HITACHI

Hitachi Solutions Europe

G-Cloud 15 Service Definition Document

Secure Multi-Cloud Connector

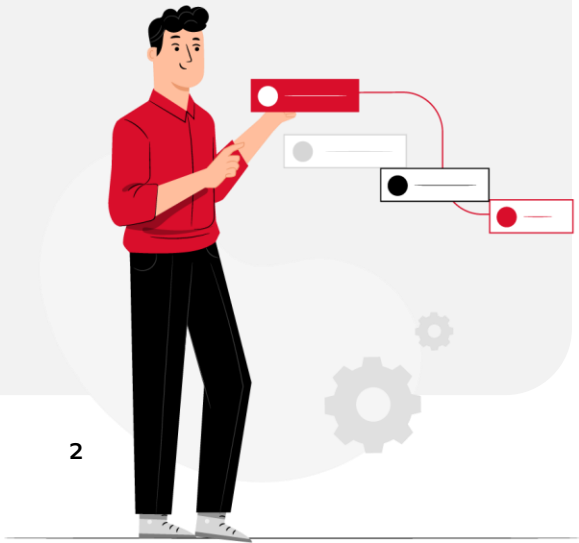
Secure Multi-Cloud Connector

HITACHI

What the service is, what you get, and the benefits

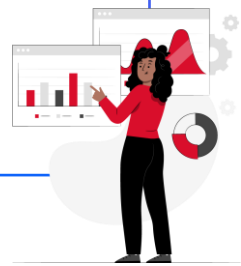
Service Description

Design and implement secure connectivity between cloud platforms and on-premise networks. We build controlled data exchange using network segmentation, encryption, identity and access controls, and monitoring. Supports Azure, Amazon Web Services and Google Cloud integrations, enabling interoperable services, migrations and shared data while meeting public sector security assurance needs.



Service Features

- Multi-cloud network design for secure interconnectivity.
- Private connectivity using peering, ExpressRoute and Direct Connect.
- Virtual private network (VPN) setup and certificate management.
- Zero trust segmentation, firewall rules and route control.
- Identity federation and role-based access control (RBAC).
- Encryption in transit using Transport Layer Security (TLS).
- Secure application programming interface gateways and service endpoints.
- Logging, monitoring and security event alerting across clouds.
- Data transfer patterns for batch, event and real-time.
- Assurance evidence pack for reviews and operational handover.



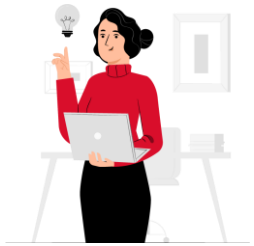
Service Benefits

- Enable secure data sharing across cloud providers.
- Reduce integration risk with standard patterns and controls.
- Improve resilience through segmented connectivity and monitored links.
- Support migrations with controlled, auditable connectivity between environments.
- Reduce attack surface using zero trust network segmentation.
- Meet assurance expectations with clear evidence and governance.
- Speed up delivery by reusing repeatable connectivity templates.
- Improve performance using private connections and optimised routing.
- Simplify operations with consistent monitoring and incident processes.
- Protect sensitive data with encryption and least privilege access.

Secure Multi-Cloud Connector

HITACHI

Secure, controlled connectivity between clouds and on-premise



What this service is for

Make cross-cloud data exchange possible without weakening security

Teams often need Azure services to use data held on AWS, GCP, or on-premise networks, but connectivity becomes the blocker: unclear network routes, inconsistent controls, and limited audit evidence for assurance. This service designs and implements secure connectivity so systems can interoperate without creating new risk.

We set up controlled pathways using segmentation, encryption, identity and access controls, and monitoring. Where required, we use private connectivity to avoid sending sensitive traffic over the public internet and to support performance and reliability expectations.

Key outcomes: Secure cross-cloud pathways | Auditable connectivity controls | Interoperable services | Migration-ready links | Assurance-ready evidence

Why this service is useful

Reduce delivery friction when services and data span multiple clouds

Without a repeatable connectivity pattern, teams lose time to one-off workarounds, slow security sign-off, and brittle integrations that are hard to monitor and support. Secure Multi-Cloud Connector reduces that waste by putting standard controls around how data moves and who can access it.

It supports secure data sharing across cloud providers and on-premise networks, improves resilience through segmented connectivity and monitored links, and simplifies operations with consistent monitoring and incident processes. It also helps teams use the best tools for the job while keeping data where it lives, rather than copying it everywhere.

