decision-making
- Improves client confidence that our choices are grounded in operational reality
- Reduces the likelihood of rework and associated costs
- Focuses investment where it will deliver the best value

### 2. Cloud-native architecture/platform design

Designing products that are secure, scalable and future-ready, we create cloud-native architectures aligned to public sector standards and buyer platform preferences. Our approach supports deployment on major cloud environments, such as AWS, Azure and Google Cloud Platform, while remaining vendor-agnostic.

Through this design-led approach, we ensure solutions are tailored to each client's technical landscape, operational model and risk appetite. We enable buyers to adopt the most appropriate solution rather than being constrained by a single technology choice.

### 3. User-centred, accessible platforms

Ensuring our solutions are usable, inclusive and adopted, we apply user-centred design principles throughout. Our activities include interviews during Discovery, user testing during Alpha and continuous refinements once live operating with real users, adjusting our solution dynamically based on user feedback and operational data.

This improves user satisfaction, reduces avoidable support demand and ensures compliance with Web Content Accessibility Guidelines (WCAG) standards. Clients benefit from solutions that are easier to adopt and use, and more likely to deliver their intended outcomes.

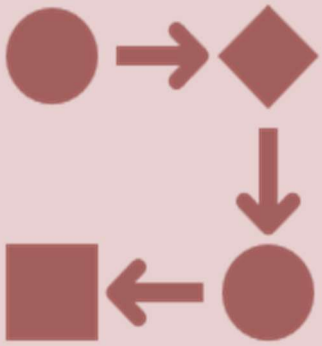
### 4. Migration planning and management

Our end-to-end, hands-on teams aim for minimal disruption migration and modernisation planning. To reduce disruption and support continuity of existing services whilst working on a new or improved solution, we manage data movement, system dependencies and cutover approaches, leveraging a phased delivery. This is backed up by a responsive Support Team available 24/7/365, who, using our ticketing support system, monitor the solution and ensure customers experience no downtime during implementations. This:

- Protects business continuity
- Reduces the likelihood of service outages during changeovers
- Enables clients to modernise systems with confidence that critical services won't be impacted
- Provides streamlined, round-the-clock access to support as-and-when required

### 5. Agile, iterative delivery of components

Delivering progress in visible, manageable increments, we use agile delivery to release working components early and frequently. This allows buyers to validate assumptions, reprioritise based on evidence and respond to emerging requirements.



Through Agile delivery, we:

- Reduce risk of misalignment or rework
- Accelerate time to value
- Provide clients with transparency and improved control
- Ensure solutions evolve in line with real-world feedback, rather than fixed assumptions made at the outset
- Uphold our user-centric approach

### 6. DevOps practices and CI/CD automations

Improving reliability and reducing operational overhead, we implement DevOps practices including automated testing, CI/CD pipelines, container deployment and infrastructure-as-code.

This enables consistent, repeatable releases and faster recovery from issues, with clients benefitting from improved solutions stability, reduced deployment risk and lower ongoing operational effort. Streamlining processes, services become easier to maintain, replicate/scale and update without introducing unnecessary risk.

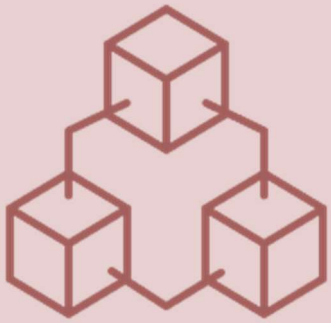
### 7. Integrated security and quality testing

Embedding assurance throughout delivery, we integrate security and quality testing into every stage of the lifecycle. Security is treated as a design consideration rather than a late-stage check, with controls aligned to secure-by-design principles and ISO27001-certified processes.

Similarly, automated and manual quality testing provides confidence that services are robust, compliant and ready for live use, reducing the risk of vulnerabilities, defects or instability during Alpha and Go Live. Benefits of this approach include:

- Stronger overall security and compliance
- Reduced operational risk through early defect detection
- Improves stability and uptime of live services
- Safer deployments and clearer go-live decisions
- Builds confidence that quality will be maintained end-to-end, as services evolve

### 8. API-first integration and interoperability



Supporting joined-up public services, we design solutions using API-first principles to enable secure, scalable integration across systems. This reduces silos, improves data flows and supports interoperability between platforms, suppliers and departments.

By enabling modular integration, services can evolve independently without introducing unnecessary coupling or risk, supporting long-term flexibility and reuse. This improves end-to-end workflows and user experience across systems and teams, reduces duplication and supports interoperability across organisational boundaries.

### 9. End-to-end support and ongoing maintenance

Ensuring services remain stable, secure and operational throughout their lifecycle, we provide structured end-to-end support and maintenance during and after delivery. Designed to suit and scale with service criticality, our support is underpinned by clearly defined escalation paths and response processes.

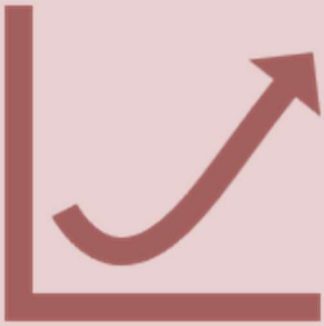
We provide access to L1, L2 and L3 support (detailed in section 2.6), ensuring issues are triaged and resolved by appropriately skilled specialists. Users can raise incidents and service requests through email or our ticketing system, with issues logged, prioritised and tracked through to resolution. For live

services, we maintain a 24/7/365 incident reporting channel, ensuring support is available when it is most needed.

Clients benefit from:

- Reliable access to round-the-clock support through defined channels
- Effective incident handling through structured P1-4 escalation
- Reduced downtime and disruption through timely issue resolution
- Confidence that products are actively managed and supported once live

## 10. Post Go-Live optimisation



Beyond initial delivery, we support continuous optimisation of live products, refining them based on end-user feedback, performance data, usage patterns and operational insight. This includes tuning performance, optimising cloud spend and strengthening security controls over time. By fine-tuning based on real-world evidence and clients' needs, we ensure solutions remain efficient, resilient and cost-effective as demand and requirements change.

