SUPER CHARGE

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

Data Platform and Analytics Implementation Services

Service Definition

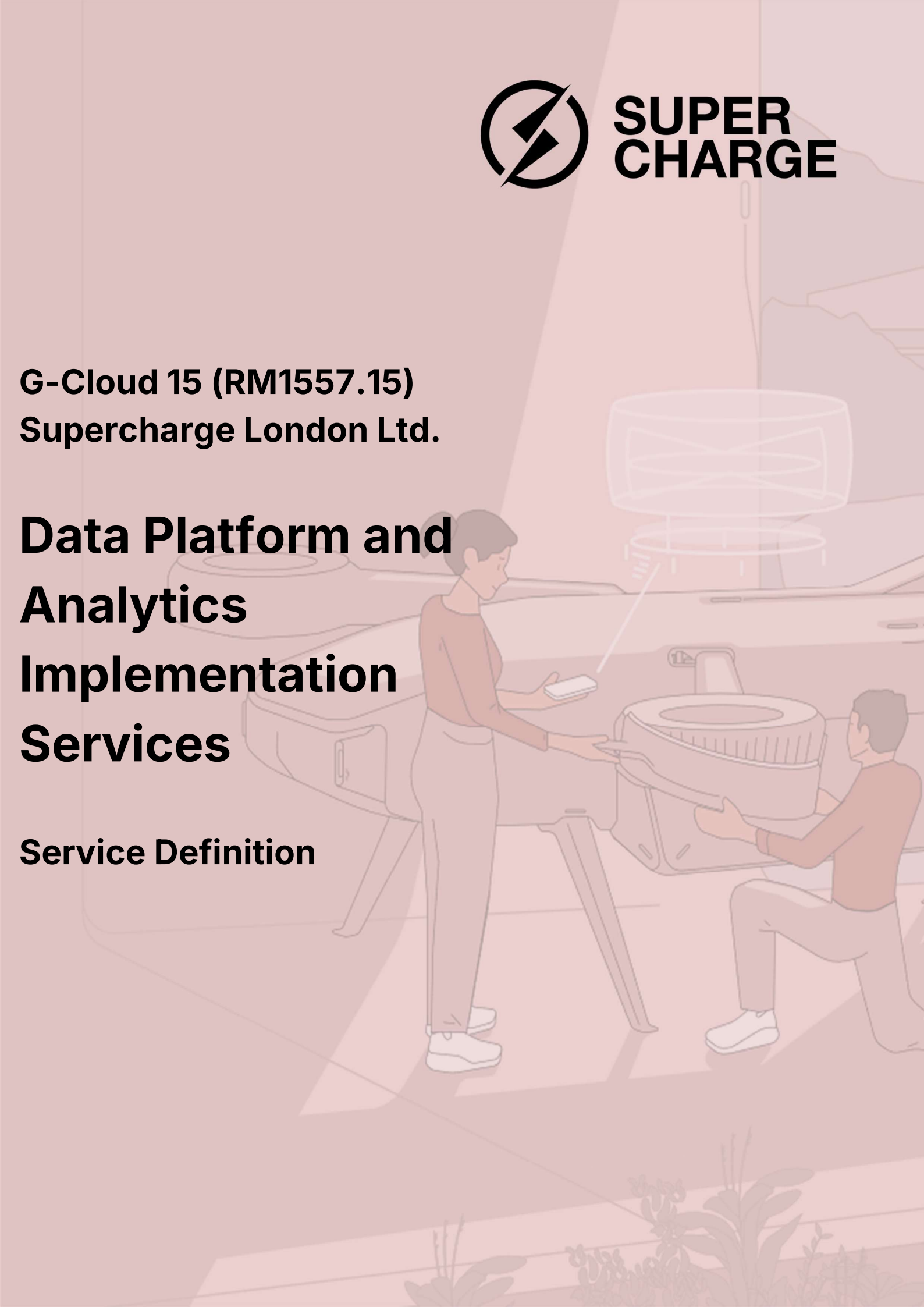


Table of contents

1 Introduction

This Service Definition document provides information about the Data Platform and Analytics Implementation 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 Data Platform and Analytics Implementation services, outlining highlights, key features, benefits for clients, 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

Supporting buyers to quickly locate the information most relevant to their stage in the procurement process, the table of contents on the previous page is clickable.

2 Service description

2.1 About our service

Our Data Platform and Analytics Implementation services help public sector organisations move from fragmented data estates to modern, governed data platforms that support reliable reporting, advanced analytics and AI readiness. We design, build and operate secure, cloud-based data foundations that improve data quality, insight and evidence-based decision-making, while meeting public sector security, compliance and data sovereignty requirements.

The service covers the full lifecycle of tailored data platform delivery, from data maturity assessment and strategy through to implementation, analytics enablement and live operation. This includes unifying data from multiple source systems, implementing scalable cloud data platforms, and embedding governance controls such as data classification, lineage, access management and quality monitoring. We focus on delivering production-ready platforms that support self-service business intelligence and advanced analytics, rather than one-off reports or isolated data solutions.