Common triggers: Multi-cloud estate | Migration between environments | Cross-cloud data sharing | Assurance gate delays | Inconsistent VPNs and routes | Limited monitoring and audit trails

Why this service is different

Secure-by-design connectivity with evidence built in

We do not treat connectivity as “just networking”. We treat it as an assurance-critical product that needs clear decisions, repeatable controls, and operational ownership from day one. That means we design segmentation, access control, encryption-in-transit, and monitoring as a single joined-up solution, not bolt-ons.

We also package the work for review and handover: clear patterns, test evidence, and an assurance evidence pack that supports governance reviews and operational readiness, so delivery does not stall at the final hurdle.

Differentiators: Zero trust segmentation by default | Private connectivity patterns | Cross-cloud monitoring and alerting | Assurance evidence pack | Operate-ready handover

The Business Problem

HITACHI

Increasingly, businesses are making use of data and application from other clouds. Microsoft's Power Platform is a great fit for these scenarios – but working in secure and highly regulated estates can be problematic.

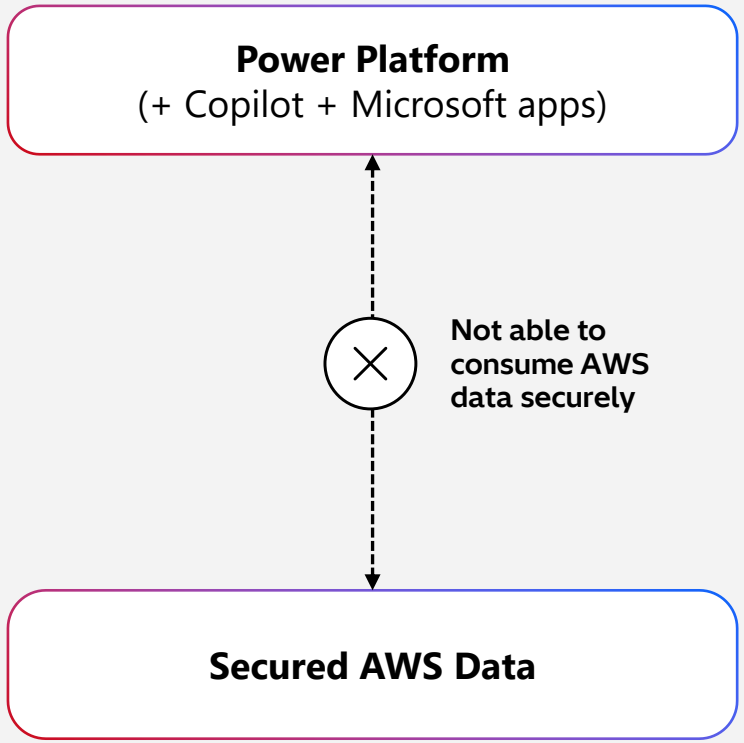
Our customers are asking for:

Low-Code Enablement

Allowing secure data usage via Power Platform tools like custom connectors and Copilot.

Data Accessibility

Enabling Microsoft first-party apps (e.g., Customer Insights) to use secure AWS data seamlessly.



Example Solution Scenario

HITACHI

Using the right app from the right cloud, securely.

Casework Officer

Manages applicant case records and workflows across departments.

Records Specialist

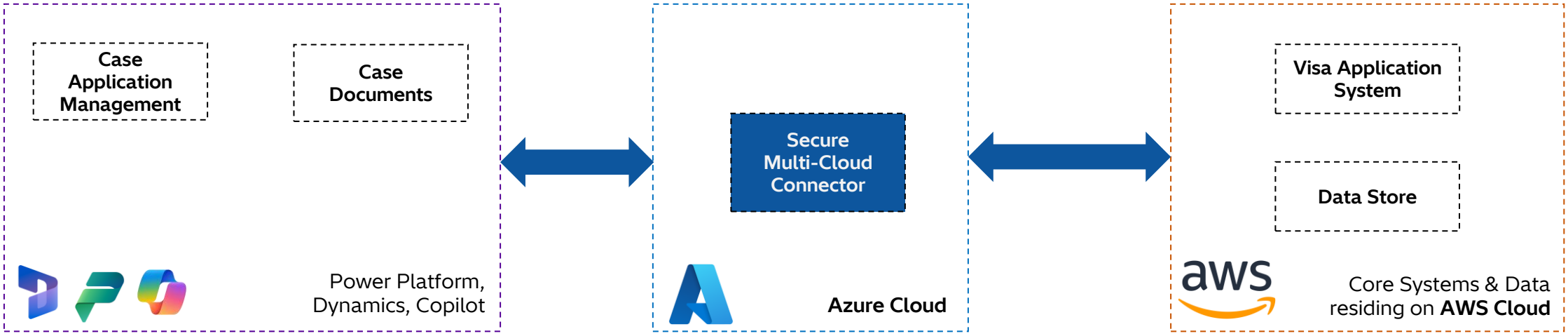
Ensures correct storage, tagging, and access to documentation.