These post-delivery improvements mean our clients benefit from ongoing strengthening of user experience and security, and a service that refuses to stagnate.

## 2.5 Service scope

### Service constraints

Providing buyers with transparency upfront, we require certain practical conditions to operate our services, which are delivered through close collaboration with client teams. For delivery to proceed effectively, we need:

- Timely access to client stakeholders and subject-matter experts, including business, technical and governance representatives, to support discovery, decision-making and validation activities
- Access to relevant systems, environments and documentation, as agreed in the Statement of Work, including legacy platforms, interfaces, operational processes and historical data of preexisting operations conducted
- Appropriate permissions to deliver tooling and environments, such as cloud accounts, code repositories, CI/CD pipelines and monitoring or logging tools, where development, testing or deployment activities are part of the scope

Where access or availability is delayed, delivery timelines and sequencing may be impacted. We mitigate the risk of this through collaborative early planning. We outline clear dependency points with clients and establish protocols for fluid communication between parties.

### System requirements

Our Cloud-Native Application Modernisation Services do not require specialist hardware or prerequisites. Our extensive in-house capabilities enable us to develop and modernise applications across all major platforms, including:

- **Mobile:** Native iOS and Android development, plus cross-platform expertise in Kotlin Multiplatform, React Native, Flutter and other modern frameworks
- **Desktop:** Windows and macOS applications
- **Server:** Windows Server and Linux-based systems

System requirements depend on the type of modernised application delivered, with typical minimum baselines outlined below

- **Simple API service:**
  **For cloud-hosted API services**
  CPU: 250m (millicores) request, 500m limit
  Memory: 512MB request, 1GB limit
  Storage: 1-2GB ephemeral storage
- **Web application-fronted:**
  Windows 10+, macOS, or Linux
  Modern browsers (Chrome, Edge, Firefox, Safari - latest 2 versions)
  Minimum 4GB RAM, dual-core processor
  Internet: 2 Mbps minimum, 5+ Mbps recommended
- **Mobile application:**
  iOS 15+ or Android 10+ Minimum 2GB RAM
  Internet: 2 Mbps minimum, 5+ Mbps recommended

Where the modernised service integrates with buyer-owned third-party systems, the buyer is responsible for maintaining any required licences or subscriptions. For example, Microsoft 365 for Dynamics 365 integrations, or licences for CRM, CMS, analytics or monitoring platforms.

## 2.6 User support

For efficient and effective user support, we provide a structured, responsive service aligned to ITIL4 best practices. **Supercharge Support Team** comprises**:**

- **23 L1 Technical Support Agents**
- **6 L2 Reliability Engineers**
- **L3 Application Engineers, assigned per project**

These agents are responsible for providing **24/7/365 service**. Additionally, each client is assigned a dedicated **Service Operations Manager**, who acts as their key escalation contact. All of our Operated Services are overseen by our **Lead Service Operations Manager** and by our **Head of Operations**.

Offering a tailored approach, support is designed to scale based on buyer needs. Both during delivery and for ongoing assistance, our model can be adjusted from standard (for example, 9 am – 5 pm, Monday-Friday availability) to full 24/7 coverage.

As the level of ongoing support required is best understood once the solution is live, we typically contract this separately. This way, we can provide an initial estimate, then agree on the support scope and commercials based on operational needs and usage.

### Support channels

To manage customer interactions, we use Zendesk's telephony and web chat management software. Leveraging our omnichannel tooling and capabilities, buyers can contact the Supercharge Support Team through:

- Email
- Online ticketing (tied to emailing services)
- Telephone, using Zendesk's built-in telephony and call centre tooling
- Web chat, through Zendesk, with information provided by our Service Management Toolkit

Ensuring visibility, auditability and appropriate triaging, we log, prioritise and track all support requests through the ticketing platform. Clients can manage the priority status of tickets by raising them as a priority with their Service Operations Manager.

### Support availability

We can provide up to 24/7/365 support for L1 and L2, with standard working hour coverage for L3. However, response and resolution times may vary depending on customer demand and the agreed support package. Supercharge Support Team's maximum availability is as follows:

- **L1 (Technical Support):** 24/7/365 availability in standard 8-hour shift patterns
- **L2 (Advanced Infrastructure Support):** 24/7/365 on-call rotation
- **L3 (Application Support):** 9am-5pm CET, Monday to Friday, Hungarian Business Days

## Response times

We operate a priority-based support model with response and resolution times defined for P1–P4 incidents and requests. Our standard service level commitments are as follows:

**L1 – Technical Support:**

Technical Support Agents are available 24/7/365, with staff working in 8-hour shift rotations. P1-4 Technical Support queries are **responded to immediately** and **resolved at the port of call**. If immediate resolution is not available, the Agent passes the query to the L2 or L3 team. This is consistent across weekdays and weekends.

**L2 – Advanced Infrastructure Support (Reliability Engineers):**

- **P1:** Response within 1 hour, resolution within 8 hours
- **P2:** Response within 4 hours, resolution within 24 hours
- **P3:** Response within 24 hours, resolution within 5 days
- **P4:** Response within 2 days, resolution within the next scheduled release

These response and resolution timescales are consistent across weekdays and weekends.

**L3 – Application Support (Application Engineers):**

- **P1:** Response within 4 working hours, resolution within 2 working days
- **P2:** Response within 1 working day, resolution within 3 working days
- **P3:** Response within 2 working days, resolution within 5 working days
- **P4:** Response within 5 working days, resolution within the next scheduled release

L3 support is primarily available on weekdays during working hours CET, Hungarian Business Days. However, providing backup for emergencies, we maintain a wider resource pool of Developers who can be reallocated to resolve urgent L3 issues.

## Escalation and management

Our Service Operations Managers function as key escalation contacts. We apply ITIL4 processes across incident management, major incident handling, request fulfilment and problem management. For ongoing engagements, we manage and refine our support approach through:

- **Weekly ticket review calls** with an operational focus
- **Monthly service review meetings** with a tactical focus
- **Quarterly service reviews** with a strategic focus

## 2.7 Service accessibility and usability

We embed accessibility and usability throughout the design, delivery and operation of our Cloud-Native Application Modernisation Services. Considering this from the outset, we develop user-centred designs, based on approved user journeys and real-person feedback from our Discovery phase.

