848

848 Intelligent Core – Cloud & Infrastructure Enablement

Part of

The Intelligent Core

Prepared by

Dave Cheetham

Pursuit Intelligence and Growth Lead

Wednesday, 07 January 2026

Service Overview and Context

What Our Customers Experience

Organisations operate technology estates that have grown complex through years of expansion, mixed platforms, and increasing cloud adoption.

Legacy infrastructure coexists with modern services, environments behave inconsistently, and technical decisions made in isolation create fragmentation across the estate. As a result, teams struggle to maintain predictable platform performance, scale environments safely, or introduce new capability without disruption.

Cloud services are adopted at speed, but without consistent design patterns or foundational structures, environments become difficult to govern and harder to evolve.

These conditions create uncertainty for IT leaders and reduce confidence in the stability of the platform layer. Organisations recognise the need for a structured approach that brings clarity, consistency, and coherence to the foundations on which digital services depend.

Our Framework for Clarity and Improvement

848's Intelligent Business Framework provides the structure organisations use to align cloud and infrastructure foundations with strategic and operational needs. It ensures that architectural direction, platform engineering, and environment governance operate as a single, coherent model.

Through this Framework, foundational services are designed intentionally rather than emerging through isolated decisions or ad-hoc expansion.

The Framework ensures that cloud and infrastructure platforms develop in a controlled manner, with consistent patterns, repeatable engineering practices, and clear expectations for how environments should behave.

It creates the foundation required for predictable operations, technical integrity, and sustainable evolution of the organisation's technology estate.

The Intelligent Core Outcome Area

The Intelligent Core strengthens the technical foundations that modern organisations depend on. It brings coherence to architecture, establishes secure and scalable cloud environments, and applies structured engineering practices that support predictable delivery and controlled evolution.

This outcome area focuses on the underlying platforms, patterns, and design decisions that determine how reliably the organisation can operate and how effectively it can respond to new demands.

By aligning strategy, architecture, cloud foundations, and modern engineering disciplines, the Intelligent Core provides the stable base on which value, security, efficiency, and insight can be built.

Services within the Intelligent Core create the architectural clarity, platform consistency, and engineering discipline required to support resilient operations and sustained transformation.

They ensure the organisation's technology estate is structured, governed, and ready to scale—providing the foundation upon which the remaining Outcome Areas depend.

848 Intelligent Core – Cloud & Infrastructure Enablement

Cloud & Infrastructure Enablement provides the foundational platform structures organisations require to operate cloud and hybrid environments reliably and at scale.

It addresses the challenges created by fragmented infrastructure, inconsistent configuration, and organically developed environments by establishing clear architectural patterns, modern infrastructure capabilities, and governed platform foundations.

This Service Stream ensures that cloud and infrastructure environments are designed and engineered in alignment with organisational intent. It supports the creation of stable, scalable, and predictable platforms that enable secure operations, efficient processes, and reliable digital services across the value chain.

By modernising and structuring the platform layer, the service strengthens the Intelligent Core and prepares the organisation for continued growth and controlled evolution.

Purpose of This Document

This document explains how 848 delivers the Cloud & Infrastructure Enablement Service Stream within the Intelligent Core outcome area.

It outlines the purpose and scope of the service, the methodology used to design and implement foundational environments, and the conditions required for successful delivery.

It also describes how the service aligns with the Intelligent Business Framework and how it contributes to stable and well-governed technical foundations.

The document provides procurement teams, technical leaders, and architectural stakeholders with a clear understanding of the service, enabling informed decision-making and effective planning.

The Intelligent Business Framework

Modern organisations depend on technology that support clear outcomes: reliable operations, effective protection, efficient processes, informed decisions, and the ability to adapt. Achieving these outcomes requires more than individual systems or isolated projects. It demands a structured approach that links technology, governance, and operational practice to the results the organisation is working toward.

The Intelligent Business Framework provides this structure. It is the model 848 uses to organise, deliver, and improve services in a way that aligns directly to business need. Rather than presenting a catalogue of independent services, the Framework shows how each area of capability connects to a defined aspect of organisational performance. This gives customers a consistent way to understand what each service is designed to achieve and how it contributes to wider improvement.

The Framework also brings coherence across the 848 portfolio. It defines the outcome areas that modern organisations typically strengthen and introduces a common language for discussing priorities, risks, and investment decisions. This supports focused planning and ensures work progresses in a coordinated and integrated manner, regardless of where an organisation chooses to begin.

Introduction to 848's Intelligent Business Framework

An Intelligent Business is an organisation that develops and operates its technology, processes, and governance in a way that directly supports its core outcomes. It uses platforms, data, security controls, and ways of working to maintain resilience, reduce risk, improve performance, and adapt to change in a controlled and predictable manner.

In an Intelligent Business, technology is not implemented as a set of isolated systems. It functions as an integrated part of how work is carried out, how decisions are made, and how the organisation meets its obligations. Stability, protection, efficiency, insight, and innovation are treated as connected aspects of the operating model rather than separate technical concerns.

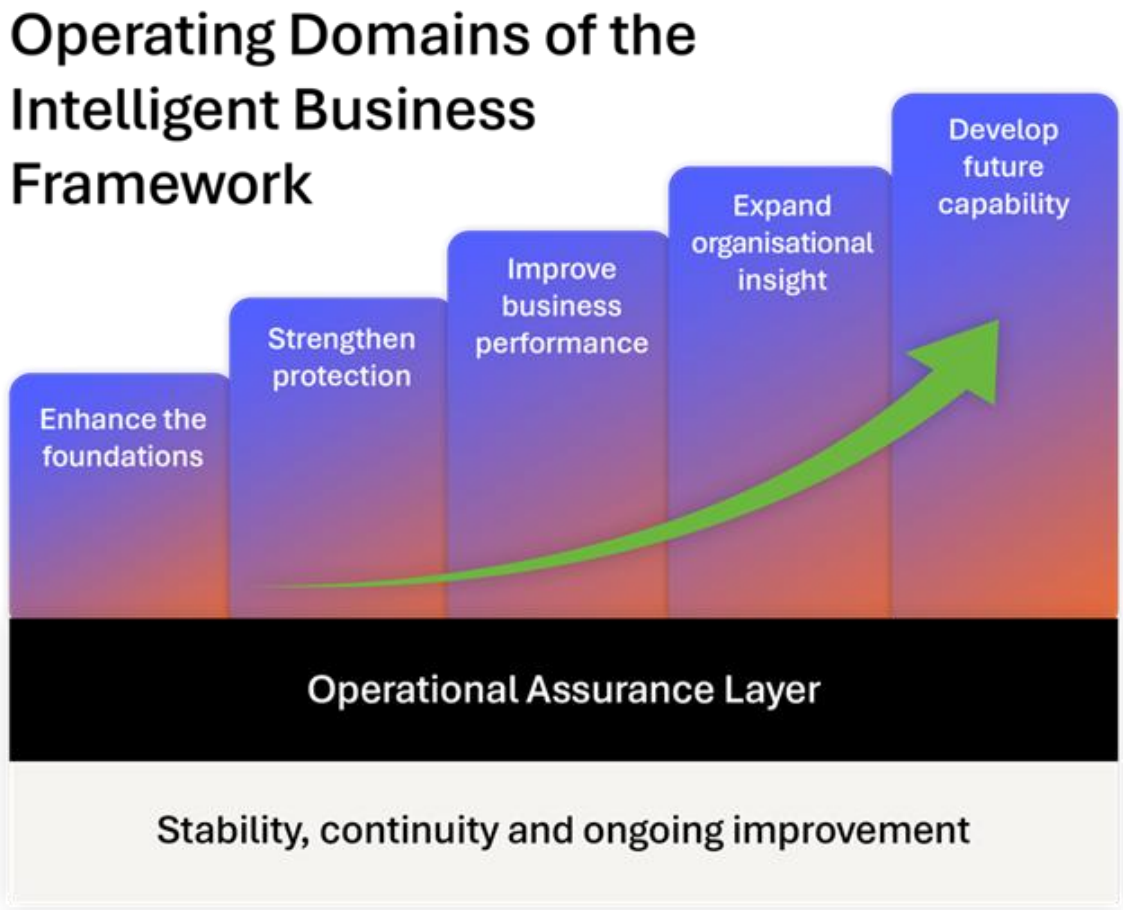
An Intelligent Business has clear visibility of its environment, understands how its services and processes interact, and makes decisions based on evidence, risk, and organisational impact. It can respond effectively to new demands, maintain operational continuity as conditions change, and introduce new capability without undermining what is already in place.

Ultimately, an Intelligent Business uses technology, governance, and operational practice to support reliable, secure, and continually improving performance. It focuses on outcomes, aligns effort to organisational need, and ensures that improvements contribute to long-term capability rather than short-term fixes.

The Intelligent Business Framework is the structure 848 uses to help organisations develop the capabilities required to operate in this way. It translates these characteristics into clear areas of focus, showing how different types of work contribute to stability, protection, efficiency, insight, and future capability. By organising services around these areas, the Framework provides a predictable way to understand what each service achieves and how it supports wider operational goals. This creates a practical link between the outcomes an Intelligent Business depends on and the work required to build and maintain them.