Specialising in complex, regulated environments where governance, security and auditability are critical, our services are ideally suited to:

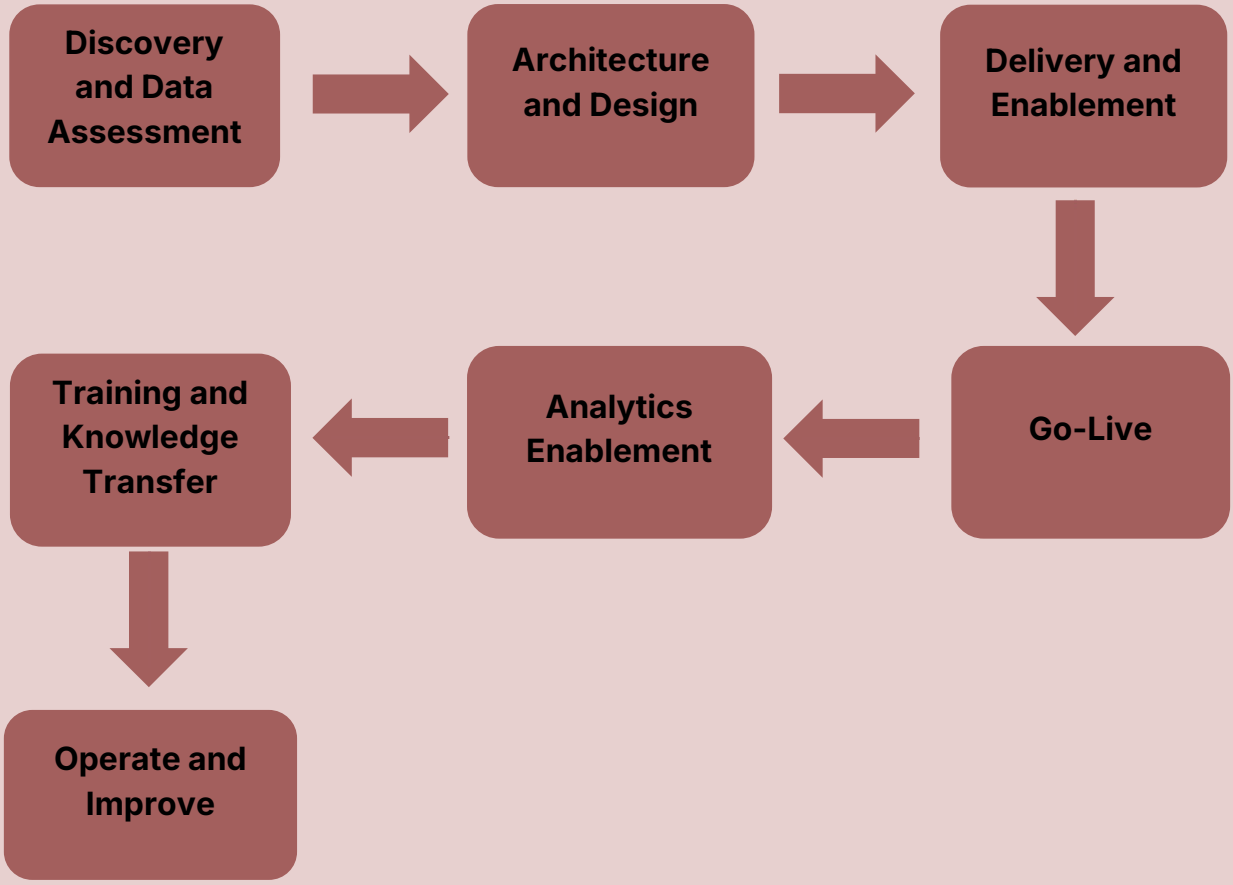
- Central government departments and arms-length bodies
- Local authorities
- NHS trusts and arms-length bodies
- Regulators
- Transport and mobility bodies
- Publicly owned utilities providers

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

Ensuring a user-focused, compliant and quality solution, we deliver our services through a structured framework. Preceded by a comprehensive discovery phase, we move from prioritised use cases to production implementation, introducing solutions in Agile sprints. Our framework is as follows:



1. Discovery and Data Assessment

To establish the current environment, desired outcomes and the steps required to move from one to the other, delivery begins with **Discovery and Data Assessment**. This phase follows onboarding, where scope, constraints and success measures are agreed. Working collaboratively with service owners, Subject Matter Experts (SMEs) and Technical Leads, we:

- Audit existing data sources, connected systems and integrations
- Assess data quality, maturity and readiness for analytics and AI use
- Review the current data architecture and operating model
- Identify governance, security, privacy and data sovereignty requirements
- Define success measures aligned to business and service outcomes

To summarise our findings, we produce a Data Assessment Report. Then, outlining a clear pathway to success, we create a prospective Data Strategy and Delivery Roadmap, closely aligned to business outcomes.

2. Architecture and Design

Transforming our assessment and desired goals into a clear delivery plan, we create and consolidate the target solution, platform architecture and operation model during **Architecture and Design**. Ensuring our solution is technically robust, secure and aligned to operational realities, we:

- Define the target platform architecture, data warehouse, data lake or lake house
- Design logical and physical data models
- Establish integration patterns and ingestion approaches with fully governed observability
- Define security controls, access management and data sovereignty measures
- Confirm governance and compliance approaches
- Establish quality monitoring and lineage procedures

Consulting with our clients throughout the design stage, usability and shared ownership underpin our approach. This phase concludes with the creation of a solidified, actionable Data Strategy and Delivery Roadmap.

3. Delivery and Enablement

Following the client-approved design, we deliver the data platform, dashboards and analytics capabilities through iterative Agile sprints. Focusing on delivering value quickly and establishing feasibility, we prioritise high-impact use cases that can deliver early insight while laying the foundations for a scalable platform. This could include or example, if a client's accounting team spends days manually compiling trial balance reports, fully automating that process would be an ideal starting point, freeing up capacity while proving the platform's value.

Building in quality checks, user validation and security, **Delivery and Enablement** includes:

- Data ingestion pipelines and Extract, Transform, Load (ETL)/Extract, Load, Transform (ELT) workflows for batch, delta and real-time processing
- Data transformations and curated datasets aligned to priority use cases
- Automated data quality checks, monitoring and alerting
- Master data management where required
- Dashboards, reporting automation and self-service analytics capabilities

Ensuring consistent alignment, we continuously validate against agreed acceptance criteria and through demonstrations with clients, Technical Leads and stakeholders during this stage. This approach reduces risk, surfaces issues early and ensures analytics outputs can be trusted in live decision-making.