During Beta and Alpha phases, we perform accessibility testing, with automated accessibility checks forming a part of our quality assurance process and potential barriers being identified and removed proactively.

Whilst on production, we continue to improve accessibility and usability based on user feedback and operational insight, feeding improvements into the prioritised backlog for ongoing enhancement. Additionally, we can provide user-friendly training and a comprehensive digital and printable handover pack to enable effective day-to-day adoption and seamless use of the products we design and build for clients.

Ensuring users can engage with support in a way that best meets their needs, all service interfaces and user-facing support channels, including online ticketing and web chat, meet accessibility standards. We aim for anyone accessing with assistive technology, such as screen readers/keyboard navigation, to have a successful and positive experience.

Our provider, Zendesk, maintains a robust Product Accessibility Policy that **exceeds the WCAG 2.2 AA industry standard**. Built on Zendesk's accessible Garden design system, our support functions have undergone both manual and automatic testing. Web chat accessibility testing, conducted on our behalf, includes:

- Formally consulting with agents, admins and end users who rely on assistive technology to collect feedback
- Accepting customer/end-user feedback through a variety of channels
- Using all feedback to inform improvements
- Retesting products following remediation and new feature updates
- Engaging third-party auditors to conduct regular compliance audits of their products

## 2.8 Service levels and availability

Providing a tailored approach, service levels and availability are agreed in collaboration with the client following Go-Live, to ensure these are bespoke to the final product and client needs. Service performance is monitored continuously by the Service Operations Manager and reported in an agreed upon format at an agreed upon frequency.

Fostering transparency, we present our performance during weekly ticketing review calls, monthly service review calls and quarterly service reviews.

A breakdown of key service level commitments we measure as a minimum can be viewed below:

| Metric | Service level/target | Measuring and reporting |
|---|---|---|
| Service availability | Agreed per engagement, typically 24/7/365 for L1-2 and 9 am-5 pm CET, Hungarian Working Days for L3 | We monitor tickets and report response and resolution times during weekly reviews with clients |
| Incident response times | Incidents are prioritised from P1-P4, with response targets defined for each support level (L1-L3) | All incidents are logged using our omnichannel ticketing platform. Response and resolution times are tracked automatically through Zendesk and reported on during review calls and meetings |
| Incident resolution and request fulfilment times | Resolution/fulfilment times are defined by and measured against the hourly/daily targets we set for each priority (P1–P4) as part of standard service level commitments | Ticket lifecycle data is captured within Zendesk, resolutions are logged manually, and performance is assessed during review meetings |
| Downtime | 99% uptime | Major incidents are tracked end-to-end, with status updates, post-incident reviews and corrective actions documented and shared for future prevention |

Preventing slippage, the Service Operations Manager proactively monitors performance against these service levels. If they identify risks, such as a rising number of incidents responded to outside of agreed-upon timescales, they will take action immediately. For example, assigning additional Support Desk Agents to the contract.

Reacting appropriately to any breaches of SLA targets, slippage or failure to meet agreements triggers internal escalation to the Service Operations Manager. They will manage escalations on a case-by-case basis, developing and implementing action plans for rectification with minimal disruption. This process is informed by ITIL4 best practices.

Driving continuous improvement, we will use slippage or breaches as a learning experience, dissecting root causes, the effectiveness of our resolution and outcomes to inform future delivery.

# 3. G-Cloud alignment information

This section explains how the service is delivered, managed and supported once a buyer has purchased it through the G-Cloud framework. This includes how we onboard and support buyers, manage data securely, ensure service resilience, monitor performance, and provide training, support and controlled offboarding. Together, they set out how client and supplier teams work in partnership to deliver outcomes safely, efficiently and in line with G-Cloud 15 requirements.

## 3.1 Onboarding and offboarding processes

### Onboarding

To align expectations, each engagement begins with a collaborative onboarding process, where we discuss all the engagement details to ensure these align with the client's expectations. By clarifying the objectives, scope, governance and approach before activity begins, we reduce risk and establish a collaborative foundation for successful delivery.

Our onboarding process includes:

#### Internal and external alignments

1. **Scope of Work (SoW) confirmation:** Meeting with key representatives from the client's side, we establish scope, deliverables, objectives, constraints and success indicators (KPIs and SLAs if needed). This provides a shared reference point for measuring progress and performance, aligning expectations from the start.
2. **Commercial confirmation:** As our pricing model is tailored to each engagement, based on the scope and required outcomes, we cement the commercial terms following scope confirmation. This includes defining the exact Fixed Price or Time and Materials (T&M) quote and invoicing preferences. At this point, we draw up and co-sign a contract with the client.
3. **Indicative timeline & team allocation**: As part of our pre-sales discussions, we share a prospective timeline to confirm how quickly we could deliver the project based on the scope. Though our initial timeline is indicative, it can estimate project length and volume. We plan resourcing internally, selecting the best team for the project based on experience and skill sets and securing them for the duration, and sync internally to prepare for kick off.

#### Project kick-off

4. **Kick-off session**: After internal preparation and onboarding the team, we book a project kick-off with the client. The goal of this session is to meet, present the detailed project approach, ways of working and planning, and align on next steps for efficient progress. This session includes:
    a. **Team introductions:** Based on the SoW, we create a dedicated team comprising a Project and Account Manager and all the Digital Experts (with project-specific specialities required for the project). We introduce our key personnel and ask our clients to assign and introduce key people, including:
        - A named product owner or point of contact to manage day-to-day alignment, unblock issues and give official approvals on the milestones

        - Optional: Business and technical stakeholders for decisions, prioritisation and approvals also tend to join (if closely involved)
    - Subject Matter Experts (SMEs) for discovery interviews, requirements clarification and regular testing (no need to join but need to be assigned)
        - End users for research, usability and accessibility testing also need to be assigned

b. **Access and setup:** The client provides access and appropriate permissions for documentation, environments, assets and tools. During the kick-off, we align on which accesses are needed for the specific project. When we are creating new products, we typically require access to previous research materials and related tools. For existing solutions, we require access to:
    - Current architecture
    - APIs
    - Data models
    - Security policies
    - Operational runbooks
    - Cloud accounts
    - Repositories
    - CI/CD
    - Logging/monitoring software
c. **Ways of working**: We establish communication preferences and details for key points of contact on all sides, outlining how the project milestone reviews and approvals will be handled. For robust planning, we also outline client input needed and establish their availability for meetings and ad hoc communication/queries.
d. **Delivery planning:** We agree on indicative timelines, establish key milestones and review points in line with the agreed delivery lifecycle. For example, outlining indicative dates for the completion of the Discovery phase and design/development milestones.

