848

848 Secure Business - Protect

Part of

The Secure Business

Prepared by

Dave Cheetham

Pursuit Intelligence and Growth Lead

Monday, 05 January 2026

Driven by **people.** Powered by **intelligence.** Value chain **led.**

Service Overview and Context

What Our Customers Experience

Organisations operate in environments where digital services, users, and data move continuously across cloud and on-premises platforms. As these environments expand, maintaining consistent safeguards becomes more challenging.

Controls are applied unevenly, configurations drift over time, and protective measures fail to keep pace with new ways of working. Teams struggle to confirm whether security safeguards are in place, whether they operate correctly, and whether changes across the environment introduce new exposure.

These conditions increase operational risk. Protection tasks become fragmented, governance lacks the evidence needed to assure security, and users encounter inconsistencies that undermine safe practice.

As threats evolve and service portfolios grow, organisations recognise the need for a clear, structured way to establish dependable safeguards that support secure and predictable day-to-day operation.

Our Framework for Clarity and Improvement

848's Intelligent Business Framework provides the structure organisations use to build and maintain dependable capability across their technology, governance, and operational landscape.

It defines how outcomes are achieved, how capability is strengthened, and how services contribute to measurable improvement.

The Framework ensures that safeguards are introduced deliberately, aligned to organisational needs, and delivered through predictable processes that maintain clarity and accountability.

Within this structure, each outcome area addresses a core condition required for safe and effective operation. The Framework provides a common language for determining priorities, assessing impact, and coordinating change.

This ensures that protective measures support not just technical requirements, but also governance, operational workflows, and the organisation's wider performance goals.

The Secure Business Outcome Area

The Secure Business outcome area supports safe operation by establishing the protection, control, and resilience required to manage security effectively. It embeds security into everyday work, ensuring that safeguards are applied consistently and aligned to organisational expectations.

This outcome area focuses on maintaining dependable service delivery in environments where risk changes quickly and where protection must support how work is carried out, not constrain it.

By strengthening this area, organisations improve visibility of their exposure, maintain confidence in their protective posture, and apply safeguards in a structured and proportionate way.

The Secure Business improves accountability, supports responsible decision-making, and underpins the stable operating conditions required across the Intelligent Business.

848 Secure Business – Protect

The Protect Service Stream establishes the safeguards an organisation depends on to operate securely. It applies the controls, configurations, and behavioural measures required to maintain safe, predictable conditions across people, devices, data, and cloud services.

Protect addresses the operational challenge of inconsistent or incomplete security measures by creating a structured approach to implementing and governing protective controls.

As part of the Secure Business outcome area, Protect ensures that access is governed responsibly, that devices and collaboration platforms operate within defined boundaries, and that information is handled safely throughout its lifecycle.

The stream supports the Intelligent Business by establishing a consistent protection model that allows modern services, hybrid work, and digital change to progress on a secure foundation.

Protect strengthens organisational capability by ensuring safeguards are introduced predictably, aligned to real operating conditions, and embedded into routine practice.

This clarity and consistency enable teams and leaders to maintain trust, uphold obligations, and support organisational performance with confidence.

Purpose of This Document

This document defines how 848 delivers the Protect Service Stream within the Secure Business outcome area. It explains the purpose of the stream, how it aligns to the Intelligent Business Framework, and what customers can expect from its delivery.

It describes the scope, method, and conditions required for establishing protective safeguards and outlines the structure through which the service is governed.

The document is intended for procurement teams, security leaders, and operational stakeholders who require clear, dependable information about how Protect strengthens the organisation's protective posture.

It should be read alongside the Intelligent Business Framework and the Secure Business overview, which together explain how Protect contributes to safe, reliable, and well-managed operations.

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.