4. Go Live

Once we have met all delivery milestones, we transition the platform into live operation, finishing sprints and cementing implementations through an agreed release process. We ensure the solution is production-ready, supported and aligned with existing operational processes. **Go-Live** includes:

- Deploying pipelines, data models and analytics and reporting assets into production environments
- Validating security controls, access permissions and data classifications
- Confirming monitoring, alerting and backup processes are active

Following official Go-Live, supporting early operation to stabilise, we provide a 1-month hypercare period, whilst training is in process.

5. Analytics Enablement

With the platform live, we enable analytics and reporting capabilities. **Analytics Enablement** includes:

- Implementing business intelligence tools and dashboards
- Automating reporting to reduce manual effort
- Enabling governed self-service analytics for analysts and operational teams

- Establishing analytics governance to promote consistent definitions and metrics
- Supporting the incorporation of advanced analytics frameworks to enable forecasting and predictive insight

6. Training and Knowledge Transfer

For successful adoption and seamless transition to new systems for clients and end-users, we can provide training as an optional add-on. Depending on client requirements and the complexity of systems implemented, this could be a comprehensive, intense programme of live sessions, recorded materials and tailored guides. For clients with internal training teams, for example, we may provide simple guidance documents and no tailored training. The **Training and Knowledge Transfer** phase is led by the Data Platform Lead and the team which supported implementation. It can include bespoke sessions/materials for all roles who will engage with the solution, including users, administrators, support teams and technical staff.

Handing over and enabling client teams to confidently operate the solution, we also provide training materials and operational documentation as a part of offboarding/handover. This minimises ongoing support requirements and facilitates knowledge transfer for new users. Materials include:

- **Governance artefacts:** Catalogue, lineage, stewardship models
- **Analytics products:** Dashboards, reports
- **Operational documentation:** Runbooks, support handover pack

7. Operate and Improve

Once live, if contracted, we **Operate and Improve** the platform. We collaboratively agree on a level of ongoing operational support aligned with the demands of the solution, including maintenance, L1-L3 support, or optimisation services.

Driving continuous improvement, where optimisation is contracted, we refine our solution based on user feedback and operational data, implementing updates or tweaks. Activities may include:

- Ongoing monitoring of platform health and data quality
- Supporting governance processes such as stewardship, cataloguing, metadata and lineage
- Iterating pipelines, datasets and dashboards based on user feedback
- Optimising performance, reliability, scalability and cost over time

2.3 Service highlights

Designed to maximise productivity in complex, regulated environments: We specialise in delivering data and analytics improvements where governance, security and assurance matter most. Avoiding the common trade-off between control and usability, our platforms embed performance, accessibility and user experience alongside security and compliance

End-to-end delivery from a single accountable partner: We deliver the full data platform lifecycle, from assessment and strategy through to implementation, governance and analytics enablement. This reduces risks and increases our accountability, enabling public sector organisations to modernise confidently.

Multi-cloud and vendor-neutral approach: We design and build data platforms across Amazon Web Services (AWS), Azure and Google Cloud, using portable patterns and infrastructure-as-code to avoid unnecessary lock-in. To support scalable analytics and model training, we implement using Databricks.

Governance and security built in by default: Leveraging our ISO 27001-certified delivery processes and UK GDPR-aligned practices, we embed security into the platform from the outset. Ensuring security is not an afterthought, we consider data classification, access controls, encryption, lineage and audit logging throughout the framework.

Proven delivery in highly regulated environments: Our experience delivering high-assurance platforms in highly regulated environments equips us to handle public sector needs. Designing for scrutiny, auditability and operational resilience, we consider data sovereignty, Freedom of Information (FOI) and complex data-sharing agreements.

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.

Scalable delivery capability: We operate with an in-house team of 200+ experts, backed by a wider resource pool of Siili Group partners and staff for resilience. Our blended team footprint enables rapid scaling whilst maintaining UK-based leadership

2.4 Service features

1. Data strategy, data auditing and maturity assessment

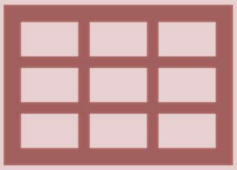
Establishing a clear, evidence-based foundation for transformation, we assess current data landscapes, capabilities and maturity across technology, governance, processes and skills. Through collaboration with Technical Leads and other stakeholders, we audit data utilisation, level of manual efforts, data sources, data quality, existing platforms, security controls and operating models. This process culminates in a proportionate Data Strategy and Delivery Roadmap that aligns with organisational objectives, regulatory requirements and delivery readiness.

2. Cloud data platform architecture design

Providing a secure, scalable foundation for analytics and AI, we design cloud data platform architectures across data warehouse, lake and lakehouse patterns on AWS, Azure and Google Cloud Platform. Aligning with the client's chosen cloud environment and assurance requirements, we clearly define target-state architectures, data flows, security boundaries, integration patterns and operating models.

We design architectures to support analytics, reporting and advanced data workloads while meeting governance, performance, resilience and cost control expectations in regulated environments.

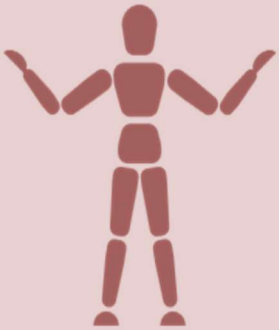
3. Databricks platform implementation



Where appropriate, to support large-scale analytics, advanced processing and AI readiness, we design and implement using Databricks as part of the data platform. This involves configuring secure workspaces, data access patterns, processing workflows and integration with cloud storage and governance controls. Maintaining compliance, oversight and alignment to the wider operating model across Databricks platforms, implementation follows cloud-native and security-by-design principles.