### Project opening: Discovery

5. **Discovery:** Completing onboarding and kick off, we begin the Discovery process, co-creating requirements and outlining in collaboration all the product features and user journeys to create the desired solution. During Discovery, we apply our Change Control Procedure for any required amendments to the SoW, ensuring everything is fully detailed, planned and quoted before commencing Alpha and Beta/design and development phases. The Discovery phase length varies depending on the scope, size of the solution and client's previous preparation work: it can last anywhere from a week to a few months.

### Offboarding

After the initial phase (including Discovery, Design, and Development of the solution agreed upon), we reconvene with the client to discuss further support for lifecycle product enhancements or maintenance/troubleshooting.

If we are to continue partnering, for optimal collaboration, we discuss a new support agreement, which may include:

- Production environments support and monitoring to ensure good performance (with our L1, L2 and L3 services)
- Product maintenance and enhancements, with a dedicated or ad-hoc team of digital experts depending on client's demands

If support, maintenance and optimisation functions will be provided in-house, with the client's own teams, we conclude the engagement with a structured handover and offboarding process to:

- Facilitate a smooth transition into operation
- Enable sustained, effective day-to-day use
- Confirm we have met all deliverables and targets
- Transfer full ownership to the client
- Ensure organisation-wide knowledge, understanding and adoption
- Revoke our access to systems and data

Offboarding typically comprises the following steps:

1. **Project closure review:** After official Go Live, we arrange a project closure review with all key stakeholders to confirm all deliverables have been provided/objectives met and assess performance against agreed success criteria (KPIs).
2. **Optional training:** Supporting adoption, offboarding could include an **intensive training programme** of knowledge-sharing sessions. Enabling client teams to use the platforms without external support, our experts deliver live remote and in-person sessions, with recorded materials to support long-term continuity.
3. **Documentation:** We provide a central Handover Pack containing comprehensive technical documentation, such as:
    - Architecture diagrams
    - Infrastructure-as-code
    - Runbooks
    - Operational procedures
    - All credentials, integration points and dependencies
    - Training materials

    Exact documentation and training materials to be provided will be agreed with the client.
4. **Data return:** Following our **ISO27001-accredited procedures**, we identify all storage locations, extract data in agreed formats and validate completeness. We either transfer ownership of cloud resources or securely destroy data, verifying through destruction certificates if required.
5. **Account closure:** Revoking our access to your systems, we remove service accounts and integrations, decommission temporary infrastructure and provide formal, co-signed confirmation of access withdrawal and data deletion. We retain audit logs in accordance with our Document Retention Policy, which is outlined in the original contract, keeping anonymised client data for a required period.

6. **Intensive post-Go-Live care:** Whether the client opts for support or not, we offer a hypercare month after Go-Live, ensuring we keep our team available for any unexpected issues.
7. **Ongoing support assessment:** Ensuring post-engagement assistance proportionate to operational usage and client needs, we assess and agree on a continued optimisation and advisory support package through a new SoW if the client wishes to continue the collaboration. Our post-go-live agreements may include:

    - **Production support**, with our L1 and L2 teams available on a 24/7 window and our L3 team, during working hours
    - **Maintenance** and **Optimisation**: we make changes and enhancements after Go-Live based on user feedback and operational data, either with a dedicated team or ad-hoc

## 3.2 Data

### Data importing, exporting and deletion

Data is shared as part of the engagement, but rather than uploaded or provided through a portal, our clients provide access to data sources, systems and datasets required to deliver the project, with the necessary permissions.

Clients may request data extraction at any point during the engagement or at contract end through a written request to the provided contact email. To minimise access and risk, all data handling follows a least-privilege approach. By default, data is provided as database exports or CSV files, using open, non-proprietary formats that support portability and reuse. Where required, to meet client preferences, export formats can be adjusted. To ensure data confidentiality and integrity, all exports are delivered using encrypted transfer.

Following our ISO27001-accredited procedures, we use certified secure wiping methods for deleting media and cloud-stored data, offering physical destruction with certificates where applicable. Additionally, **active systems are purged within 30 days of contract end** or deletion request, with **backups deleted 90 days post-contract** (unless legally required to be longer).

### Data at rest

Protecting data at rest, we ensure secure data storage and location cloud infrastructure through AWS, Google Cloud Platform and Microsoft Azure. For flexibility, Regions can be configured based on client requirements. Sensitive data at rest is encrypted under A3/A4 classification, and we store business data exclusively on approved corporate systems, such as Google Drive and approved SaaS platforms. Backups to cloud storage are securely encrypted and tested annually by our Data Protection Officer.

Securing assets, we implement access controls, including Okta Multi-Factor Authentication (MFA), which is enforced across all systems. Our Password Policy requires all passwords to:

- Contain a lower-case letter and an upper-case letter
- Contain a number (0-9) and symbol (e.g., !@#$%^&*)
- Not contain part of the username, first or last name
- Not be a ‘common password’
- Have a minimum of 8 characters
- Not be one of the user’s last 4 passwords
- Be changed every 90 days
- Lock after 20 unsuccessful attempts (brute force protection)

We apply the **Principle of Least Privilege** for access to all assets and store privileged credentials in a secure vault. Minimum necessary access is granted per project, per developer, and logical segregation is maintained between client environments. Preventing cross-client exposure, we segregate client data by storing it under the given cloud provider (AWS/GCP/Azure) in a separate account dedicated and owned by the client. We maintain detailed logs highlighting who has access to which client data, which are available for auditing and review by senior staff.