The Operating Domains of The Intelligent Business

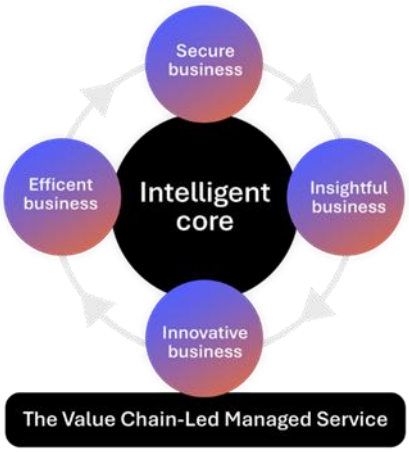
An Intelligent Business strengthens capability across several interconnected domains that influence how effectively the organisation operates. These domains reflect the areas where stability, protection, performance, insight, and future capability are developed over time. Each domain represents a different aspect of organisational need, and improvements in one area support progress in others. Organisations may focus on any domain depending on their priorities, with no fixed starting point or prescribed order.



The Operating Domains describe where organisations strengthen capability, while the Outcome Areas show how the 848 portfolio is structured to support that development. Each Outcome Area represents a defined category of work within the Framework, organising services into clear themes that align to organisational performance. Together, they translate the operating domains into a practical, service-aligned structure that enables consistent planning, delivery, and improvement.

The Six Outcome Areas

The Outcome Areas represent the structured way the Intelligent Business Framework organises capability. Each area describes a distinct aspect of organisational performance and provides the lens through which 848 designs, delivers, and aligns its services. Together, they form a connected model that supports stable, secure, efficient, insightful, and adaptable operations. These areas are not sequential; organisations may focus on any one of them depending on priorities, pressures, or the state of their current environment.



The Intelligent Core

The Intelligent Core provides the technical foundations that support the organisation's ability to operate reliably and scale responsibly. It focuses on the architecture, platforms, and engineering practices that underpin modern digital environments. This includes establishing stable cloud environments, defining coherent enterprise architecture, and applying disciplined platform engineering approaches such as DevOps and SecDevOps.

Strengthening the Intelligent Core ensures that technology aligns to organisational objectives, reduces operational fragility, and creates the structural consistency required for higher-level capability. It enables the organisation to introduce new services, adapt to change, and maintain performance without compromising stability or security.

The Secure Business

The Secure Business focuses on protecting people, data, applications, and operations. It helps organisations understand their risk landscape, implement appropriate safeguards, and maintain resilience as threats and environments evolve. This outcome area ensures that security is embedded into everyday operations rather than treated as a separate or reactive activity.

By strengthening this area, organisations gain clearer visibility of their exposure, greater confidence in their protection measures, and a structured way to govern risk. It supports responsible decision-making and ensures that security contributes directly to safe, predictable, and well-managed operations.

The Efficient Business

The Efficient Business strengthens how work flows across the organisation. It focuses on reducing friction, improving process reliability, and supporting teams to deliver work consistently and effectively. This outcome area addresses the operational constraints that affect performance, from duplicated effort and unclear responsibilities to inconsistent ways of working.

By improving efficiency, organisations reduce operational drag and increase the capacity of teams to deliver value. This supports better utilisation of technology, clearer accountability, and smoother end-to-end processes that contribute to predictable, scalable performance.

The Insightful Business

The Insightful Business enables organisations to make informed, timely, and confident decisions. It focuses on improving visibility of operations, strengthening reporting, and ensuring that data is captured, managed, and interpreted in a way that supports organisational objectives.

Developing this outcome area improves the organisation's ability to understand current performance, identify emerging issues, and assess the impact of change. It provides the foundation for measurement, analysis, and evidence-based planning across all areas of the Intelligent Business.

The Innovative Business

The Innovative Business supports the development of new capability and structured improvement. It enables organisations to explore new approaches, adopt modern tools and methods, and respond effectively to changing needs or opportunities. This outcome area covers areas such as automation, AI adoption, and the creation of new service models or ways of working.

Strengthening this area helps organisations evolve at a controlled pace. It ensures that innovation is introduced safely, aligned to organisational priorities, and built on a stable foundation, without disrupting existing operations or increasing the organisation's level of risk.

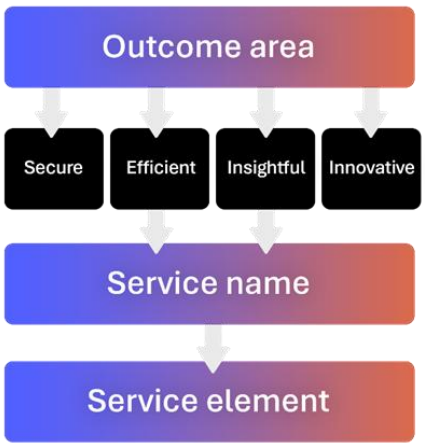
The Value Chain-Led Managed Service

The Value Chain-Led Managed Service provides the operational assurance that underpins every other outcome area. It maintains continuity, stability, and performance by aligning support to the organisation's value chain — the real end-to-end flow of work that keeps the organisation operating.

This outcome area ensures that services are monitored, governed, and improved through a structured, consistent approach. It reduces operational friction, maintains alignment between service delivery and business need, and supports the organisation's ability to sustain improvements made across the other outcome areas.

How Services Align to the Outcome Areas

Each Outcome Area is supported by a set of Service Streams, and each Stream contains the individual Service Elements that make up the work delivered. This structure provides a clear line of sight from each Service Element to the organisational outcome it supports. It ensures that services are delivered consistently, contribute to defined areas of performance, and can be selected according to the organisation's priorities without needing to follow a fixed sequence or maturity path.



The Intelligent Core

The Intelligent Core establishes the technical foundations that modern organisations depend on to operate with confidence. It shapes the structure of the technology estate by defining how platforms are architected, how engineering practices are applied, and how change is introduced in a controlled and predictable way. This outcome area ensures that the organisation's core systems, cloud environments, and integration patterns evolve with purpose rather than drift, enabling technology to support strategic goals, operational resilience, and future capability. It forms the anchor point from which reliable operations, secure practices, and sustainable transformation can be delivered.

What The Intelligent Core Is

The Intelligent Core is the part of The Intelligent Business that provides structural integrity across the organisation's digital estate. It establishes the architectural principles, platform standards, and engineering disciplines that determine how technology is designed, implemented, and governed. This includes the definition of target-state architectures, cloud and network foundations, platform patterns, and the technical conventions that shape how services and systems are built.

The Intelligent Core aligns technology decisions to organisational intent, ensuring platforms are secure, scalable, and coherent. It provides the framework through which new capability is introduced safely, environments are maintained consistently, and dependencies across systems and services are understood and managed. By establishing clear structures and disciplined delivery practices, it creates a dependable environment that supports current operations and enables controlled evolution.

How Work Is Structured Within The Intelligent Core

Work within the Intelligent Core is organised around three areas of technical enablement that together create a stable and scalable technology estate:

Architectural direction and design

Architecture activities define the structural decisions that guide how technology evolves. This includes the development of enterprise and solution architecture, the creation of target-state blueprints, and the governance processes that ensure designs remain aligned to organisational priorities. These activities provide the clarity and standards required for consistent and traceable decision-making.

Platform and foundation engineering

Cloud, network, and infrastructure foundations are engineered using predefined patterns that support operational resilience and secure connectivity. Landing zones, identity structures, network models, and core platform services are designed and deployed using consistent approaches that establish a reliable base for workloads and applications.

Engineering discipline and delivery practices

Modern engineering methods, such as Infrastructure as Code, CI/CD pipelines, configuration baselines, observability, and DevSecOps practices, are applied to ensure environments are

created and changed in repeatable and controlled ways. These practices reduce variability, strengthen compliance, and accelerate delivery while maintaining stability.

These components operate as a single structural framework. Each service contributes to a specific aspect of the Intelligent Core, but all support the same objective: a coherent, governed, and dependable environment that can sustain ongoing change.

What The Intelligent Core Helps Organisations Achieve

The Intelligent Core enables organisations to operate with stronger control, reduced risk, and clearer architectural direction. By establishing a coherent foundation, it reduces the fragility and complexity that arise in unmanaged or organically grown estates. Organisations benefit from technology platforms that scale predictably, support consistent change, and align directly to strategic and operational objectives.

Strengthening this outcome area improves the reliability of core services, accelerates delivery of new capability, and reduces the effort required to manage, maintain, and integrate systems. It creates an environment where technical debt is contained, decision-making is supported by clear architectural insight, and future improvements can be planned and executed with confidence. The result is a technology estate that supports sustained transformation and long-term value creation.

How This Outcome Area Supports The Intelligent Business

The Intelligent Core provides the foundation on which all other Outcome Areas depend. It gives The Intelligent Business a stable, well-governed platform that supports secure operations, efficient processes, insightful decision-making, and controlled innovation. Without the structures and engineering practices established through this outcome area, wider organisational improvements would be constrained by inconsistent platforms, unmanaged dependencies, and unpredictable change.

By aligning architecture to strategy, defining platform standards, and applying disciplined engineering methods, the Intelligent Core ensures that each of the remaining Outcome Areas is supported by reliable and coherent foundations. It enables services to interoperate, data to flow securely, and change to be introduced without undermining operational stability. In doing so, it strengthens the organisation's ability to plan, operate, and evolve in a deliberate and well-managed manner.