4. Logical and physical data modelling for analytics and AI workloads

Improving data usability, consistency and performance, we design logical and physical data models cascaded down from the business need, optimised for analytics and AI use cases. Working collaboratively with clients and stakeholders, we define shared data definitions, relationships and structures that support reporting, analytics and AI workloads. This ensures our platforms and data are:



- Scalable
- Aligned to business needs
- Well-organised
- Less complex

5. Data ingestion pipelines

Ensuring reliable and timely access to data, we design and implement ingestion pipelines that securely bring data from source systems into the platform. We build data pipelines to handle varying data formats, volumes and frequencies, with appropriate validation and error handling. By aligning ingestion approaches to data sensitivity, quality and operational constraints, we ensure data is available when needed and suitable for analytical use.

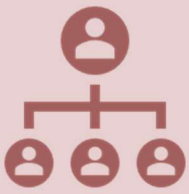
6. ETL/ELT workflows with automated orchestration and alerting

Supporting dependable and maintainable data processing, we implement ETL or ELT workflows to prepare data for analytics and reporting. For operational resilience, workflows are orchestrated using automated scheduling, dependency management and alerting. This feature provides transparency and control to clients, enabling teams to monitor pipelines and data services confidently, even at scale.

7. Data quality framework with monitoring

Improving trust and confidence in data, we establish data quality frameworks for batch, delta and real-time processing. These define rules, thresholds and validation checks aligned to business and regulatory requirements. Supported by automated monitoring, this framework enables identification of completeness, accuracy and timeliness, providing clear visibility of data quality status. By embedding data quality controls into pipelines and platforms, we enable early detection of issues and drive continuous improvement of data reliability over time.

8. Master data management



Where required, we facilitate master data management capabilities. Creating consistent and authoritative data across services, this enables governance of key entities such as people, organisations, locations or assets. Master data management reduces duplication and inconsistency, supporting accurate reporting, data sharing and accurate analytics across complex organisational landscapes.

9. Data governance implementation

Providing assurance, accountability and compliance, we implement data governance frameworks covering:

- Stewardship
- Cataloguing
- Metadata
- Lineage ownership
- Classification
- Access controls
- Lifecycle management

Ensuring compliance, our data governance frameworks are designed to align with organisational policies, UK GDPR obligations and public sector assurance requirements. We support secure data use, enabling analytical access in a controlled and auditable manner by embedding governance as a key aspect of delivery.

10. Business intelligence and advanced analytics enablement

For insight-driven decision-making, our platforms are AI ready, supporting business intelligence and AI / ML capabilities. This includes self-service Business Intelligence, ML forecasting, predictive intelligence and analytical functions. Working with stakeholders, we confirm analytics outputs are usable, relevant and aligned to operational and strategic needs, supporting confident decision-making across the organisation.

2.5 Service benefits

Enabling public sector organisations to reliably use data for reporting, decision-making, and AI integrations, we provide strategic data platform implementation services, transforming fragmented estates into unified platforms. Our service and the resulting platforms deliver unique benefits, such as:

✓ Faster, more reliable insight with reduced delivery risk

By unifying fragmented data sources into a single, governed platform, we enable quicker access to trusted insights for operational and strategic decision-making. Automated ingestion, transformation and validation pipelines reduce dependency on manual data preparation and minimise the risk of inconsistent or outdated reporting.

✓ Improved efficiency and productivity

Automated data pipelines, quality controls and reporting features significantly streamline manual, repetitive and document-heavy workflows. This enables analysts and operational teams to spend less time preparing, reconciling and validating data, and more time on insight, service improvement and frontline delivery.

✓ Increased trust in data and analytical outputs

Embedding governance, data quality frameworks, lineage and monitoring into the platform improves confidence in insights used for statutory reporting, audits and performance management. We reduce errors, rework or challenges during audits, for example, through transparent data provenance and quality measures. This helps users understand where data comes from, how it has been transformed and whether it is fit for purpose.

✓ Better decisions and improved service delivery

Providing timely, reliable and accessible data, we enable evidence-based decision-making for policy development, commissioning and resource allocation. Enabling faster access to information, dashboards and analytics give stakeholders clearer visibility of outcomes, spend and performance for more informed choices.

✓ Secure cross-agency data sharing

Our compliant, governed platforms enable secure data sharing across teams and government organisations, without compromising data sovereignty or posing GDPR non-compliance risks. Supporting collaboration, controlled access integrations and audit trails enable safe interoperability and joined-up insights across agencies.

✓ Scalable, cost-effective foundations with AI readiness

Cloud-native right-sized architectures, automated operations, curated datasets and reusable data support scalable data platforms suitable for analytics and future AI workloads and integrations. Avoiding unnecessary spend as data volumes and usage grow, right-sized architectures, automation and monitoring helps control cloud costs over time.

2.6 Service scope

Service constraints

Providing buyers with transparency upfront, we require certain practical conditions to operate the service. As our service is delivered through close collaboration with client teams and systems, for delivery to proceed effectively, we require access to:

- Business and technical stakeholders for decisions, prioritisation and approvals
- Subject Matter Experts (SMEs), data owners, and data stewards for discovery, requirements clarification and regular validation
- Existing documentation and assets such as current data models, integration specs, security policies, data sharing agreements and operational runbooks
- Relevant environments and tools (for example, cloud accounts, source systems, repositories, CI/CD, monitoring), with appropriate permissions
- Test users for dashboard and reporting validation and accessibility testing where required
- A named product owner or point of contact to manage day-to-day alignment and unblock issues

Where access or availability is delayed, delivery timelines and sequencing may be impacted. We mitigate the risk of this by engaging in collaborative early planning, outlining clear dependency points with clients.