Our Network Security includes:

- Network segmentation, separating development, testing, and production environments
- Border firewalls to disable unused ports and protocols
- Real-time malware protection with automatic updates
- Vulnerability patching, occurring within 30 days of disclosure

Client data is prohibited on personal devices or personal cloud storage, and remote access on authorised devices requires VPN connection through Tailscale, our trusted partner.

### Data in transit

To protect data in transit, we use mandatory TLS/SSL encryption. All confidential email attachments and sensitive data transfers are encrypted, with passwords sent through a separate email or communication. Minimising risk, we only use mock or anonymised data in non-production environments.

## 3.3 Business continuity and disaster recovery

The service is designed to be highly available, resilient and recoverable. We ensure continuity of service even in the event of infrastructure failures, security incidents or other adverse circumstances as specified in our Operational Ways of Working document. Our 24/7 teams, who are always available to investigate and resolve issues when flagged, further support our continuity approach. Evidencing the robustness of our services and policies, we have never encountered a long-lasting major service disruption or business continuity issue.

As the delivery of our services does not rely on a single physical location or system, business availability is unlikely to be compromised. Work is delivered using secure, cloud-based environments provided by major platforms with regions configurable to UK or EU requirements. We maintain backup resources, allowing capacity to be flexed and reallocated quickly if individuals, locations or systems are unavailable.

Strong security controls, including encryption, access management, continuous monitoring and incident response procedures, further reduce the likelihood of disruption caused by security incidents. This combination of decentralised resources, cloud infrastructure, resilient system design and mature operational controls significantly lowers the risk of continuity incidents and supports rapid recovery.

For business continuity and resilience, we implement the following measures:

- **Incident response:** For rapid rectification of issues, we maintain documented incident response procedures. This includes our Business Continuity Plan (BCP) and Supercharge Operational Procedures. For ongoing preparedness, our Head of Operations reviews our BCP annually, and it is tested at least annually. Ensuring consistent knowledge across our teams, we provide incident training upon induction, refresh learning annually and confirm agreement with these policies. Additionally, our Service Operation Teams (including all service levels) have a recurring tabletop exercise system on a half-yearly basis.
- **Redundancy and recovery:** Enabling systems to continue to function despite failures, we practice redundant system design. This includes load sharing, using multiple cloud regions/availability zones and backup systems. For rapid recovery, we maintain documented and formalised system restore and reboot processes.
- **Offsite storage:** Encrypted cloud backups are stored geographically separate from primary systems.
- **Crisis management:** We maintain a 24/7 incident reporting channel, with the Supercharge Support Team aiming to rectify issues within 1-4 hours (P1) – 2-5 days (P4). This includes L1, L2 and L3 live service capability from expert Agents and Engineers.

### Disaster recovery and rectification

For timely restoration of service following an incident, we maintain formal disaster recovery targets, these are as follows:

- **Recovery Point Objective (RPO):** Up to 24 hours using standard daily backups (configurable to shorter intervals)

- **Recovery Time Objective (RTO):** System-dependent and verified through annual recovery testing

If requested (encountering additional costs), critical systems can be configured with shorter RPO/RTO targets through more frequent backups and redundant architecture. Ensuring predictable and repeatable recovery, our system restore and reboot procedures, including timescales, are documented, tested and formalised.

## 3.5 Governance

### Accreditations and certifications

Demonstrating the robustness of our management system and alignment with industry standards, the following accreditations and certifications underpin our services and delivery:

- **ISO 9001:** Quality Management Systems
- **ISO 14001:** Environmental Management Systems
- **ISO/IES 20000-1:** IT Service Management Systems
- **ISO 27001:** Information Security Management Systems (ISMS)
- **Cyber Essentials**
- **Cyber Essentials Plus**

Adding value, we uphold secure management of customer data in our delivery processes by aligning with SOC 2. Applying secure-by-design principles and SOC Trust Services Criteria, we protect data with resilient systems, particularly suited to public security needs. Evidencing compliance with this framework, we completed and passed a **SOC type I audit** in 2022.

## 3.4 Security

Protecting customer systems and data and supporting regulatory compliance, we build security into every aspect of our delivery. Our ISO27001-accredited ISMS, Cyber Essentials Plus certification and SOC Type I assurance evidence robust security management across people, processes and technology.

Combining preventative controls, active monitoring and defined response procedures, we instil confidence that security risks are managed proactively, with incidents managed efficiently and effectively.

### Operational security

Minimising the likelihood of security incidents, we embed operational security controls into day-to-day delivery and service management. Live services are protected through structured practices, including:

- **Secure change and release management:** Reducing the risk of vulnerabilities or service instability during updates, we manage changes to systems and configurations through controlled processes. Our methodology is supported by peer review, testing and approval workflows
- **Vulnerability and patch management:** We protect systems against emerging threats and reduce exposure to known weaknesses by actively monitoring for newly disclosed vulnerabilities, applying security patches within defined timeframes. Additionally, we partner with external vendors, such as Silent Signal or the client's preferred vendor, for annual penetration testing
- **Monitoring, logging and auditability:** Enabling early detection of unusual activity, we centrally log and manage security-relevant events across environments, including access activity and system changes. Logs are protected from tampering, retained in line with our Data Retention policy, and made available for audit or investigation on request.
- **Incident detection and response:** We maintain a 24/7/265 incident reporting channel, accessible through email or phone, with L1, L2 and L3 live service capability. Adhering to our crisis management strategy, we follow the defined incident response procedures outlined in our Supercharge Operational Procedures and BCP
- **Tightly controlled accesses:** We secure our accesses via MFA on all platforms, and we use time-based access levels (Just-in-Time Access) for production-level systems. In addition to technical measures, we review our access control and our access policy on a half-yearly basis.