848 Intelligent Core – Cloud & Infrastructure Enablement

848 INTELLIGENT CORE PORTFOLIO

CLOUD & INFRASTRUCTURE ENABLEMENT	PLATFORM ENGINEERING	ENTERPRISE ARCHITECTURE
Cloud Strategy and Adoption Roadmap	DevOps Enablement Service	Enterprise Architecture Service
Cloud Architecture & Migration Planning	Infrastructure as Code (IaC) Implementation	Solution Architecture Consultancy
Azure Landing Zone & Cloud Foundation Build	Automation Workflow Design and Deployment	Technology Roadmap Design
Cloud Migration & Modernisation Service	CI/CD Pipeline Design & Automation	Architecture Governance Framework
Cloud-Native Platform & Automation Enablement	Environment Standardisation & Configuration Management	Digital Transformation Architecture
SD-WAN Design & Deployment Service	Monitoring, Observability & Feedback Integration	
Hybrid Connectivity & Network Architecture Design	Automation & Orchestration Framework Design	
Disaster Recovery & Business Continuity Enablement	DevSecOps Enablement	
Cloud Cost & Performance Optimisation Review	Containerisation & Kubernetes Platform Enablement	
Digital Workplace Continuous Improvement Review	GitHub Enterprise & Azure DevOps Integration	
	DevOps-as-a-Service	

Alignment to The Intelligent Business

The Cloud & Infrastructure Enablement Service Stream strengthens the Intelligent Business by establishing the platform foundations required for reliable, scalable, and well-structured digital operations.

It provides the architectural clarity, technical consistency, and environment governance needed to support modern workloads and evolving business requirements. By ensuring that cloud and infrastructure platforms operate predictably, the service contributes directly to the organisation's ability to deliver outcomes with confidence and stability.

Within the Intelligent Business Framework, this Service Stream supports platform integrity by defining how environments are structured, how they evolve, and how technical change is managed.

It establishes patterns that guide platform engineering, ensure consistent deployment of services, and maintain a cohesive architecture across hybrid and cloud estates. These patterns reduce complexity, improve maintainability, and ensure that platforms remain aligned to organisational intent.

The stream also strengthens value flow by providing the technical foundation on which operational, customer, and analytical services depend. When core infrastructure is reliable and well-designed, dependent services experience fewer interruptions, and teams can focus on delivering business value rather than resolving platform issues.

This improves the organisation's ability to introduce new capabilities, scale services, and support transformation at pace.

Cloud & Infrastructure Enablement further supports human-centric operation by ensuring that platforms behave consistently and that engineering teams understand how environments should be configured and maintained.

Clear patterns, structured tooling, and reliable environments reduce ambiguity for technical teams and enable them to deliver change safely and efficiently. This clarity supports the broader goal of the Intelligent Business: creating an organisation in which technical foundations enable, rather than constrain, progress.

Through these contributions, the Service Stream reinforces the Intelligent Business vision by providing the structural and architectural stability required for sustained digital growth and dependable day-to-day operation.

Service Purpose

The Cloud & Infrastructure Enablement Service Stream exists to address the challenges created by inconsistent platform design, fragmented infrastructure, and cloud environments that have evolved without clear architectural direction.

Many organisations operate a mixture of legacy systems, hybrid estates, and rapidly adopted cloud services that lack the foundational structures required for predictable performance and controlled evolution. These conditions reduce confidence in the platform layer and limit the organisation's ability to modernise effectively.

This service strengthens organisational capability by establishing the architectural patterns, engineered environments, and platform structures required for stable and scalable operation.

It ensures that cloud and infrastructure foundations are aligned to organisational intent, built using modern engineering practices, and able to support workloads reliably. Through deliberate design and structured enablement, the service creates clarity over how environments should behave and how they should evolve as needs change.

The purpose of Cloud & Infrastructure Enablement is to provide the technical foundations that allow the organisation to operate with confidence.

It delivers the platform consistency and architectural integrity required for digital services to run effectively, for change to be introduced safely, and for the wider estate to grow in a controlled manner.

By establishing these foundations, the service supports the Intelligent Core outcome area and enables long-term technology evolution.

What This Service Provides

Cloud & Infrastructure Enablement is designed to support IT leaders who are responsible for maintaining reliable platforms, managing operational risk, and preparing the technology estate for continued change.

Role Group	What They Gain	Why They Matter
Executive Teams & Senior Leaders	Clear architectural direction for cloud and infrastructure evolution. Confidence that foundational platforms are reliable, scalable, and aligned to strategy. Reduced complexity and clearer planning for future digital investments.	They set the technology strategy and depend on stable platforms to deliver transformation effectively.
Enterprise Architecture & Technology Strategy Functions	Defined patterns, reference architectures, and alignment across cloud and hybrid environments. Clarity over how foundational services should operate and evolve. Greater consistency across platform, solution, and integration architecture.	hey provide the architectural guardrails that ensure long-term coherence across the technology estate.
Infrastructure, Cloud, and Platform Engineering Teams	Reliable, well-structured environments built on modern engineering principles. Clear expectations for configuration, deployment, and environment behaviour. Simplified platform operations that reduce rework and technical overhead.	They design, build, and maintain the platforms that underpin all digital services.
Solution Architects and Technical Delivery Teams	Consistent platform foundations on which to deploy workloads and services. Clear understanding of platform constraints, capabilities, and integration patterns. Improved predictability when designing and delivering new solutions.	They depend on stable and well-defined foundations to deliver solutions safely and effectively.
IT Operations & Service Management Functions	Greater clarity over platform structure, behaviour, and dependencies.	They maintain day-to-day operational continuity and rely on predictable infrastructure behaviour.

	Environments engineered for reliability and consistency, reducing operational overhead. Improved collaboration with engineering and architecture teams.	

How This Service Is Delivered

The Cloud & Infrastructure Enablement Service Stream is delivered through a structured methodology that establishes the architectural patterns, engineered environments, and platform foundations required for consistent and scalable cloud and hybrid operations. Each stage builds the clarity, structure, and technical integrity needed to support predictable platform behaviours and controlled evolution of the technology estate.

Method Component	Stage 1: Assess Current State & Define Foundational Requirements	Stage 2: Design the Cloud & Infrastructure Foundations	Stage 3: Engineer & Configure Foundational Environments	Stage 4: Enable Platform Adoption & Operational Readiness	Stage 5: Review, Refine & Prepare for Platform Evolution
Stage Description	This stage develops a clear understanding of the existing infrastructure and cloud environments and identifies the architectural, operational, and engineering requirements for foundational platform capability.	This stage defines the architectural structures, patterns, and platform components required for stable and scalable cloud and hybrid environments.	This stage builds the platform components defined in the foundational design, using modern engineering practices to ensure consistency and repeatability.	This stage prepares technical teams, operational groups, and solution stakeholders to adopt and operate the foundational platform effectively.	This stage ensures foundational environments remain aligned to evolving organisational needs and platform engineering best practice.
Purpose of the Stage	To ensure foundational design is based on accurate insight and aligned to organisational needs.	To create architectural clarity and ensure platform foundations support predictable and intentional growth.	To translate foundational designs into reliable and scalable technical environments.	To ensure foundational environments are adopted correctly and support reliable day-to-day operation.	To maintain strong platform foundations and ensure they continue to support organisational growth and modern engineering practices.
Activities Included	Reviewing current infrastructure, cloud services, environment	Designing cloud landing zones, network topology, and identity platform alignment	Deploying cloud landing zones and core platform services	Providing guidance on platform usage, deployment patterns,	Reviewing platform performance, scalability, and alignment with design principles

	structure, and deployment models Assessing technical debt, dependencies, and platform constraints Identifying gaps against modern cloud architecture principles Confirming platform requirements with architecture, engineering, and operational stakeholders	Defining reference architectures, design patterns, and platform guardrails Establishing environment segmentation, resource organisation, and platform boundaries Aligning platform design to enterprise architecture principles	Implementing network, identity, and environment configuration Applying platform-as-code, modular engineering, and controlled deployment practices Establishing baseline automation, tooling, and platform management components	and engineering practices Supporting operational alignment with platform behaviours and dependencies Enabling teams to transition from legacy or fragmented environments Ensuring platform knowledge, documentation, and responsibilities are clear	Identifying refinement opportunities and environment improvements Adjusting patterns, tooling, or engineering approaches as needed Preparing guidance for future platform expansion or capability enablement
What This Provides	A well-evidenced understanding of the current platform landscape and the requirements for foundational enablement.	A clearly defined cloud and infrastructure foundation that directs how environments should be structured and evolve.	Confidence and clarity for teams interacting with the new platform foundations.	Clear outputs that explain current state and required attention.	A structured environment for sustained platform integrity and continuous architectural evolution.

Service-Level Benefits

The key business-level benefits of the service are:

- Strengthens stability across core cloud and infrastructure platforms.
- Improves control over foundational services and configurations.
- Reduces operational risk from inconsistent or legacy environments.
- Enables predictable change across hybrid and cloud estates.
- Supports reliable workload performance and platform behaviour.
- Simplifies management of complex infrastructure dependencies.
- Establishes clear structures for future platform evolution.
- Improves oversight through defined patterns and standards.
- Enhances operational resilience and continuity readiness.
- Reduces effort required to maintain core environments.

Service Scope

In-Scope Summary

The Cloud & Infrastructure Enablement Service Stream covers the structured activities required to design, engineer, and establish the foundational cloud and infrastructure platforms that support reliable and scalable digital operations.

It focuses on defining architectural patterns, building platform components, aligning cloud and hybrid environments, and ensuring technical teams can adopt and operate the platform effectively.