IT / Security & Operations

Maintains secure data flows and access policies between systems.

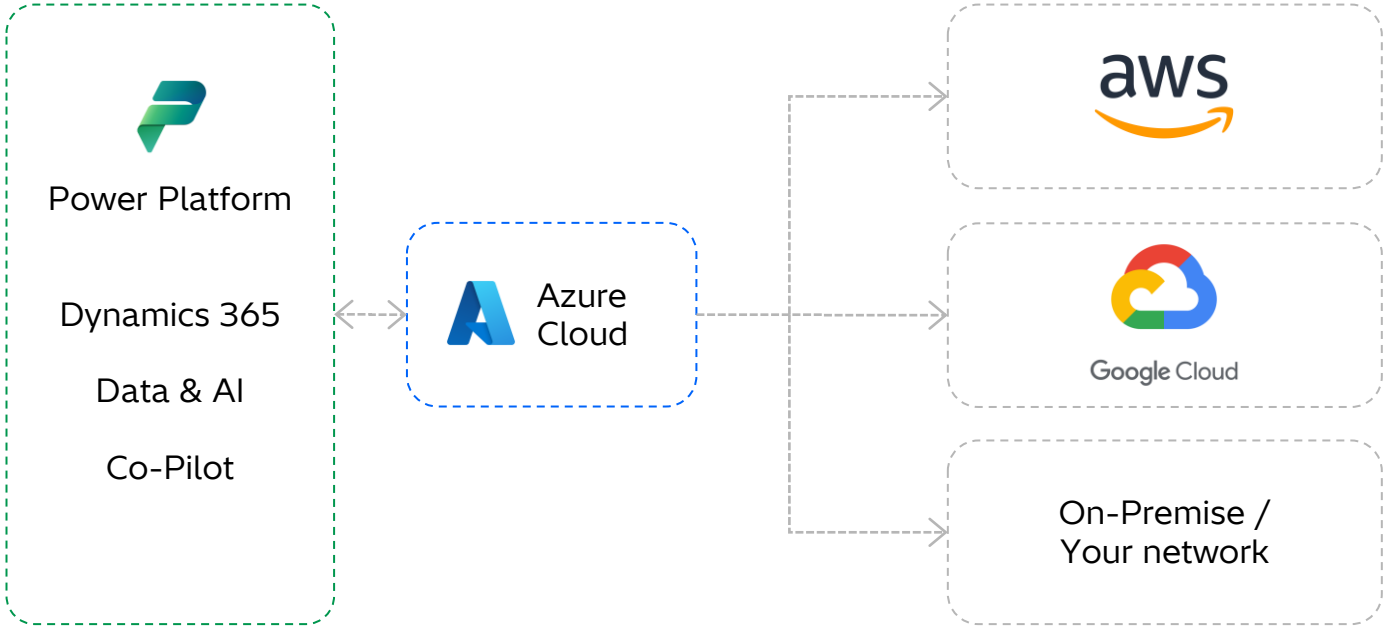
Visa Assessment Officer

Reviews applications and updates visa records in the core system.



The Solution

HITACHI



Using the right app from the right cloud, securely!

Enabling Multi-Cloud

- Cross cloud interoperability
- Smart Workload Placement
- Reduce vendor lock-in
- Remove barriers to choosing Microsoft

How we will deliver

HITACHI

Discovery-led, iterative, and assurance-ready from day one

We deliver in clear phases with regular checkpoints so you can review working outputs, not just documents. Early decisions cover standards, security controls, onboarding and change, so teams don't rebuild the same integration patterns repeatedly. Throughout, we keep an auditable trail through design decisions, acceptance criteria, test evidence and operational handover assets.

We start by agreeing priority integrations and how data should be shared safely. We then design the API standards and gateway controls, build iteratively with monitoring and documentation in place, and prove reliability through contract, performance and resilience testing. Finally, we transition to BAU with runbooks, ownership and a managed lifecycle approach.