### Staff security

Ensuring only suitable, trusted individuals can access customer systems and data, we apply strict personnel security controls from pre-employment to live work. This includes:

- **Pre-employment screening and confidentiality:** For security from day 1, we conduct comprehensive background screening for all staff before employment. Upon induction, we require them to sign confidentiality agreements confirming intent to comply with our policies

- **Security-cleared personnel:** For public sector engagements, we confirm/provide any additional security screening requirements. For example, UK-based experts screened in line with BS7858:2019 and up to and including Developed Vetting (DV), subject to authority requirements
- **Security training and awareness:** Fostering company-wide awareness of security legislation, controls and responsibilities, we mandate information security and GDPR training as a part of induction. For ongoing alignment, we deliver annual refresher training
- **Role-based, least-privilege access:** Minimising risks, we grant access to client systems strictly on a minimum-necessary basis, aligned to each employee's role and project responsibilities. We review access regularly and remove it promptly when no longer required. For any production-level access, we use Just-in-Time access methods
- **Segregation of client environments:** We prevent potential errors and misuse by limiting cross-client access, maintaining logical separation between customer environments and teams

### Secure development

To reduce security risk from the outset, we design and build systems using secure-by-design principles and a structured secure development lifecycle. We:

- **Embed security into design and architecture**, with security requirements gauged early and data protection, access control and risk mitigation measures built into solutions
- **Apply secure coding and review practices**, identifying potential issues early through automated testing for defects or vulnerabilities in environments
- **Conduct independent testing**, with regular security audits and annual penetration testing, assuring that effective, best practice measures are in place

### Identity and authentication

Preventing unauthorised access to systems and data, we enforce strong identity and authentication controls across all environments. Our approach ensures that only verified users can access services, that access is appropriately restricted and that all authentication activity is auditable. We protect identity and access through:

- **Multi-Factor Authentication (MFA):** Enforced across corporate systems using centrally managed identity services
- **Strong password and credential management:** Applying password complexity requirements, minimum length controls and regular credential rotation, with privileged credentials stored securely in a managed vault to prevent exposure or misuse
- **Role-based access control:** Assigning system permissions based on defined roles and responsibilities with least-privilege access, adjusted when roles change or engagements end
- **Just-in-Time Access control:** For production-level environments, we distribute access based on a request policy, and we grant access for a certain time period (e.g. 3 hours)
- **Controlled administrative access:** Protecting sensitive systems, we tightly restrict administrative privileges and require additional authentication controls for elevated access. All privileged actions are logged and monitored to support auditability and accountability

- **Regular access reviews:** Maintaining ongoing assurance, we conduct periodic access reviews to confirm that permissions remain appropriate, removing dormant or unnecessary access to minimise risk

## 3.5 Auditing, monitoring and performance

Providing transparency, accountability and regulatory assurance, we maintain comprehensive audit and monitoring capabilities across all environments where client data is processed or accessed. These controls ensure our/user activity is traceable, reviewable and available to support governance, compliance and investigation requirements.

### Audit logs

Enabling all significant activity to be traced, reviewed and evidenced, we maintain clear audit logs in a searchable index. For a tailored approach, we confirm the audit logs to be maintained and processes to be followed with the client during mobilisation, adjusting our approach as necessary. Typically, our audit logs capture:

- **User access and authentication activity:** Enabling visibility of who accessed systems and when, we log authentication events and access attempts to support security monitoring
- **System and configuration changes:** Reducing risk and supporting accountability, we log changes to system configurations, deployments and environments, ensuring that operational actions are traceable to authorised individuals or processes
- **Data processing and handling activity:** Supporting GDPR compliance and data governance, we log data processing activities and access to client data, allowing data owners to audit usage and respond to data subject requests where required
- **Supplier and administrative activity:** Providing full transparency, all supplier access to client environments is logged and can be audited, reviewed and extracted on request

### Protection, retention and access

Protecting the integrity and confidentiality of audit data, logs are centrally managed and protected from tampering under our ISMS. Ensuring consistent control over where sensitive information is stored and processed, logs are retained in-region by default, avoiding cross-region processing unless explicitly approved.

Retention is managed in line with our Data Retention Policy, contractual agreements and GDPR requirements, with retention periods defined and enforced for all data categories. We anonymise customer data following engagement completion.

Fostering transparency, we extract and provide audit logs to clients in a shareable format on request to support compliance reviews, investigations or assurance activities.

### Performance monitoring and metrics

Proactively managing our performance, progress and any issues/risks, we leverage our centralised monitoring capabilities and report results to clients. Providing accountability, Service Operations Managers are responsible for monitoring, measuring and reporting on the service, providing updates at regular check-ins. The frequency and format of check-ins/reviews, as well as communication channels and protocols, are agreed collaboratively with clients during mobilisation. For immediate

visibility of unforeseen changes, they also provide ad hoc updates using the client's preferred channel, enabling real-time awareness and resolution, where necessary.

Maintaining visibility of operations and tracking performance data, we monitor:

- System behaviour
- Access activity
- Operational events across environments
- Incidents and response times
- Milestones achieved
- Anomalies and issues
- Slippage risks

To report on performance and metrics for each engagement, we hold regular review meetings/calls. This typically comprises:

- Weekly ticketing review calls, with an operational focus
- Monthly service review calls, focusing on key issues, action plans and tactical improvements
- Quarterly service reviews, with a tactical/strategic and improvement focus

At these reviews, the Service Operations Manager presents our reports, highlights progress, addresses concerns and identifies scope for improvement. We are receptive to client feedback, using their comments to inform the next delivery period.

## 3.6 Training

Supporting effective adoption and long-term value, we offer training and knowledge transfer as an optional add-on, sitting within our Go Live and offboarding process. We quote training separately during onboarding or following development, allowing clients the flexibility to choose to add or remove this element based on budget and needs.

To ensure client teams understand the solution and can operate it confidently, we offer tailored training and support options. Depending on the client's requirements, training could be a 2-month intensive programme delivered through live sessions with comprehensive materials. Or a simple, basic guidance sheet, if the client decides to take training, maintenance and support in-house, for example.

### Training approach

Delivering relevant, usable and proportionate training, we design training activities around real workflows, user roles and operational responsibilities.