These activities strengthen the Intelligent Core by delivering clarity, consistency, and technical integrity across the organisation's foundational technology estate.

Theme	Description
Current-State Platform Assessment	Reviewing existing infrastructure, cloud services, dependencies, and environment structures.
Foundational Architecture Design	Defining cloud landing zones, reference architectures, design patterns, and technical guardrails.
Platform Engineering & Environment Build	Deploying foundational services, platform components, and engineered environments using modern practices.
Identity, Network & Environment Alignment	Establishing core platform integrations that ensure consistent behaviour across cloud and hybrid estates.
Platform-as-Code & Engineering Enablement	Applying modular, repeatable engineering approaches to build consistent environments.
Operational Readiness & Platform Adoption	Providing guidance, documentation, and enablement for teams operating or deploying onto the foundation.
Foundational Tooling & Baseline Automation	Implementing tooling, automation, and management components required for stable platform operation.
Platform Review & Evolution Planning	Reviewing foundational environments and preparing for iterative refinement and future capability expansion.

Out-of-Scope Summary

The Cloud & Infrastructure Enablement Service Stream does not include advanced workload migration, application modernisation, solution delivery, or end-to-end transformation programmes.

It is not a managed service and does not provide ongoing operational management of the platform. The service is focused strictly on foundational environments, not application-layer design, high-code engineering, or enterprise-scale transformation beyond the defined scope.

Exclusion	Description
Workload or Application Migration	Moving applications, databases, or workloads to cloud or new platforms.
Application Modernisation or Refactoring	Redesigning or re-engineering applications or business systems.
Full Enterprise Platform Implementations	Deploying ERP, CRM, or other line-of-business systems.
Advanced High-Code Engineering	Developing custom engineering components, integrations, or complex automation beyond foundational needs.
Security Operations or Threat Management	Activities related to detection, response, vulnerability management, or cyber security operations.
Managed Platform or Infrastructure Services	Providing ongoing operational management of cloud or infrastructure environments.
Networking Overhaul or Large Infrastructure Refresh	Replacing or upgrading physical networks, datacentres, or major infrastructure components.
Organisation-Wide Transformation Initiatives	Delivering enterprise transformation programmes or large-scale operating model redesign.
Compliance, Audit, or Regulatory Services	Performing compliance assessments or formal certification activities.
Unscoped Environments or Teams	Reviewing or enabling areas not agreed within the service boundaries.

Service Element: Cloud Strategy and Adoption Roadmap

Description

The Cloud Strategy & Adoption Roadmap service defines the organisation's direction, priorities, and approach for adopting cloud services. It establishes the case for change, clarifies intended outcomes, and sets out the principles and decisions that will guide cloud adoption.

The service assesses readiness, identifies operational and architectural constraints, and prioritises workloads based on value, risk, and interdependencies. It also defines the governance, control, and structural considerations required before technical work begins.

The output is a clear and actionable adoption roadmap that aligns stakeholders, reduces uncertainty, and prepares the organisation to progress through cloud transformation in a controlled and deliberate manner.

Deliverables

Deliverable	Description
Cloud Strategy & Drivers Summary	Defined business drivers, desired outcomes, and strategic intent for cloud adoption.
Current-State Readiness Assessment	Analysis of organisational, technical, and operational readiness including risks, constraints, and capability gaps.
Workload Prioritisation Model	Classification and sequencing of workloads based on value, complexity, dependency, and suitability for cloud.
Adoption Approach & Guiding Principles	Defined principles for governance, architecture, security, and operating model considerations that inform cloud adoption.
High-Level Target Model Overview	Initial platform and structural assumptions to support future detailed design activities.
Cloud Adoption Roadmap	A sequenced plan that outlines the phases of adoption, key activities, and decision points.
Stakeholder Alignment and Briefing Material	Structured communication and summary packs to support stakeholder engagement and approval.

Dependencies

Delivery of this Service Element requires:

- Access to stakeholders able to describe business priorities, operational requirements, and strategic objectives.
- Availability of information regarding current systems, workloads, infrastructure, and cloud usage.
- Customer representatives who can describe governance expectations, security obligations, and compliance constraints.
- Agreement on the level of detail required for roadmap outputs and strategic recommendations.

Constraints

This Service Element is subject to the following constraints:

- Strategy development relies on the accuracy and completeness of information provided by the customer.
- Roadmap recommendations are indicative and require validation during later design phases.
- Deep financial modelling, licensing analysis, or total cost-of-ownership assessment may require additional engagement.
- Regulatory or industry-specific compliance modelling is not included unless explicitly agreed.
- No technical configuration, migration, or architectural implementation is performed under this Service Element.

Benefits

This Service Element strengthens The Intelligent Business by establishing clear strategic direction and the conditions required for deliberate and controlled cloud adoption.

It supports informed decision-making, reduces uncertainty across stakeholders, and ensures cloud transformation is aligned to organisational goals, operational realities, and architectural principles.

By defining priorities, dependencies, and governance considerations early, the service provides the structure needed to introduce cloud capability predictably and responsibly, enabling subsequent technical work to proceed with clarity and confidence.

848 Responsibilities

Under this Service Element, 848 will:

- Conduct assessments to establish readiness, drivers, constraints, and organisational priorities.
- Develop the cloud adoption strategy, guiding principles, and prioritisation model.
- Produce a structured and actionable adoption roadmap.
- Facilitate workshops and discussions with relevant stakeholders.
- Provide analysis, recommendations, and briefing materials to support alignment and approval.
- Ensure outputs align with The Intelligent Core methodology and the customer's strategic intent.

Customer Responsibilities

The customer must:

- Provide access to stakeholders with knowledge of business needs, operational practices, and strategic direction.
- Supply accurate information regarding existing infrastructure, workloads, applications, and cloud usage.
- Confirm organisational drivers, governance expectations, and security considerations.
- Review and validate findings, recommendations, and roadmap outputs.

- Approve strategic assumptions that will inform downstream design and implementation work.

Assumptions

This Service Element is delivered on the basis that:

- The customer can supply accurate information about existing systems and operating practices.
- Stakeholders will be available to participate in workshops, assessments, and review sessions.
- Strategic priorities and business objectives are defined and can be shared with 848.
- Roadmap timelines may evolve during later design or implementation phases.
- Any required detailed architectural design will be delivered under separate Service Elements.

Exclusions

This Service Element does not include:

- Design or deployment of any cloud or on-premises platform components.
- Technical configuration, migration, or modernisation of workloads.
- Development of detailed architecture artefacts or landing-zone designs.
- Creation of operating models, service management processes, or cloud governance frameworks.
- Financial modelling requiring granular utilisation metrics or tooling.
- Implementation of tools, automation, or cloud-native services.

Success Measures

This Service Element is successfully delivered when:

- Cloud drivers, priorities, and outcomes are defined and agreed.
- Readiness assessment findings are documented and validated.
- Workload prioritisation and sequencing are clearly established.
- Adoption principles and target structural assumptions are confirmed.
- A roadmap is produced, communicated, and approved by stakeholders.
- Alignment materials are delivered and acknowledged by customer representatives.

Service Element: Cloud Architecture & Migration Planning

Description

The Cloud Architecture & Migration Planning service develops the technical blueprints and structured migration plan required to move from the current-state environment to the defined cloud target state.

It translates strategic direction into actionable designs by defining the architectural patterns, governance considerations, sequencing logic, and platform requirements needed for a controlled transition to cloud services.

The service analyses dependencies, constraints, and workload characteristics to determine appropriate migration approaches and prepares the organisation for foundation build and subsequent implementation activities.

The outcome is a clear, structured, and technically grounded plan that enables cloud adoption to proceed reliably and in alignment with organisational intent.

Deliverables

Deliverable	Description
Current-State Architecture Assessment	Structured analysis of existing platforms, integrations, dependencies, and constraints.
Target-State Architecture Blueprint	High-level or detailed architecture design outlining the required cloud structures, patterns, and platform components.
Migration Approach Definition	Classification of workloads with recommended migration paths (e.g., rehost, replatform, refactor where applicable).
Sequencing and Dependency Model	Defined ordering of migrations based on technical dependencies, operational requirements, and business priorities.
Governance and Platform Considerations	Architectural guardrails, control requirements, and foundational assumptions to be used during platform build.
Integration and Connectivity Overview	High-level network, identity, and service integration considerations required for later implementation.
Architecture and Migration Planning Pack	Consolidated documentation summarising all design decisions, sequencing plans, and transition recommendations.
Stakeholder Review and Alignment Materials	Communication artefacts to support approval, technical alignment, and programme planning.

Dependencies

Delivery of this Service Element requires:

- Access to architectural, infrastructure, and operational information for all relevant workloads and platforms.
- Stakeholder input regarding prioritisation, constraints, and operational requirements.
- Visibility of existing integrations, network topologies, and identity structures.
- Agreement on the level of detail required for architectural artefacts and migration planning outputs.

Constraints

This Service Element is subject to the following constraints:

- Architectural designs rely on the accuracy and completeness of information provided by the customer.
- Sequencing plans may require refinement as foundation engineering is completed.
- Application-specific assessments may require engagement with application owners or third-party suppliers.
- No environment configuration, deployment, or migration activity is carried out under this Service Element.
- Detailed design of individual workloads or application components is not included unless explicitly agreed.

Benefits

This Service Element strengthens The Intelligent Business by providing a structured and technically informed plan for cloud adoption. It ensures that architectural decisions, migration sequencing, and platform assumptions are aligned to organisational needs and are supported by clear analysis of dependencies and constraints.