Mobilise

Create the conditions for safe delivery.

Confirm the clouds in scope (Azure, AWS, GCP and or on-prem), priority data flows and users, plus success criteria for secure connectivity. Agree stakeholders, access, decision forums and assurance expectations. Capture constraints like "no public internet", "no long-lived secrets" and "no data replication"

Outputs

- Delivery plan + security success criteria
- Access, environment and dependency readiness plan

Design

Define the target connector design and controls.

Choose private connectivity patterns and routing, apply zero-trust segmentation and egress controls, and define identity and least-privilege access. Agree how data will be accessed "in place" to reduce copying and duplication. Define logging, monitoring and audit events so assurance evidence is a by-product of delivery

Outputs

- Target connectivity design + control set
- Prioritised use case backlog + acceptance criteria

Build

Implement the secure pathways and connector components iteratively, starting with the highest-value use case.

Configure private, encrypted routes and restricted access controls, then enable the required Microsoft services to securely access AWS or GCP data without moving it into a new platform. Instrument the connection with logs, metrics and alerts so failures are visible early.

Outputs

- Working secure multi-cloud connection for priority use case
- Monitoring, logging and alerting baseline

Test

Prove correctness, security and resilience.

Validate encryption in transit, identity and access controls, auditing, blocked egress and expected data behaviours (including no replication where required). Run performance and failover checks so teams can rely on the connection for real services. Capture test evidence and decisions (where required) to support governance and sign-off.

Outputs

- Test pack and results (security/resilience/performance)
- Assurance evidence set (where required)

Transition to BAU

Make it operable and reusable beyond the project.

Define ownership, support model and operational routines (where required). Deliver runbooks, knowledge transfer and an onboarding playbook so teams can add new datasets and consumers safely. Confirm how changes will be governed, and how access, certificates and routes will be managed over time.

Outputs

- Runbooks + handover + knowledge transfer
- Onboarding and change governance playbook

At the end, you have:

- Approved private, encrypted routes avoiding the public internet
- Strong identity checks + full auditing
- Zero-trust segmentation and egress control
- Data accessed where it lives, reducing copying
- Reusable connector pattern for new use cases
- Monitoring, logging and alerting baseline
- Assurance-ready evidence pack

HITACHI

Hitachi Solutions Europe

UK Government Overview

Hitachi Solutions for the UK Government

HITACHI

Our **vision** is to be government's partner of choice for the design and delivery of **sustainable, human-centred, Microsoft Solutions and digital services**.

Human-centred Services

Every service starts with people and how technology can make their day simpler.

+

Deep Microsoft Expertise

Hitachi Solutions is dedicated exclusively to the Microsoft ecosystem.

+

Emotionally Aware Delivery

Our former civil servants bring deep understanding and cultural alignment.

+

One Hitachi

Hitachi Solutions is part of Hitachi, Ltd., one of the world's largest and most respected organisations.

=

Sustainable government transformation.

Human-centric by default.

Powered by Microsoft.

Our Credentials

HITACHI

Microsoft

Microsoft Solutions Partner

Microsoft global Government and Finance **Partner of the Year 2025**

Microsoft Partner of the Year 2025 Finalists in Build and Modernise AI Apps, Dynamics 365 Supply Chain, Dynamics 365 Sales and Customer Insights, and Low Code Application Development

22 Years in **Microsoft's Inner Circle** (including 2025)

Microsoft Solutions Partner across AI Business Solutions, Cloud and AI Platforms and Security with **18+ specialisations**