Minimising disruption, we plan maintenance windows to align with customer needs, scheduling work for the lowest-traffic times.

System requirements

Our Data Platform and Analytics Implementation Services do not require specialist hardware or prerequisites, as most compute and storage requirements are provisioned in the cloud.

The platforms we implement support access from all major operating systems through web-based tooling and standard data interfaces. We deliver solutions that work across Windows, macOS, and Linux for engineering and administration, and across major browsers for analytics consumption.

Minimum software requirements for end users of analytics dashboards and self-service reporting are:

- 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

And for the delivery and administration of the platform:

- A modern workstation, such as Windows, macOS, or Linux, capable of running standard developer tooling
- Secure network access to the chosen cloud environment and source system, typically through VPN or private connectivity

Integration options

Creating solutions tailored to the client's security and governance needs, we select services, platforms, hosting region and data-handling controls carefully. Depending on requirements, common integration options may include, but are not limited to:

- **Authentication and identity:**
  - Azure AD, Okta, Cognito, Auth0
  - SAML 2.0 SSO providers
  - OAuth 2.0 / OpenID Connect
- **Data Sources:**
  - Databases: Azure SQL, SQL Server, PostgreSQL, DuckDB
  - Cloud warehouses: Snowflake, BigQuery, Redshift, Azure Synapse
  - Storage: S3, Azure Blob, Google Cloud Storage, network shares
  - Streaming: Kafka, Kinesis, Event Hubs, Pub/Sub
  - Legacy systems via secure API gateways or ETL connectors
- **Enterprise applications:**
  - ERP: SAP, Oracle E-Business Suite, Microsoft Dynamics
  - CRM: Salesforce, Dynamics 365, ServiceNow
  - Case management, HR, finance systems via REST APIs
  - SharePoint and document management systems
- **BI and AI/ML:**
  - Platforms: Power BI, Tableau, Qlik, Looker
  - Data science: Jupyter, RStudio, Azure ML, SageMaker, Vertex AI
- **APIs:**
  - RESTful APIs with OpenAPI documentation
  - Webhooks for event-driven workflows
  - Rate limiting, authentication, monitoring and logging
- **Cloud Services:**
  - Native AWS, Azure, and GCP managed service integration
  - Infrastructure-as-code: Terraform, Bicep
  - Container orchestration: Kubernetes, ECS, GKE
  - Serverless compute integration

Ongoing responsibilities

Following Go-Live, ongoing client responsibilities include:

- Owning priorities and approvals for changes and data onboarding
- Managing users, roles, and access approvals within agreed governance
- Maintaining third-party licences and subscriptions for platform tooling
- Day-to-day operational ownership

Although daily ownership falls to the client, we can provide ongoing monitoring and L1/L2/L3 support, in line with the model outlined in 2.7, if contracted.

2.7 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, 9am – 5pm, Monday-Friday availability) to full 24/7 coverage.

As the level of ongoing support required is best understood once data platforms are live with analytics enabled, 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, all support requests are logged, prioritised and tracked through the ticketing platform. Promoting agency, 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 Priority 1 to Priority 4 (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 possible, the Agent passes the query to the L2 or L3 team. This is consistent across weekdays and weekends.

L2 – Advanced Infrastructure Support:

- **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:

- **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

2.8 Service accessibility and usability

We embed accessibility and usability throughout the design, delivery and operation of our service. Considering accessibility from the outset, we co-create requirements and designs with the client during **Discovery and Data Assessment** and **Architecture and Design**. Demonstrating how user-centred design shapes the service experience, we engage researchers and target users in the early phases.

Extending our collaborative approach throughout **Delivery and Enablement**, we work closely with client SMEs during development. This ensures decisions are made with the people who know the domain best, which will support internal teams to build the understanding needed to operate the service after go-live. Automated and manual accessibility checks form a part of our quality assurance process throughout. Validating usability and compatibility continuously, we implement in Agile Sprints, using test cases and agreed acceptance criteria. Any potential barriers are identified and removed proactively.

Ensuring usability following deployment, an intensive hypercare period follows **Go-Live**. We monitor the solution closely, seek to stabilise performance issues and resolve problems quickly. To improve usability, we confirm whether the service is operating as expected and make refinements if not.

When provided, our **Training and Knowledge Transfer** Phase is user-centred. We coach relevant roles through jargon-free and accessible live/remote training sessions. Additionally, to enable effective day-to-day adoption and seamless use of our services, we produce user-friendly, comprehensive handover packs.

During **Operate and Improve**, we can continue to improve accessibility and usability based on user feedback and operational insight, feeding improvements into the prioritised backlog for ongoing enhancement.

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

2.9 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 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 Works (SoW) confirmation:** Meeting with key representatives from the client's side, we establish scope, deliverables, objectives, constraints and success indicators (KPIs and SLAs). This provides a shared reference point for measuring progress and performance, aligning expectations.
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 SoW 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 an indicative timeline to confirm how quickly we could deliver the project based on the scope. Though our initial timeline is indicative, it can provide an idea of 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. It 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 (if they will be closely involved)

        - Subject Matter Experts (SMEs) for discovery interviews, requirements clarification and regular testing (who can also be assigned without joining the kick off)
            - Optional: End users for user research, usability testing and accessibility testing

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 this specific project. We may require access to:
    - Current architecture
    - Source system APIs
    - Source system UAT data bases
    - Source code, Git repository
    - Data models, transformation logics and data quality documentation
    - Existing reports or dashboards
    - Data sets to be used for training, inference and automation
    - Security policies and key sensitivities
    - 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 and establish key milestones and review points in line with the agreed delivery lifecycle. For example, outlining indicative dates for the completion of each phase.