By defining the transition path from current-state to target-state architecture, the service enables cloud adoption to proceed in a controlled, predictable, and well-governed manner, reducing risk and supporting consistent operational outcomes.

848 Responsibilities

Under this Service Element, 848 will:

- Analyse current-state architecture, integrations, and dependencies.
- Develop the target-state architecture blueprint.
- Define appropriate migration approaches and workload classifications.
- Produce sequencing and dependency models based on organisational priorities.
- Document governance, integration, and platform considerations.
- Prepare architectural and planning artefacts for stakeholder approval.
- Facilitate review sessions to ensure alignment and shared understanding.
- Ensure outputs support downstream platform build and migration services.

Customer Responsibilities

The customer must:

- Provide access to current-state information, documentation, and system stakeholders.
- Supply details of business priorities, operational constraints, and expected outcomes.
- Make subject matter experts available for workshops and dependency discussions.
- Review and validate architectural designs and migration plans.
- Approve the assumptions and sequencing model that will guide downstream work.

Assumptions

This Service Element is delivered on the basis that:

- Relevant subject matter experts will be available during design and planning activities.
- The organisation has defined strategic objectives that inform architectural decisions.
- Existing documentation, system inventories, and architectural artefacts are accessible and reasonably accurate.
- Platform assumptions identified in this stage will be validated during the foundation build and migration execution phases.
- Any required detailed analysis of specific applications will be conducted separately.

Exclusions

This Service Element does not include:

- Deployment or configuration of cloud platforms or landing zones.
- Execution of workload migration or modernisation activities.
- Detailed low-level design of applications, databases, or integration services.
- Development of Infrastructure as Code or automation pipelines.
- Network, identity, or security configuration changes.
- Operational support or ongoing management of environments.
- Cost modelling beyond high-level architectural considerations.

Success Measures

This Service Element is successfully delivered when:

- Current-state architecture and dependencies are documented and validated.
- Target-state architecture designs are completed and approved.
- Migration approaches for all in-scope workloads are defined.
- A clear, sequenced migration plan is produced.
- Governance and architectural guardrails are agreed for downstream work.
- Stakeholders acknowledge the architecture and planning outputs as ready for platform build and migration activities.

Service Element: Azure Landing Zone & Cloud Foundation Build

Description

The Azure Landing Zone & Cloud Foundation Build service designs and deploys the core cloud environment required for secure, governed, and scalable use of Microsoft Azure. It implements the foundational platform components defined during earlier architecture and planning stages, including identity structures, network topology, security baselines, governance controls, and management configurations.

The service establishes a consistent and compliant environment that supports reliable operation of workloads and prepares the organisation for structured cloud adoption. The resulting platform provides the technical integrity needed for migration, modernisation, and ongoing cloud evolution.

Deliverables

Deliverable	Description
Landing Zone Design Pack	Documented design covering identity, networking, governance, management, and baseline security structures required for the landing zone.
Identity and Access Foundations	Configuration of Azure identity and access structures, including management groups, RBAC models, and alignment with the customer's directory environment.
Network and Connectivity Configuration	Deployment of core virtual network structures, routing, segmentation, and connectivity elements required for platform operation.
Security and Governance Baselines	Implementation of baseline Azure Policies, security controls, compliance settings, and resource governance conventions.
Logging and Monitoring Enablement	Configuration of monitoring, diagnostics, and logging services to support visibility of platform behaviour.
Management and Platform Services Setup	Configuration of management groups, subscription hierarchy, tagging conventions, automation accounts, and other platform services.
Operational Readiness and Validation Pack	Verification that landing zone components are deployed, aligned to design, and ready to support migration and platform use.
Documentation and Administration Pack	Documentation covering all deployed configurations, platform conventions, and operational guidance for customer teams.
Knowledge Transfer Session	Structured sessions to review the landing zone, explain operational expectations, and clarify governance and management responsibilities.

Dependencies

Delivery of this Service Element requires:

- Administrative access to the customer's Azure tenant and connected identity platform.
- Access to network and security stakeholders to define required connectivity and control boundaries.
- Agreement on landing zone design assumptions provided through previous planning stages.
- Availability of any required on-premises infrastructure for hybrid connectivity configurations.
- Confirmation of governance, compliance, or alignment requirements relevant to the landing zone.

Constraints

This Service Element is subject to the following constraints:

- Deployment is limited to foundational Azure platform components and does not include configuration of individual workloads or applications.
- Identity or network remediation may be required where existing configurations restrict the landing zone model.
- Complex regulatory frameworks may require additional governance design outside the baseline.
- Custom Policy definitions, role templates, or extended governance features require separate scoping.
- Hybrid connectivity capability depends on the readiness and stability of the customer's on-premises environment.
- No workload migration, data movement, or application platform configuration is included.

Benefits

This Service Element strengthens The Intelligent Business by establishing a secure, consistent, and operationally ready Azure foundation. It ensures cloud environments are structured and governed from the outset, reducing risk and improving predictability as cloud adoption progresses.

By implementing aligned identity, network, security, and management baselines, the service enables controlled platform evolution, supports reliable workload placement, and provides a dependable foundation for further migration and modernisation activity.

848 Responsibilities

Under this Service Element, 848 will:

- Produce the landing zone design based on agreed architectural direction.
- Configure identity, networking, governance, and management structures in the Azure platform.
- Apply baseline security controls and compliance settings.
- Deploy monitoring, diagnostics, and logging configurations.
- Validate that platform components operate according to design and are ready for workload onboarding.
- Deliver documentation and knowledge transfer to support operational readiness.

- Align the build to the standards and patterns defined for The Intelligent Core.

Customer Responsibilities

The customer must:

- Provide administrative access to the Azure tenant and associated identity services.
- Supply information regarding network boundaries, security requirements, and compliance expectations.
- Ensure availability of subject matter experts for design validation and configuration decisions.
- Review and approve design outputs and deployed configurations.
- Address on-premises network, firewall, or connectivity requirements needed for hybrid integration.
- Maintain governance and management responsibilities post-handover unless covered under a managed service.

Assumptions

This Service Element is delivered on the basis that:

- The customer's identity environment is stable and supports the required landing zone structure.
- Network configurations needed for hybrid connectivity are available and functional.
- Baseline governance and security requirements have been defined during prior planning phases.
- Azure subscriptions and licensing required for foundational services are active.
- Customer stakeholders will participate in workshops, reviews, and handover sessions.
- Ongoing platform management will be undertaken by the customer or a contracted managed service.

Exclusions

This Service Element does not include:

- Migration of workloads, applications, or data into the landing zone.
- Detailed application or database platform configuration.
- Deployment of PaaS services beyond those required for platform operation.
- Development of Infrastructure as Code templates or CI/CD pipelines.
- Operational support, monitoring, or management of the environment after handover.
- Custom governance frameworks or advanced compliance configuration.
- Remediation of existing identity, network, or security issues unless separately scoped.

Success Measures

This Service Element is successfully delivered when:

- The landing zone is deployed according to the approved design.
- Identity, security, network, and governance baselines are operational.
- Platform services and monitoring capabilities function as expected.
- Documentation is completed and reviewed by customer stakeholders.

- Knowledge transfer sessions are delivered to relevant teams.
- Customer representatives acknowledge that the Azure foundation is ready for migration and platform enablement activities.

Service Element: Cloud Migration & Modernisation Service

Description

The Cloud Migration & Modernisation Service executes the structured transition of workloads from existing environments into Azure or hybrid platforms. It applies the migration approaches defined during earlier planning stages and performs the technical activities required to move, configure, and validate workloads in their target state.

The service includes assessment of workload readiness, preparation of source and target environments, execution of migration tasks, and light modernisation where necessary to ensure compatibility and operational stability. It ensures that workloads integrate effectively with cloud identity, network, security, and management foundations, enabling them to operate reliably within the established cloud platform.

Deliverables

Deliverable	Description
Workload Readiness Assessment	Validation of workload dependencies, technical constraints, and migration prerequisites.
Migration Approach Confirmation	Final confirmation of migration method for each workload based on technical findings.
Source and Target Environment Preparation	Configuration of required source and destination settings to support migration execution.
Data Migration and Synchronisation	Controlled transfer and synchronisation of application, database, or file data as required.
Workload Migration Execution	Migration of workloads into the Azure or hybrid environment, using approved methods and tools.
Light Modernisation Activities	Minimal refactoring or configuration adjustments needed to ensure cloud compatibility.
Integration and Configuration Alignment	Integration of workloads with identity, network, security, and monitoring services.
Testing and Validation Pack	Structured testing confirming functional behaviour, connectivity, security alignment, and operational readiness.

Handover Summary and Transition Pack	Documentation covering migration outcomes, configuration changes, and operational expectations.

Dependencies

Delivery of this Service Element requires:

- Access to source systems, workloads, databases, and related infrastructure.
- Access to the customer's Azure environment and any required hybrid components.
- Availability of system and application owners to support readiness validation and testing.
- Appropriate licensing, migration tooling, and connectivity for the workloads in scope.
- Confirmed migration approaches and sequencing defined through earlier planning stages.

Constraints

This Service Element is subject to the following constraints:

- Migration outcomes depend on the stability, performance, and accessibility of source systems.
- Light modernisation is limited to changes required for cloud compatibility; extensive redesign is out of scope.
- Testing and cutover activities require coordination with customer teams and adherence to change control processes.
- Some workloads may require third-party vendor input or licensing validation.
- Performance optimisation outside migration acceptance criteria is not included.
- No deployment of landing zone components or foundational services is included.