Industry

Government Digital Sustainability Alliance

CYBER ESSENTIALS PLUS

Crown Commercial Service Supplier

Keystone member of the **Government Digital Sustainability Alliance**

Crown Commercial Service Supplier

Cyber Essentials Plus Certified

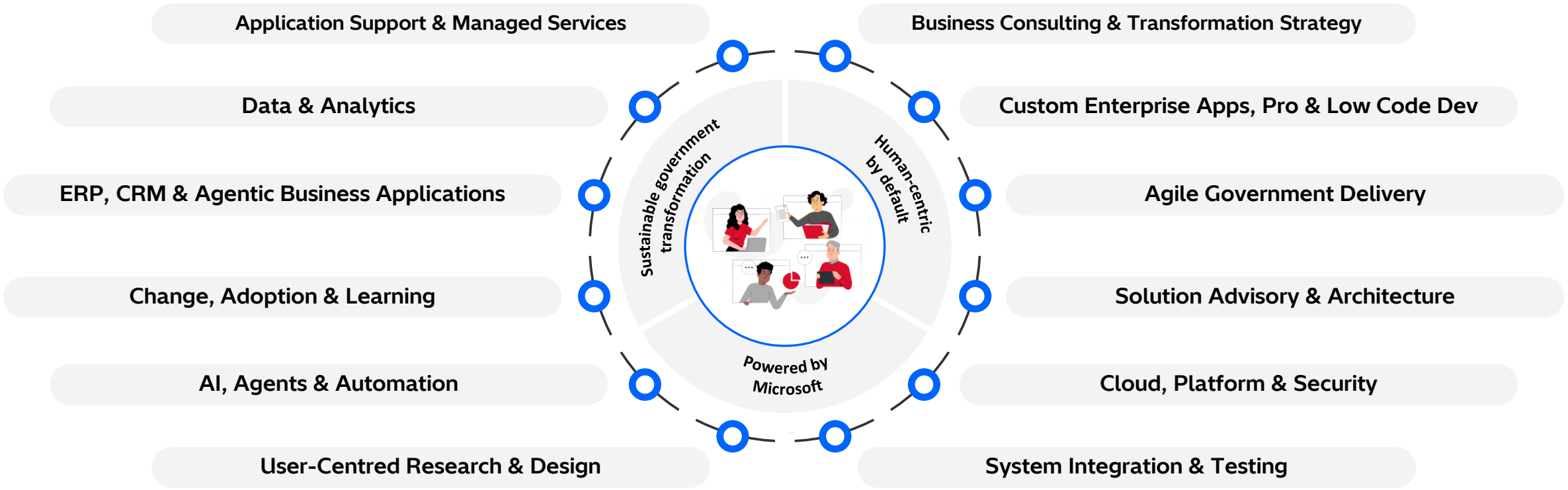
ISO-certified across Quality, Environment, Service, Business Continuity, Information Security, and Privacy Management

Recognised in the **Smarter Working Live Awards** for our regulatory services Customer Experience work with the Environment Agency

Our Services and Expertise

HITACHI

Sustainable business transformation through tailored advisory, consulting, and technology solutions.



Our Clients

HITACHI

"Hitachi Solutions brings substantial digital expertise to the table, complementing our robust business experience. Their insights have been instrumental in identifying opportunities for enhancement and accelerating our initiatives."

Gillian Pratt
Deputy Director Future Regulation at Environment Agency

"Hitachi Solutions brought in a great project team who we kept for the full duration; they engaged with The Royal Mint side of things very effectively. It really felt like they were part of our own team."

Richard Hobbs
CIO The Royal Mint

"Hitachi Solutions bring the innovation, space and expertise needed to deliver digital transformation at a pace that is needed."

Andy MacDonald
Director of Customer Services, Aberdeen City Council

"Hitachi Solutions were really good to work with, expertly turning our processes into slick system functionality. Their patience, understanding and "one team" approach to this project facilitated a free-flowing, inclusive environment. Hitachi Solutions' expert technical teams have delivered a great user experience, employing creative thinking to deliver to our often complex requirements."

Daniel Saward
OIA Head of Digital Technology

"DHSC collaborates closely with Hitachi Solutions LTS, emphasising the significance of our enduring partnership characterised by collaborative teamwork and mutual trust. Operating with a framework of high trust and capability, Hitachi Solutions ensures the delivery of quality and excellence to DHSC. Hitachi Solutions should be very proud of their track record in DHSC."

Bryan Rayner
Head of IT Business Systems

"Right from the start, we recognised in Hitachi Solutions a potential partner that would listen to us and really recognise the value of what we were trying to achieve, the lifesaving benefits of what we were trying to build and support."

Alex Duncan
Chief Technology Officer

Centre for Environment Fisheries & Aquaculture Science

Department for Environment Food & Rural Affairs

Valuation Office Agency

HM Revenue & Customs

Rural Payments Agency

City of Westminster

Homes England

The Royal Borough of Kensington and Chelsea

UK Export Finance

Forestry and Land Scotland
Coilltearachd agus Fearann Alba

HITACHI

Contact Us

UK

110 Bishopsgate,
23rd floor

EC2N 4AY London

enquiries@hitachisolutions.com

+44 (0)204 526 8510

hitachi-solutions.co.uk

hitachi-solutions-europe