Project opening: Discovery

5. **Discovery:** Completing onboarding, 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, so we can ensure all is fully detailed, planned and quoted before starting the 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 several months.

Offboarding

After Deployment, we meet with the client to discuss add-ons, such as further support for lifecycle product enhancements or maintenance services. If we are to continue partnering, we discuss and draw up a new support agreement, which may include:

- Production environments support to ensure good performance (with our L1, L2 and L3 services)
- Product maintenance and enhancements, with a dedicated or ad-hoc team depending on 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 and SLAs).
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 can 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

    The exact documentation and training materials to be provided are agreed with clients during offboarding.
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
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. However, rather than being 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 through encrypted transfer.

Following 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.

To maintain data sovereignty, meet regulatory requirements and reduce exposure risk, we configure AI training and inference to run in the agreed geographic region where supported. We avoid cross-region processing unless explicitly approved. Ensuring consistent control over where sensitive information is stored and processed, operational logs, monitoring data and backups are also retained in-region by default. Where third-party model APIs are required, we only use approved providers and configure them to comply with the client's data-handling, retention and security policies.

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 by a separate email or communication. Minimising risk, we only use mock or anonymised data in non-production environments.

Sub-processors

Owing to the nature of the services, we may use sub-processors for effective delivery. We engage these entities in line with our ISO 27001-accredited Information Security Management System (ISMS) and GDPR obligations, and only where necessary.

Our primary sub-processors typically include:

- **Cloud infrastructure providers:** AWS, Google Cloud Platform and Microsoft Azure. Hosting regions (UK, EU or global) are configurable to meet client data residency, security and compliance requirements
- **Development and collaboration tools:** Used where required for project delivery, such as secure communication, design and code management tools (for example, Slack, Figma, or code repositories and CI/CD platforms). Where possible, we use buyer-provided tools and environments

We apply a strict data minimisation approach, ensuring sub-processors only process the minimum data necessary to perform their function and only for the duration required. Reducing risk, no sub-processor is permitted to use client data for any purpose beyond the contracted service.

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.

Because delivery of the service 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

Upon client request, critical systems can be configured with shorter RPO/RTO targets through more frequent backups and redundant architecture, which would incur additional costs. Ensuring predictable and repeatable recovery, our system restore and reboot procedures, including timescales, are documented, tested and formalised.

.

3.4 Governance

Accreditations and certifications

Demonstrating the robustness of our management system and alignment with industry standards, the following accreditations, certifications and frameworks 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.

3.5 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 from the outset**, with security requirements and sensitivities gauged early and data protection, access control and risk mitigation measures built into solutions.
- **Apply secure coding and review practices**, applying secure coding standards, peer review and automated testing to identify defects, vulnerabilities and unintended behaviours early. **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

3.6 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 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.

3.7 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. It is typically delivered through a combination of collaborative sessions and supporting materials, including:

- **Role-based training and walkthroughs:** Helping users understand how data platforms support 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 users/audiences, such as SMEs 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. Collaborative scoping, continuous testing and handover sessions ensure client teams gain understanding incrementally, rather than training beginning during later phases
- **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 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
- Governance artefacts, such as catalogue, lineage and stewardship models

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

3.8 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 a 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 Deployment. This enables us to provide a package and price aligned to the client's actual needs, whether they choose to receive ongoing support, maintenance or optimisations.

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
- **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. This period will be agreed at the kick off

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 National Association of Securities Dealers Automated Quotations (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**.

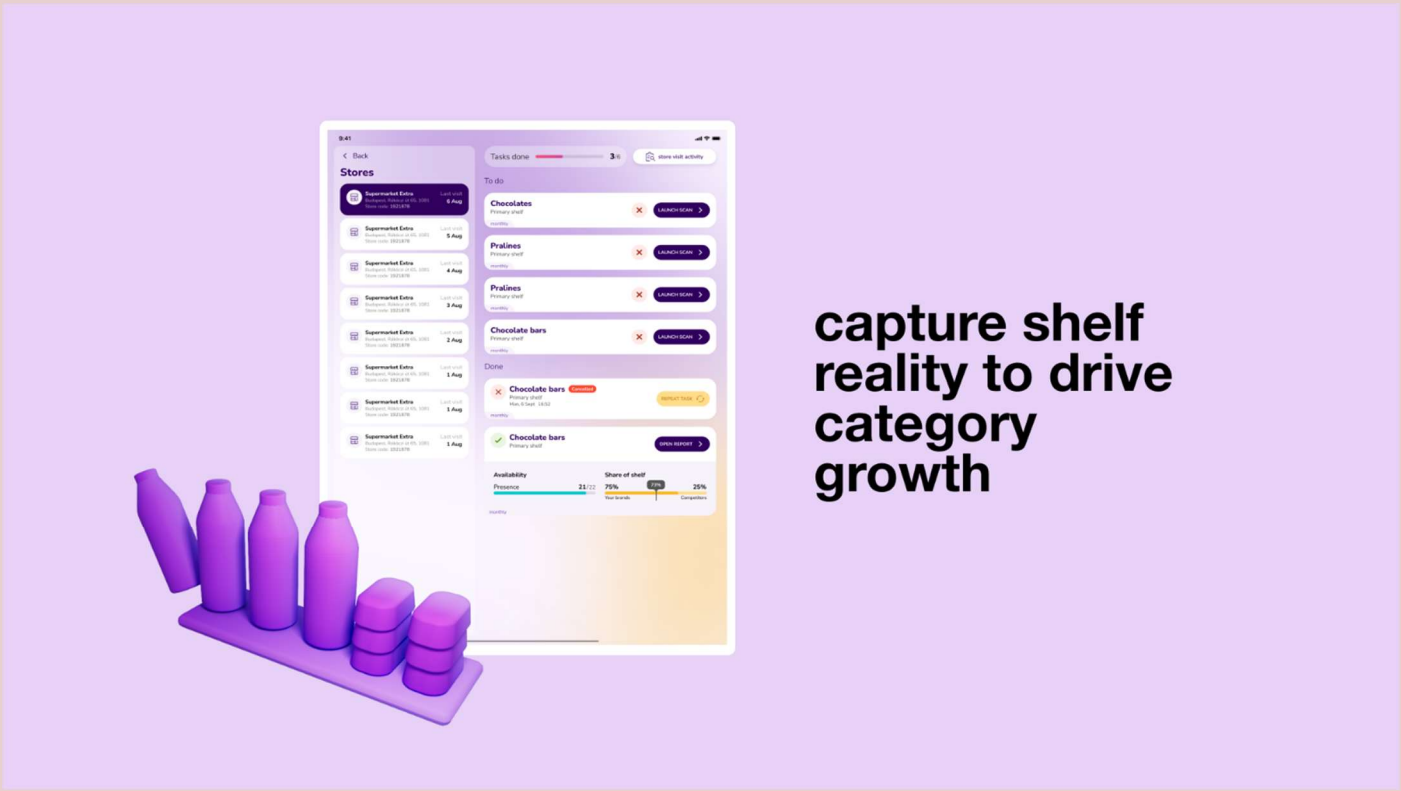
Demonstrated through our achievement of the following accreditations, our work is underpinned by quality, security and sustainability:

- **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 I**

4.2 Case studies and testimonials

Demonstrating how our Data Platform and Analytics Implementation services have supported organisations to move from fragmented data estates to modern, governed platforms, we have provided 2 case studies below.

Case study 1: Trax



Challenge

Trax works with global brands and retailers to provide insight into product placement, availability and shelf performance.

Historically, shelf auditing relied on a manual, fragmented process: sales representatives captured photographs of shelves, uploaded them for offline image recognition processing and later compiled reports manually. Limiting Trax's ability to provide real-time, store-level analytics to clients, this approach was time-consuming, susceptible to human error, required reliable connectivity and delayed insight delivery.

Trax required a scalable solution capable of capturing shelf data in real time, transforming it into trusted analytics and facilitating the presentation of immediate actionable insights. This needed to operate reliably in-store, reduce manual reporting effort and provide a strong data foundation for analytics at scale.

Our solution and approach

We partnered with Trax to design and deliver a real-time shelf analytics platform underpinned by robust data engineering and analytics capabilities, alongside an Augmented Reality (AR)-enabled mobile experience.

Working collaboratively from discovery through to live operation, we combined product design, software engineering and data platform implementation to transform how shelf data was captured, processed and analysed. Trax's existing AR Software Development Kit (SDK) provided the core image recognition capability, while we designed and delivered the surrounding data pipelines, analytics layer and user-facing products.

Our approach included:

- Design and delivery of a real-time AR shelf-scanning application for iOS and iPadOS, enabling in-store data capture without reliance on photo uploads
- Implementation of data ingestion pipelines to capture shelf recognition events and product metadata at scale
- Transformation and enrichment of raw shelf data into structured, analytics-ready datasets
- Design of logical data models to support store-level, product-level and trend-based analysis
- Delivery of a self-service analytics dashboard providing immediate insight into product availability, shelf share and compliance
- Automated report generation, converting captured shelf data directly into shareable, actionable reports
- Ongoing L3 support and maintenance to ensure platform stability, performance and scalability

Outcomes

Strengthening transparency, improving operational efficiency and laying strong foundations for future advanced analytics, our platform enabled Trax and its clients to move from delayed, manual reporting to real-time, data-driven decision-making.

Key outcomes included:

- Real-time shelf analytics delivered directly to sales representatives during store visits
- Significant reduction in time spent auditing stores and producing reports
- Increased accuracy and consistency of shelf data through automated capture and processing
- Improved productivity for sales teams, enabling more stores to be audited per visit cycle
- Trusted, analytics-ready datasets supporting trend analysis, product performance insight and client reporting
- Positive end-user feedback, with users highlighting speed, usability and reduced manual effort

Case study 2: gateretail

Challenge

Serving over 20 airlines and more than 300 million passengers each year, gateretail is the world's leading in-flight retailer. Operating across 4 continents and supporting a fleet of over 1,000 aircraft, accurate demand forecasting is essential for optimising stock levels, minimising waste and maintaining high service standards.

While gateretail held several years of historical sales data, forecasting was primarily driven by traditional, rule-based approaches. These methods struggled to account for the complex and highly variable nature of in-flight retail demand, often influenced by intersecting factors such as route profiles, seasonality and passenger demographics.

To improve forecasting accuracy and operational efficiency, gateretail required a machine learning (ML)-based approach. It had to be capable of leveraging historical data at scale, integrating into existing supply chain workflows and supporting automated, repeatable forecasting processes. However, they lacked the data platform foundations required to implement and operationalise such a solution.

Our solution and approach

Leveraging our data assessment, strategy and architecture development expertise, we partnered with gateretail for a critical step in their wider, data-driven transformation.

Applying our framework, we worked closely with gateretail to understand their operational context at the intersection of aviation and retail. Using years of historical sales data, we conducted thorough exploratory data analysis to establish a baseline understanding of customer behaviour, uncover patterns and test forecasting hypotheses.