Benefits

This Service Element strengthens The Intelligent Business by enabling workloads to transition into a secure, governed, and scalable environment in a controlled and predictable way. It reduces operational risk during migration, ensures workloads integrate with established cloud foundations, and supports the organisation in moving away from legacy constraints. By executing structured migration and targeted modernisation activities, the service provides a reliable path towards improved platform resilience and the long-term capability enabled by cloud adoption.

848 Responsibilities

Under this Service Element, 848 will:

- Conduct readiness assessments and confirm migration methods.
- Prepare source and target environments for migration activities.
- Execute workload migration and data synchronisation tasks.
- Apply configuration adjustments to support cloud compatibility.
- Integrate workloads with identity, network, security, and monitoring services.

- Perform testing and validation activities post-migration.
- Provide documentation and handover materials to support operational transition.
- Align migration activities with the patterns and standards defined for The Intelligent Core.

Customer Responsibilities

The customer must:

- Provide access to source systems, application owners, and technical SMEs.
- Supply information regarding dependencies, operational requirements, and change constraints.
- Validate and approve migration approaches, timelines, and cutover plans.
- Support testing, acceptance, and verification of migrated workloads.
- Maintain responsibility for change control, communication, and any required business approvals.
- Ensure licensing and vendor support requirements are addressed for workloads in scope.

Assumptions

This Service Element is delivered on the basis that:

- Workload information, application inventories, and dependency records are available and accurate.
- The Azure landing zone and cloud foundations are already deployed and operational.
- Customer teams participate in readiness assessments, testing, and acceptance activities.
- Migration activities can be planned and executed within the agreed windows.
- Any refactoring required for cloud compatibility is limited in scope and complexity.

Exclusions

This Service Element does not include:

- Design or deployment of cloud landing zones or foundational platform components.
- Extensive application redesign, redevelopment, or architectural re-engineering.
- Development of DevOps pipelines, IaC templates, or automation frameworks.
- Implementation of operational monitoring or ongoing platform management.
- Migration of unsupported legacy systems requiring custom tooling.
- Business process redesign or organisational change support.
- Performance tuning beyond acceptance-level validation.

Success Measures

This Service Element is successfully delivered when:

- Workload readiness assessments are completed and validated.
- Migration methods and sequencing are confirmed.
- Workloads are successfully migrated to the target environment.
- Light modernisation ensures stable operation within the cloud platform.

- Testing confirms connectivity, security alignment, and operational readiness.
- Documentation and handover materials are delivered.
- Customer stakeholders acknowledge successful migration and acceptance of workloads in their new environment.

Service Element: Cloud-Native Platform & Automation Enablement

Description

The Cloud-Native Platform & Automation Enablement service introduces and operationalises cloud-native capabilities within the organisation's established Azure environment.

It enables the structured use of platform services, container platforms, and automation patterns that extend the foundational cloud platform and support modern workload deployment.

The service provides targeted enablement of PaaS components, baseline container platforms, and platform-level automation required for consistent, scalable, and controlled cloud operations.

It ensures that cloud-native services align to identity, network, security, and governance models, preparing the organisation to adopt modern cloud capabilities in a reliable and predictable manner.

Deliverables

Deliverable	Description
Cloud-Native Enablement Design Pack	Defined patterns, configurations, and conventions for enabling cloud-native platform services within the existing landing zone.
PaaS Service Enablement	Deployment and configuration of agreed platform services such as App Services, Functions, or managed databases, aligned to governance and security requirements.
Container Platform Foundation	Baseline deployment of AKS or equivalent container platform with core configuration required for initial use.
Platform Automation Configuration	Implementation of automation scripts, runbooks, or Bicep/ARM templates for platform-level provisioning or operational tasks.
Integration and Governance Alignment	Validation that enabled services align with identity, network, security, and governance baselines.
Operational Readiness and Validation Pack	Testing and verification of cloud-native components to confirm operational behaviour and alignment with platform expectations.
Documentation and	Documentation covering configurations, platform-level automation, and operational guidance for customer teams.

Administration Pack	
Knowledge Transfer Session	Structured sessions to explain how cloud-native services and automation patterns are used, managed, and maintained.

Dependencies

Delivery of this Service Element requires:

- A deployed Azure landing zone with identity, network, security, and governance foundations.
- Administrative access to Azure services required for PaaS, container, and automation deployment.
- Agreement on which cloud-native components or services will be enabled.
- Access to customer stakeholders responsible for governance and platform oversight.
- Clarity on operational requirements, access controls, and usage expectations for cloud-native services.

Constraints

This Service Element is subject to the following constraints:

- Enablement is limited to platform-level PaaS, container, and automation services; application-level implementation is out of scope.
- Container platform deployment is limited to baseline configuration and does not include operational lifecycle management.
- Automation activities are restricted to platform provisioning and management tasks.
- Full DevOps operating model, CI/CD pipelines, and Infrastructure-as-Code libraries are not delivered.
- Advanced PaaS usage, such as enterprise-scale integration or API management patterns, may require additional scoping.
- Application refactoring or containerisation requires separate engagement.
- Consumption and configuration of cloud-native services must align with governance and security controls defined by the customer.

Benefits

This Service Element strengthens The Intelligent Business by enabling the organisation to use cloud-native capabilities in a structured and controlled way. It provides the platform-level services and automation patterns needed to support modern, scalable workloads and reduces reliance on traditional infrastructure models.

By operationalising cloud-native services and aligning them with established governance and security foundations, the service prepares the organisation to adopt modern engineering and deployment practices with greater confidence and reduced operational risk.

848 Responsibilities

Under this Service Element, 848 will:

- Define patterns and conventions for cloud-native platform enablement.
- Deploy and configure targeted PaaS and automation components.
- Implement baseline container platform configurations.
- Ensure platform components align with identity, network, security, and governance models.
- Validate the operational readiness of cloud-native components.
- Provide documentation and knowledge transfer on platform usage and management.
- Align delivery to the structures and principles established within The Intelligent Core.

Customer Responsibilities

The customer must:

- Provide administrative access to Azure services required for enablement.
- Supply information on governance, security, and operational policies relevant to cloud-native services.
- Confirm priorities regarding which PaaS or automation components to enable.
- Participate in reviews, validation steps, and knowledge transfer sessions.
- Manage application changes or development activities associated with consuming cloud-native services.
- Maintain responsibility for ongoing operational oversight unless supported by a managed service.

Assumptions

This Service Element is delivered on the basis that:

- The Azure landing zone and foundation platform are deployed and operational.
- Customer stakeholders can validate service enablement requirements and decisions.
- Required Azure subscriptions and licensing for cloud-native components are active.
- Platform-level governance and security controls have been defined during earlier phases.
- Application development teams will adopt cloud-native components independently of this Service Element.

Exclusions

This Service Element does not include:

- Detailed application design, refactoring, or modernisation.
- Development of CI/CD pipelines or automation frameworks beyond platform provisioning.
- Containerisation of existing applications.
- Enterprise-scale integration platforms or advanced PaaS architectures.
- Ongoing platform operations or lifecycle management.
- Infrastructure as Code library creation or DevSecOps tooling configuration.
- Migration of workloads into cloud-native services.

Success Measures

This Service Element is successfully delivered when:

- Cloud-native components are deployed and aligned to design decisions.
- Platform automation functions operate as expected.
- Container platform foundations are deployed and validated.
- PaaS services function within governance and security constraints.
- Documentation is completed and reviewed by customer teams.
- Knowledge transfer sessions are delivered.
- Customer stakeholders confirm readiness to consume cloud-native capabilities.

Service Element: SD-WAN Design & Deployment Service

Description

The SD-WAN Design & Deployment Service establishes a resilient, secure, and centrally managed wide-area network using Cisco SD-WAN technology.

It provides the architecture, configuration, and deployment activities required to introduce a software-defined network fabric that improves connectivity across sites, cloud platforms, and hybrid environments.

The service designs the SD-WAN topology, configures controller and edge components, and implements routing, segmentation, and policy models aligned to organisational requirements.

It integrates the SD-WAN platform with existing network and cloud foundations, enabling consistent performance, simplified management, and improved resilience across the technology estate.

Deliverables

Deliverable	Description
SD-WAN Architecture and Design Pack	Documented SD-WAN architecture covering controller topology, edge design, routing models, segmentation, cloud connectivity, and security patterns.
Controller Deployment and Configuration	Deployment and configuration of Cisco SD-WAN controllers, including vManage, vSmart, and vBond.
Edge Device Deployment	Installation and configuration of SD-WAN edge devices (physical or virtual) across agreed locations.
Routing, Segmentation, and Policy Configuration	Implementation of routing policies, segmentation structures, QoS, and traffic engineering rules.
Cloud Connectivity Enablement	Configuration of Cloud OnRamp or equivalent features to optimise connectivity to Azure and other cloud environments.
Telemetry, Monitoring, and Logging Setup	Enablement of SD-WAN monitoring, performance insights, and telemetry within Cisco management tools.
Cutover and Transition Support	Controlled cutover activities, validation of connectivity, and support during the transition to SD-WAN operation.