Training is typically delivered through a combination of collaborative sessions and supporting materials, including:

- **Role-based training and walkthroughs:** Helping users understand how the service supports their day-to-day responsibilities, we provide guided walkthroughs of functionality, workflows and operational processes. Sessions can be remote or in-person, and are tailored for different audiences, such as operational users, administrators and technical stakeholders
- **Knowledge transfer during delivery:** Providing a strong foundation for successful adoption, we co-create solutions with the client, minimising and streamlining knowledge-transfer requirements. Our discovery workshops, design reviews, acceptance testing and handover sessions ensure client teams gain understanding incrementally, rather than training beginning during the Live phase
- **Technical and operational enablement:** Supporting client technical teams, we provide structured handover sessions covering system architecture, CI/CD pipeline usage, integrations, data flows, operational scenarios and support/escalation processes
- **Recorded materials and accessible guides:** Enabling access to information as and when required and continuity as teams change, we provide recorded materials for ongoing consultation
- **Internal champions:** By involving key personnel in ongoing user research and testing, supplemented by comprehensive training, we create in-house internal champions who can support adoption, train colleagues and answer queries

Reinforcing learning and supporting self-service, we provide clear, accessible documentation as part of training and handover. Tailored to the solution and audience, materials may include:

- User guides and operational documentation
- Process flows and configuration guidance
- API documentation and integration guides (where applicable)
- Runbooks and support handover materials for live services

All documentation is provided in accessible digital formats and aligned with agreed accessibility standards.

## 3.7 Service pricing, invoicing and termination terms

### Pricing

Providing transparency and flexibility for public sector buyers, our commercial approach includes both Fixed Price and Time and Materials (T&M) models under G-Cloud. Full pricing details are published separately in the **Pricing Document** provided as part of our submission.

As a services-led provider, we rarely offer fixed, off-the-shelf packages. We tailor each engagement to the client's needs, agreeing on the scope, deliverables and commercials based on the required outcomes. Our models are as follows:

- **Time & Materials (T&M):** Suitable where requirements are evolving or where discovery and iteration are required. Providing flexibility to reprioritise as needs change, clients pay only for the time and roles used
- **Fixed Price:** Suitable where scope and deliverables are well-defined, we agree on pricing upfront based on outcomes and deliverables. Providing cost certainty for clearly bounded work, we define clear acceptance criteria, requirements and deliverables which we use for the fixed price quote.

Typical UK day rates vary depending on role and seniority. Supporting value for money, we sometimes offer volume-based discounts for larger teams or longer-running engagements, subject to agreement.

Providing all-inclusive, transparent quotations, we capture all client requirements upfront, which minimises surprises and unplanned costs. If additional requirements arise during delivery, we apply our formal Change Control Process, costing all variations and mutually agreeing the charge where they fall outside of the original scope and quote.

As the level of ongoing support required is best understood once the solution is live, we typically contract this separately following Go-Live. This enables us to provide a package and price aligned to the client's actual needs.

### Invoicing process

For strong financial management and compliance with public sector requirements, we agree on invoicing arrangements upfront. We take a flexible approach to invoicing cycles, operating according to the client's chosen commercial model and preferences. Typically:

- T&M engagements invoiced **monthly** in arrears
- Fixed Price engagements are invoiced **against agreed milestones**

In line with UK government requirements, **standard payment terms are 30 days**. We typically send invoices against a Purchase Order (PO) and expect transfers to the bank account detailed on our invoices.

## Contract duration and termination terms

Reducing commercial risk for buyers, there is no minimum contract term. Our engagements may span weeks or years.

Designing termination agreements to be fair, transparent and proportionate, we maintain procedures for natural and early termination:

- **Natural termination:** Where contracts end at the end of their natural term, we carry out our formal off-boarding process, revoking access to systems and sending all final deliverables to the client, or performing any training if the client has opted for this
- **Early termination:** Buyers may terminate an engagement early, and specific terms for each engagement will be agreed and outlined during mobilisation. No additional early termination fees apply. However, we require payment for work completed to date and throughout the notice period agreed
- **Early termination notice:** We request notice proportionate to the team size and project scope, typically between 1 and 3 months for scale down, with larger teams requiring a longer notice period. We will agree on this period during contract negotiation

# 4 Supplier information

## 4.1 About us

Recognised by the **Financial Times (FT1000)** and **Deloitte (Fast50)** as one of the fastest-growing tech companies in Europe, we are a next-generation product innovation agency driving growth, efficiency and resiliency for our partners. Cutting through business, tech and regulatory complexity, we fuse behaviour-based design with unique data competence to propel businesses, offering:

- Software engineering
- Product design
- Data and AI services
- Strategy services
- Managed support services

Turning some of the most challenging digital initiatives into success stories, we believe in the power of technology to enable human achievement, drive progress and be a force for positive change. Every solution we deliver is shaped by clients who choose to innovate and redefine the future, and we're proud to support them on that journey.

Since our inception in 2011, when Supercharge was founded by 4 Engineers in Budapest, we have expanded to operate **internationally** with **200+ in-house digital experts.** We are part of Siili Solutions, a NASDAQ-traded Scandinavian group focused on digital innovation, employing **1,000+ staff**. With offices in **London**, **Amsterdam**, **Helsinki** and **New York**, we are fortunate to partner with the most ambitious companies across **Europe**, the **United States** and **Asia**.

Demonstrated through our achievement of the following accreditations, our work is underpinned by quality, security and sustainability:

- **Cyber Essentials**
- **Cyber Essentials Plus**
- **ISO 9001:** Quality Management Systems
- **ISO 14001:** Environmental Management Systems
- **ISO/IES 20000-1 2018:** IT Service Management
- **ISO 27001:** Security Management Systems
- **SOC 2 Type 1**

## 4.2 Relevant experience and testimonials

## Case study 1: Transport for London (TfL)

### Challenge

TfL engaged us to modernise its Road User Charging system as part of a transition away from legacy infrastructure and towards in-house, cloud-based operations. This involved consolidating and migrating petabytes of historical structured and unstructured data from multiple legacy systems, while maintaining data integrity, compliance and business continuity. The migration needed to be delivered at scale, with minimal operational disruption, and required parallel-run capability to ensure continuity of critical public services during transition.