Our approach included:

- Design of a cloud-based data and analytics architecture suitable for ML workloads
- Exploratory data analysis to assess data quality, seasonality, route-level behaviour and purchasing patterns
- Development of a machine learning forecasting Proof of Concept (PoC), trained on historical sales data
- Evaluation and comparison of multiple forecasting model approaches
- Implementation using Databricks to support large-scale data processing and model training
- Design of an automated forecasting workflow aligned to the day-to-day needs of the supply chain team

The solution was designed not only to improve forecast accuracy, but to be easily automated and integrated into operational planning processes, supporting repeatable and scalable use and future innovations.

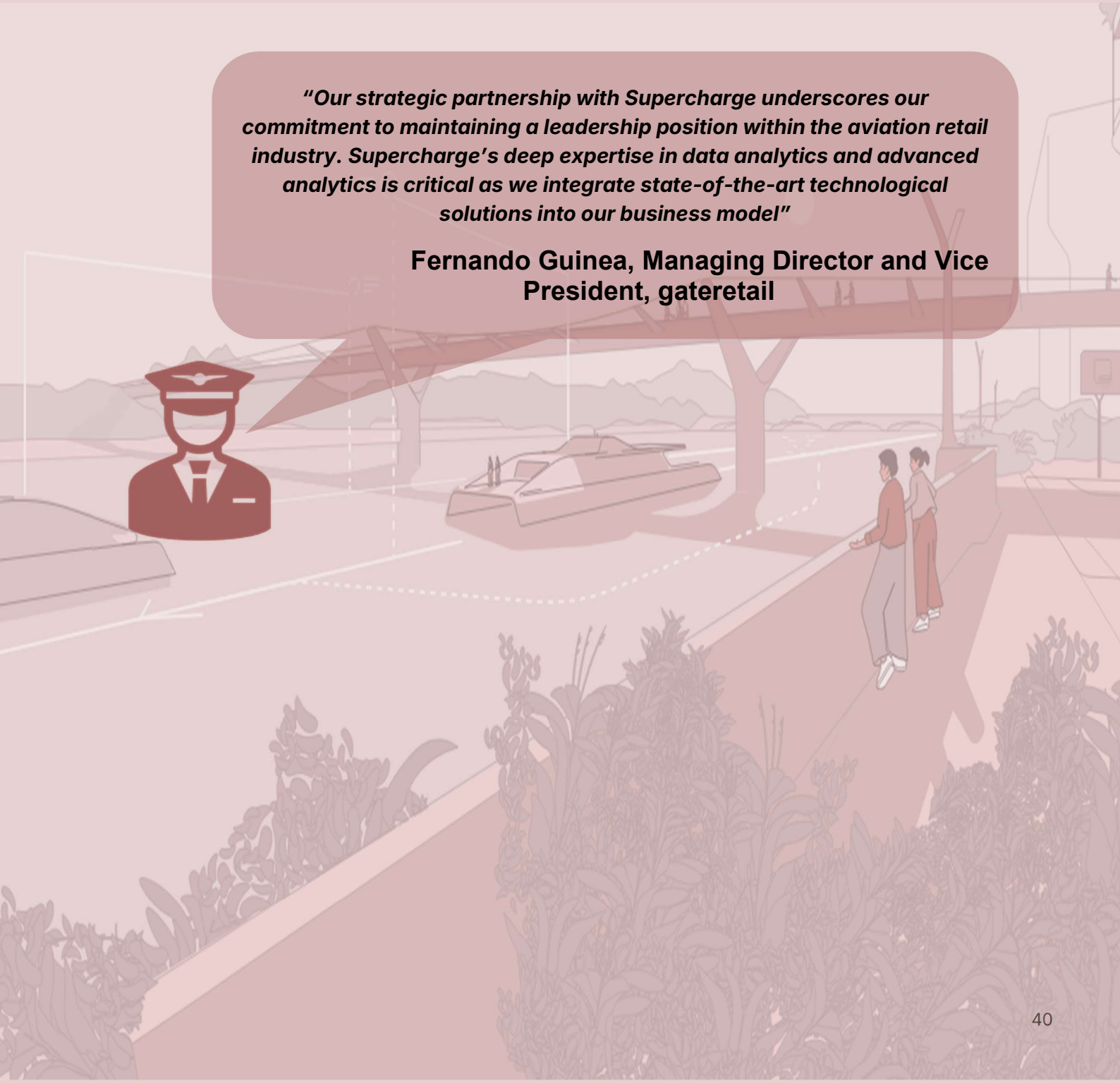
Outcomes

The transition from traditional forecasting methods to a machine learning-driven approach delivered measurable business impact.

Key outcomes included:

- Double-digit improvement in forecasting accuracy compared to existing rule-based methods
- A 10x return on investment from improved stock optimisation and reduced inefficiencies
- More reliable demand forecasts, supporting better inventory planning and reduced operational risk
- Improved decision-making for supply chain teams through data-driven insights
- A scalable technical foundation for future expansion beyond the initial PoC

Beyond immediate gains, the solution established strong foundations for gateretail's long-term data strategy. With a proven ML forecasting capability and a modern analytics platform in place, gateretail is now positioned to scale the solution across additional routes, products and use cases, replacing legacy forecasting approaches and supporting sustained innovation in a highly dynamic operational environment.



"Our strategic partnership with Supercharge underscores our commitment to maintaining a leadership position within the aviation retail industry. Supercharge's deep expertise in data analytics and advanced analytics is critical as we integrate state-of-the-art technological solutions into our business model"

Fernando Guinea, Managing Director and Vice President, gateretail

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 through direct award, selecting the 'Data Platform and Analytics Implementation 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**