Operational Readiness and Validation Pack	Testing and verification confirming that SD-WAN services operate as intended and are ready for use.
Documentation and Administration Pack	Documentation covering SD-WAN configuration, design decisions, policy definitions, and operational guidance.
Knowledge Transfer Session	Structured sessions explaining SD-WAN operation, management tasks, and governance expectations.

Dependencies

Delivery of this Service Element requires:

- Customer procurement or availability of Cisco SD-WAN licensing and hardware or virtual appliances.
- Administrative access to relevant network, firewall, and Azure components.
- Availability of carrier circuits, transport links, or connectivity services required for SD-WAN operation.
- Access to on-premises or cloud network environments for integration.
- Engagement with customer network and security SMEs for validation and approval of design and policy decisions.
- Confirmation of network boundaries, routing requirements, and segmentation needs.

Constraints

This Service Element is subject to the following constraints:

- Deployment is limited to Cisco SD-WAN technologies; alternative platforms require separate scoping.
- Physical installation, cabling, and hardware logistics must be provided by the customer or a third party.
- Achievable performance and resilience depend on the quality of underlying connectivity and existing infrastructure.
- Integration with legacy routers, firewalls, or non-Cisco components may require additional work.
- No LAN redesign, firewall reconfiguration, or broader network transformation is included.
- SD-WAN policies depend on accurate application, routing, and traffic information provided by the customer.
- Ongoing management or monitoring of SD-WAN environments is out of scope.

Benefits

This Service Element strengthens The Intelligent Business by enabling a resilient and centrally managed network fabric that supports predictable, secure, and scalable operations.

It improves connectivity across cloud and hybrid environments, enhances performance through policy-driven routing, and simplifies network management.

By deploying Cisco SD-WAN within a governed architecture, the service provides the stability, control, and visibility required for reliable digital operations and supports the organisation's ability to evolve its environment without introducing unnecessary risk.

848 Responsibilities

Under this Service Element, 848 will:

- Develop the SD-WAN architecture and design in line with organisational requirements.
- Deploy and configure Cisco SD-WAN controllers and edge devices.
- Implement routing, segmentation, and policy structures.
- Enable cloud connectivity and optimise performance for hybrid and multi-cloud environments.
- Configure telemetry, monitoring, and logging capabilities.
- Conduct cutover activities and support the transition to SD-WAN operation.
- Validate platform behaviour and provide operational documentation.
- Deliver knowledge transfer sessions to customer teams.

Customer Responsibilities

The customer must:

- Procure and provide licensing and hardware required for Cisco SD-WAN.
- Provide access to network devices, firewall systems, and Azure components relevant to SD-WAN integration.
- Supply accurate network diagrams, routing requirements, and application traffic information.
- Ensure site readiness for edge device installation and connectivity.
- Participate in design reviews, policy decisions, and cutover planning.
- Validate testing outcomes and accept SD-WAN configurations prior to go-live.
- Maintain ongoing network operations unless supported by a managed service.

Assumptions

This Service Element is delivered on the basis that:

- Customer transport circuits are active and available for use.
- The Azure landing zone or equivalent cloud foundations are deployed and operational.
- Customer stakeholders participate in workshops, validation sessions, and cutover approval.
- Site access for deployment is available when required.
- Existing network and security configurations are stable enough to support SD-WAN integration.

Exclusions

This Service Element does not include:

- Deployment of non-Cisco SD-WAN platforms.

- LAN switching, Wi-Fi design, or local network remediation.
- Firewall replacement, redesign, or policy overhaul.
- Carrier circuit procurement or management.
- Development of DevOps pipelines or automation frameworks.
- Ongoing SD-WAN monitoring, event handling, or operational support.
- Application migration or refactoring activities.

Success Measures

This Service Element is successfully delivered when:

- SD-WAN architecture and design are approved by customer stakeholders.
- Controllers and edge devices are deployed and configured as designed.
- Routing, segmentation, and policies operate as expected.
- Cloud and hybrid connectivity function reliably.
- Telemetry and monitoring provide clear visibility of SD-WAN performance.
- Documentation and knowledge transfer artefacts are delivered.
- Customer stakeholders acknowledge successful deployment and readiness for operational use.

Service Element: Hybrid Connectivity & Network Architecture Design

Description

The Hybrid Connectivity & Network Architecture Design service defines the unified network architecture required to support secure, resilient, and predictable connectivity across on-premises environments, Azure, edge locations, and supporting services.

It establishes the patterns, routing models, and integration points that enable workloads and platforms to communicate reliably across hybrid and multi-cloud environments.

The service designs the connectivity boundaries, performance structures, and resilience patterns that link cloud foundations, on-premises networks, and SD-WAN services into a coherent architecture.

The resulting design ensures that the organisation can operate a consistent and well-governed network environment that supports stable platform performance and controlled evolution.

Deliverables

Deliverable	Description
Hybrid Connectivity Architecture Pack	Comprehensive architecture design covering on-premises, cloud, and edge connectivity patterns, routing structures, and integration points.
Azure Network Integration Design	Defined structures for VNet/VWAN connectivity, routing boundaries, cloud ingress/egress, and hybrid link patterns.
On-Premises Integration Mapping	High-level mapping of required connectivity between existing networks, cloud services, and dependent systems.
Routing and Traffic Flow Models	Documented routing, segmentation, and traffic flow designs across hybrid environments.
Resilience and Performance Design	Defined network resilience, redundancy, and performance patterns to support critical workloads.
SD-WAN Alignment Overview	Design considerations for integrating the hybrid network architecture with Cisco SD-WAN or existing SD-WAN environments.
Identity and Security Boundary Alignment	High-level alignment of network architecture with identity, governance, and security boundaries.
Architecture Validation Pack	Summary of assumptions, constraints, and design considerations validated with customer stakeholders.
Architecture Review and Handover Pack	Final documentation and materials for customer review, governance, and onward implementation planning.

Dependencies

Delivery of this Service Element requires:

- Access to current network diagrams, routing information, and connectivity documentation.
- Visibility of the Azure landing zone design and any existing cloud network structures.
- Engagement with customer network, infrastructure, and security stakeholders.
- Information regarding critical workloads, performance requirements, and operational constraints.
- Details of existing WAN, SD-WAN, VPN, or interconnect services in use.
- Confirmation of organisational governance and security expectations relevant to the network architecture.

Constraints

This Service Element is subject to the following constraints:

- Architectural design relies on accurate and up-to-date customer network information.
- Achievable routing and connectivity patterns may be limited by existing carrier circuits or legacy infrastructure.
- Security, identity, and compliance requirements may influence network design decisions.
- No physical deployment, configuration, or implementation of network devices is included.
- Firewall design, LAN redesign, or Wi-Fi architecture are out of scope.
- Multi-cloud architecture design beyond Azure requires separate scoping.
- Integration with third-party routing or security products may require vendor involvement.

Benefits

This Service Element strengthens The Intelligent Business by establishing a unified and well-structured network architecture that supports secure and predictable connectivity across all core environments.

It reduces fragmentation across on-premises and cloud networks, improves routing clarity, and ensures consistent behaviour of workloads and services. By defining a coherent connectivity model, the service enhances resilience, simplifies integration, and provides the stability required for controlled platform evolution and reliable hybrid operations.

848 Responsibilities

Under this Service Element, 848 will:

- Analyse current network structures, routing configurations, and connectivity requirements.
- Design the unified hybrid connectivity architecture across on-premises, cloud, and edge environments.
- Define routing, segmentation, and traffic flow patterns.
- Align network design with identity, governance, and security boundaries.
- Produce resilience and performance design considerations.

- Provide architecture documentation, review materials, and stakeholder validation sessions.
- Ensure designs align with The Intelligent Core principles and established cloud foundations.

Customer Responsibilities

The customer must:

- Provide accurate and up-to-date network documentation, routing information, and connectivity maps.
- Supply details of workloads, performance requirements, and critical interdependencies.
- Make network, infrastructure, and security SMEs available for design reviews.
- Validate design assumptions, connectivity requirements, and architectural decisions.
- Approve the final architecture for downstream implementation and integration.

Assumptions

This Service Element is delivered on the basis that:

- The Azure landing zone or equivalent cloud network structures are deployed or defined.
- Customer stakeholders can validate connectivity requirements and design assumptions.
- Existing networks are stable enough to support analysis and architectural definition.
- Carrier circuits, on-premises infrastructure, and cloud connections are available or planned.
- Any required firewall or LAN changes will be managed through separate engagements.

Exclusions

This Service Element does not include:

- Deployment or configuration of any network or connectivity components.
- Firewall redesign, rule configuration, or network security policy implementation.
- LAN switching, Wi-Fi design, or physical infrastructure work.
- Procurement or management of carrier circuits or connectivity services.
- Implementation of SD-WAN solutions or network appliances.
- Detailed design of non-Azure cloud network architectures beyond the agreed scope.
- Ongoing network operational support or monitoring.

Success Measures

This Service Element is successfully delivered when:

- Hybrid connectivity architecture is documented and approved by customer stakeholders.
- Routing, segmentation, and connectivity patterns are clearly defined and validated.
- Cloud and on-premises integration designs align with platform and security requirements.
- Resilience and performance patterns support organisational needs.
- Documentation and architecture packs are delivered and reviewed.

Service Element: Disaster Recovery & Business Continuity Enablement

Description

The Disaster Recovery & Business Continuity Enablement service designs and implements Azure-native recovery and continuity capabilities that protect critical workloads and support resilient operations.