### Our solution and approach

We designed and delivered a custom cloud-native data migration solution using a structured, risk-managed delivery approach aligned to Agile and user-centred principles. Following a tooling assessment, we selected Databricks as the core migration platform due to its ability to handle large-scale workloads, provide strong data governance controls and support flexible, cloud-based architectures. The solution was delivered on Microsoft Azure, using Azure Data Lake alongside Databricks, Python and SQL.

The Cloud-Native Application Modernisation Services we provided included:

- End-to-end data engineering and migration services
- Detailed requirements analysis and migration planning to identify source systems, compliance needs and performance measures
- Data profiling, validation and cleansing to ensure accuracy and integrity before migration
- Design of complex data mappings, transformation rules and error-handling mechanisms
- Delivery of a metadata-driven, dynamic migration pipeline, providing orchestration, reconciliation, reporting and visibility through dashboards
- Parallel-run 24/7/365 support to minimise downtime and operational risk

### Outcomes

Our solution successfully consolidated and migrated TfL's legacy data into a modern Azure-based environment, providing a scalable and future-ready foundation for the Road User Charging system.

Key outcomes included:

- Mapping and integration of **7 complex source systems** and **26 distinct data bodies**
- Migration of over **5 billion records** and **9.16 billion documents**
- Secure transfer of **1 petabyte** of unstructured data to **Azure**
- Improved operational efficiency through optimised infrastructure sizing and tooling
- A flexible architecture capable of supporting future service changes and expansion

## Case Study 2: BritNed

### Challenge

BritNed operates a 1,000MW High-Voltage Direct Current (HVDC) interconnector between Great Britain and the Netherlands, enabling electricity trading between the 2 national grids. Over 70 market participants rely on their systems to allocate capacity, nominate power flows and manage settlements.

Historically, these workflows were spread across multiple disconnected platforms used for auctions, nominations and operational control. This fragmented landscape reduced productivity, introduced operational risk, limited integration with participant systems and constrained BritNed's ability to innovate and introduce new products.

The client required a single, integrated, high-performance platform capable of supporting critical national infrastructure, strict operational timelines and complex third-party integrations, while remaining easy to use for operators and market participants.

### Approach and solution

Working in close collaboration from Discovery through to Live, we acted as BritNed's end-to-end product design and delivery partner to create **Empire**, a **bespoke nomination and allocation platform**. We used Agile delivery practices, with close coordination between design, engineering and quality assurance teams to ensure stability, performance and compliance from day 1.

Our approach included:

- Discovery and mapping of end-to-end operational workflows for interconnector operators and market participants
- User-centred design of a bespoke unified platform supporting auctions, allocation, nominations and operational oversight
- Design and development of a modern, cloud-ready architecture, supporting complex allocation and nomination logic
- Full frontend and backend development, with integration to 12 third-party systems across the European energy ecosystem
- Design and documentation of modern, well-documented REST APIs to support direct system-to-system integration for large market participants
- Execution of customer acceptance testing and integration testing on behalf of BritNed
- Delivery aligned to a fixed operational window, with careful planning to ensure a safe transition during a scheduled maintenance period
- Provision of 24/7/365 operational monitoring and L1 helpdesk support and L2 Infrastructure on-call support following go-live, with a dedicated team of engineers working on maintenance and product enhancements

Empire provides a single-window operational solution for BritNed's operators and market participants. Our solution supports both long- and short-term capacity trading and real-time nomination management. Reflecting its impact on the interconnector and wider energy sector,

**Empire won the Energy Eagle Award for Innovation of the Year**, praised for 'transforming energy trading'.

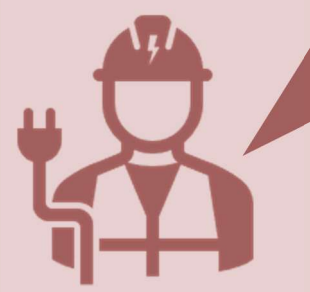
## Outcomes

The new platform provides a single-window solution for BritNed's operators and market participants, enabling the end-to-end management of capacity auctions, allocation and nominations across all timescales. Key outcomes include:

- Enablement of 1,000MW electricity trading capacity through a fully integrated digital platform
- Replacement of fragmented legacy tools with streamlined, automated workflows, significantly improving operator and trader productivity
- Consolidated, real-time dashboards providing 360-degree visibility across auctions, allocated capacity and nominations, supporting faster and more accurate decision-making
- Reduced operational and financial risk through faster response to planned and unplanned outages, helping to minimise curtailment losses and imbalance penalties
- Seamless integration for market participants through modern, well-documented APIs, reducing integration effort and ongoing IT operational costs
- A flexible, scalable technical foundation enabling BritNed to launch new products, including innovative auction models not previously supported by legacy systems
- The platform launched successfully within a tightly constrained maintenance window, with market participants onboarded in advance and first capacity auctions conducted immediately following go-live
- Winning the Energy Eagle Award for Innovation of the Year

*"Working with Supercharge was an exceptional experience. We swiftly established common goals, building a platform which stands out from what's currently in the market, fostering a collaborative environment focused on innovation and quality. Supercharge's rapid knowledge acquisition, clear vision, and user-centric approach ensured the seamless delivery of the Empire platform not only on time but also at a great quality level, which in the end led to a very smooth and uneventful go-live despite the huge complexity of such a transition. We are convinced that the Empire platform will step up our business to a new level and help us to deliver a wider range of products and enhance customer support."*

- Nils Teipel, Commercial Operations and Planning Manager, BritNed



## 4.3 How to Buy

Supercharge's services can be procured directly through the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace.

Buyers can search for Supercharge on the Digital Marketplace and procure the service through direct award, selecting the 'Cloud-Native Application Modernisation Services' listing.

Once selected, the buyer and Supercharge will:

- Raise a Call-Off Contract under the G-Cloud framework terms
- Agree a Statement of Work (SOW) detailing scope, deliverables, timescales and pricing
- Issue a Purchase Order (PO) to confirm commencement

Ensuring transparency and compliance with public-sector procurement regulations, all engagements are delivered in line with G-Cloud framework conditions.

Enquiries or pre-contract discussions can be arranged through our central contact point:

**Contact:** **Laura Rodriguez, Managing Director**

**Email:** **laura.rodriguez@supercharge.io**

**Telephone:** **07425 248371**