It establishes the recovery objectives, platform patterns, and automation required to restore services following disruption, using Microsoft Azure's built-in replication, backup, and orchestration features.

The service enables structured failover and failback processes, validates recovery behaviour, and ensures continuity models align with the organisation's platform, governance, and security requirements.

The result is a cloud-based recovery capability that enhances resilience and prepares the organisation for controlled response to service interruptions.

Deliverables

Deliverable	Description
Recovery Objectives and Criticality Mapping	Defined RPO/RTO targets and workload criticality classifications.
Azure-Native DR Architecture Pack	Architecture design describing Azure-based recovery regions, replication models, and continuity patterns.
ASR Replication Configuration	Configuration of Azure Site Recovery for supported workloads, including replication policies and failover settings.
Azure Backup Enablement	Deployment and configuration of Azure Backup for workloads covered by backup requirements.
Recovery Automation and Runbooks	Implementation of Azure Automation or equivalent native orchestration for structured failover and recovery tasks.
Continuity Validation and DR Testing Pack	Testing scripts, execution, and validation to confirm recovery behaviour and alignment with objectives.
Monitoring and Alerting Alignment	Configuration of Azure Monitor alerts to support visibility of replication health and recovery readiness.
Documentation and Administration Pack	Documentation covering recovery architecture, configurations, runbooks, and operational guidance.

Knowledge Transfer Session	Structured session explaining DR patterns, recovery steps, and operational responsibilities.

Dependencies

Delivery of this Service Element requires:

- Access to Azure subscriptions, landing zone components, and required resource groups.
- Visibility of workload architectures, dependencies, and business-criticality classifications.
- Customer input to confirm recovery priorities, RPO/RTO targets, and acceptable recovery approaches.
- Sufficient connectivity, bandwidth, and identity configuration to support replication.
- Availability of Azure regions that meet replication and continuity requirements.
- Participation of workload owners for testing and validation activities.

Constraints

This Service Element is subject to the following constraints:

- DR capabilities are dependent on Azure-native functionality and region availability.
- RPO/RTO results may vary based on workload characteristics, replication behaviour, and network performance.
- Legacy or unsupported workloads may require refactoring before Azure-native replication can be used.
- DR testing must align with customer change control processes and available testing windows.
- No third-party DR tooling, backup platforms, or multi-cloud DR is included.
- Application-level recovery logic or custom DR integration is out of scope.
- Azure-native services may incur additional consumption costs for replication and failover environments.

Benefits

This Service Element strengthens The Intelligent Business by enabling reliable, platform-aligned recovery capabilities that support continuity of critical services.

It reduces the operational risk associated with platform failures, provides structured Azure-based recovery models, and ensures workloads benefit from cloud-native replication and automation.

By establishing predictable recovery processes and validating their behaviour, the service supports stable and resilient operations across the technology estate.

848 Responsibilities

Under this Service Element, 848 will:

- Define recovery objectives and workload criticality classifications.

- Design Azure-native DR architectures aligned with organisational requirements.
- Configure Azure Site Recovery and Azure Backup for in-scope workloads.
- Implement Azure Automation runbooks for recovery orchestration.
- Conduct DR tests to validate failover and failback behaviour.
- Provide documentation covering configurations, architecture, and operational guidance.
- Deliver knowledge transfer sessions to customer teams.
- Align all activity with The Intelligent Core principles and existing cloud foundatio

Customer Responsibilities

The customer must:

- Provide workload information, dependencies, and criticality classifications.
- Supply access to Azure resources and any required identity or network components.
- Confirm recovery objectives and approve DR architecture decisions.
- Participate in testing, validation, and acceptance of DR capabilities.
- Maintain responsibility for ongoing backup, monitoring, and replication operations unless supported by a managed service.
- Ensure business units are available to support DR validation activities as required.

Assumptions

This Service Element is delivered on the basis that:

- Azure landing zone foundations and required connectivity are already deployed.
- Workloads intended for replication are technically compatible with Azure-native DR patterns.
- Customer stakeholders participate in recovery planning and testing activities.
- Required Azure regions support the necessary services and replication capabilities.
- Operational responsibilities post-handover are clearly defined and accepted by customer teams.

Exclusions

This Service Element does not include:

- Deployment or configuration of third-party DR or backup solutions.
- Full business continuity planning or organisational response design.
- Detailed application-level resilience engineering.
- Network design, firewall configuration, or routing changes unrelated to DR.
- Multi-cloud DR architecture or cross-cloud continuity patterns.
- Ongoing DR testing, monitoring, or operational management.
- Migration or modernisation of workloads outside the DR configuration scope.

Success Measures

This Service Element is successfully delivered when:

- RPO/RTO objectives and workload classifications are agreed and documented.
- Azure-native recovery architecture designs are approved by customer stakeholders.
- Replication and backup configurations are deployed and validated.

- Recovery automation is implemented and tested.
- DR tests confirm recovery behaviour and readiness.
- Documentation and knowledge transfer artefacts are delivered.
- Customer stakeholders acknowledge successful enablement of cloud-based recovery capabilities.

Service Element: Cloud Cost & Performance Optimisation Review

Description

The Cloud Cost & Performance Optimisation Review assesses the organisation's Azure environment to identify opportunities to improve cost efficiency, performance, and operational effectiveness.

It evaluates resource consumption, configuration patterns, governance alignment, and workload behaviour using Azure-native insights, telemetry, and analytical tools.

The service provides clear, prioritised recommendations that support improved utilisation, reduced waste, and stronger financial and operational control.

The outcome is an evidence-based view of the environment's optimisation potential, enabling IT leadership to make informed decisions about improvements without disrupting ongoing operations.

Deliverables

Deliverable	Description
Cost Consumption Analysis	Assessment of Azure spend, usage patterns, waste, and cost anomalies.
Performance and Capacity Review	Evaluation of resource performance, utilisation, and alignment to workload requirements.
Governance and Tagging Assessment	Review of tagging standards, resource grouping, and governance alignment.
Configuration and Architecture Check	Analysis of platform-level configuration against best practice for efficiency and performance.
Right-Sizing Recommendations	Recommendations for resizing, reconfiguration, or decommissioning of resources.
Optimisation Recommendations Pack	Consolidated guidance on cost, performance, and efficiency improvements.
Prioritised Remediation Plan	Defined priorities, dependencies, and effort-level guidance for optimisation activities.
Executive Summary Report	High-level overview of findings, insights, and outcomes to support decision-making.
Stakeholder Review Session	A structured walkthrough of findings and recommended next steps.

Dependencies

Delivery of this Service Element requires:

- Access to Azure subscriptions, monitoring data, and cost management insights.
- Availability of tagging conventions and governance policies.
- Visibility of workload performance baselines, where available.
- Engagement with stakeholders responsible for cloud governance and operational oversight.
- Access to relevant Azure monitoring, logging, and performance data sources.

Constraints

This Service Element is subject to the following constraints:

- The accuracy of findings depends on the completeness and quality of monitoring, governance, and tagging data.
- Some optimisation opportunities may require separate design or implementation services.
- Legacy or hybrid dependencies may limit achievable performance or cost improvements.
- Deep application-level analysis or performance tuning is out of scope.
- Azure-native insights are dependent on region availability and supported resources.
- No live reconfiguration or operational changes are made during the review.

Benefits

This Service Element strengthens The Intelligent Business by improving the efficiency, predictability, and financial control of cloud operations.

It provides clarity on cost drivers, identifies underperforming or inefficient resources, and highlights governance or configuration issues that affect operational stability.

By offering clear, prioritised recommendations, the service supports informed decision-making and enables targeted improvement that enhances platform reliability and value.

848 Responsibilities

Under this Service Element, 848 will:

- Conduct cost, performance, and configuration assessments using Azure-native insights.
- Review governance, tagging, and resource structures.
- Analyse utilisation, performance, and consumption patterns across the environment.
- Produce clear, actionable optimisation recommendations.
- Create an executive summary and remediation plan.
- Facilitate review sessions with stakeholders to explain findings and next steps.
- Align analysis to The Intelligent Core principles and customer governance expectations

Customer Responsibilities

The customer must:

- Provide access to Azure cost data, monitoring tools, and relevant subscriptions.

- Supply governance standards, tagging policies, and resource ownership details.
- Support discussions with workload owners and operational teams.
- Validate findings and confirm priorities for optimisation recommendations.
- Approve access required for analysis activities.

Assumptions

This Service Element is delivered on the basis that:

- Monitoring and cost data is available, accessible, and sufficiently detailed for analysis.
- Azure foundation and governance structures are partially or fully implemented.
- Stakeholders can describe workload criticality, performance expectations, and operational constraints.
- Recommendations may require additional services for implementation.
- Customer teams will participate in review sessions and decision-making activities.

Exclusions

This Service Element does not include:

- Implementation of optimisation recommendations.
- Redesign of workloads or applications.
- Development of CI/CD pipelines or automation tooling.
- Deep application performance tuning.
- Vendor or contract negotiation.
- Multi-cloud cost analysis or non-Azure optimisation.
- Ongoing monitoring, reporting, or continuous FinOps services.
- Any operational changes made within the customer environment.

Success Measures

This Service Element is successfully delivered when:

- Cost and performance assessments are completed and validated.
- Governance and configuration insights are documented clearly.
- Right-sizing and optimisation recommendations are produced.
- A prioritised remediation plan is created and approved.
- An executive summary is delivered and understood by stakeholders.
- Customer teams acknowledge the findings and next steps.