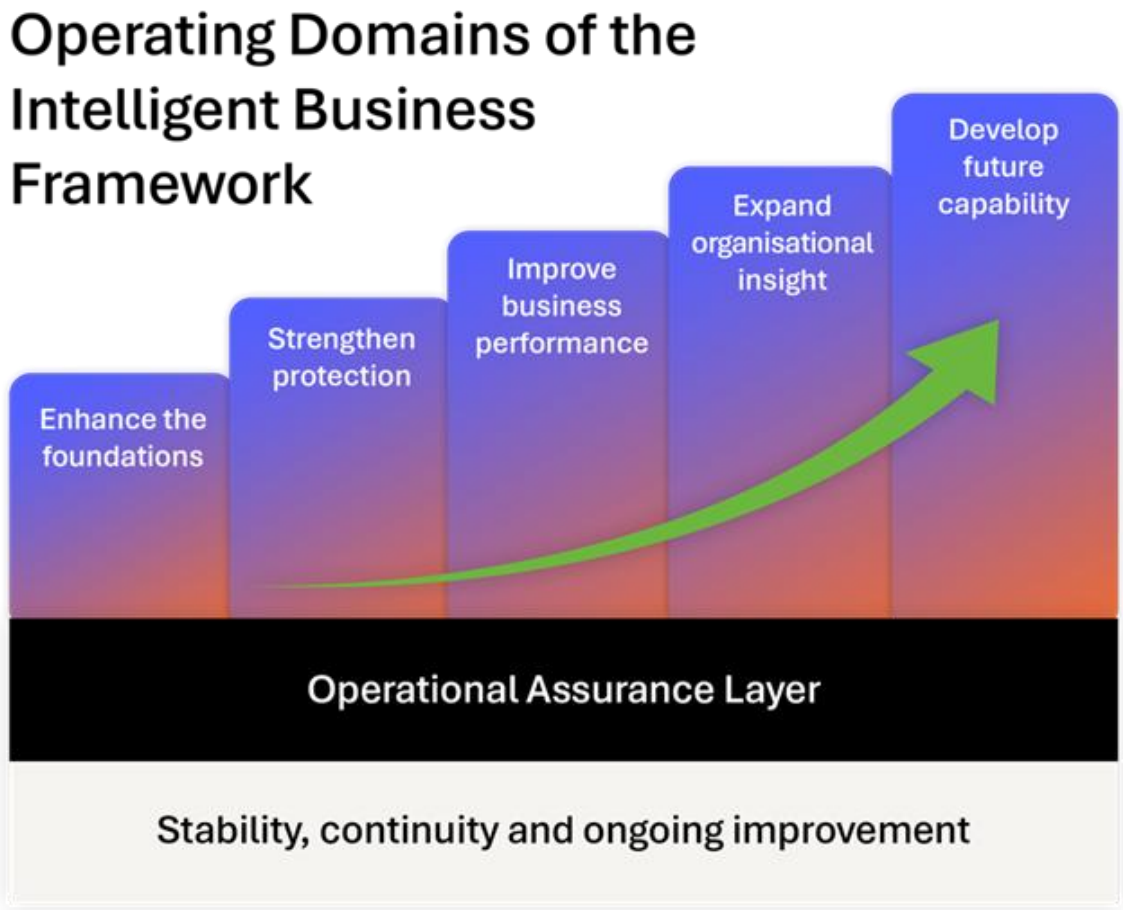
An Intelligent Business has clear visibility of its environment, understands how its services and processes interact, and makes decisions based on evidence, risk, and organisational impact. It can respond effectively to new demands, maintain operational continuity as conditions change, and introduce 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

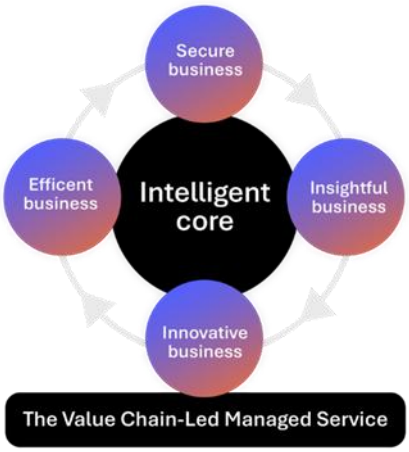
An Intelligent Business strengthens capability across several interconnected domains that influence how effectively the organisation operates. These domains reflect the areas where stability, protection, performance, insight, and future capability are developed over time. Each domain represents a different 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.

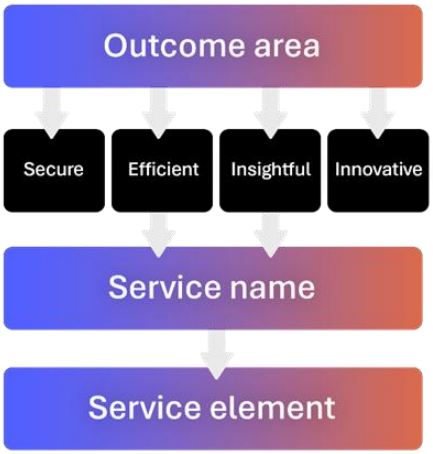
The Value Chain-Led Managed Service

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 Secure Business

The Secure Business is one of the six outcome areas that make up the Intelligent Business Framework. It represents the organisational conditions required to operate safely, maintain control, and manage security in a way that supports wider business objectives. Within the Framework, the Secure Business strengthens the organisation's ability to reduce exposure, maintain resilience, and ensure that protection is integrated into everyday operations rather than treated as a separate technical activity.

What the Secure Business Is

The Secure Business outcome area focuses on the capability an organisation needs to protect people, data, platforms, and operations in a controlled and consistent manner. It helps organisations maintain dependable service delivery in environments where risks evolve quickly and where security must support, not constrain, how work is carried out. Rather than addressing threats in isolation, the Secure Business provides a structured way to assess exposure, understand risk, and maintain appropriate safeguards across the organisation.

Security within this outcome area is not limited to technical controls. It includes how the organisation manages access, governs information, validates behaviour, and responds to emerging conditions. The Secure Business contributes to stability, continuity, and responsible operational practice by ensuring that protection is applied proportionately and aligned to the organisation's risk landscape and operating environment.

How Work Is Structured Within the Secure Business

To organise the work required across this outcome area, the Secure Business is delivered through five Service Streams. Each Stream represents a different aspect of security capability and provides a defined structure for assessment, protection, monitoring, response, and recovery. While each Stream focuses on a distinct area of work, together they provide a coherent approach for maintaining appropriate levels of protection and for managing security in a predictable and systematic way.

This structure allows organisations to engage with the areas that matter most to them, without needing to follow a fixed sequence or maturity path. It ensures that each service delivered within the Secure Business contributes to a clear outcome and is aligned to the organisation's wider operating model and priorities.

What the Secure Business Helps Organisations Achieve

The Secure Business supports organisations by strengthening their ability to:

- Maintain safe and reliable operations in changing conditions;
- Reduce exposure through appropriate safeguards and informed decision-making;
- Ensure consistent standards of control, governance, and oversight;
- Integrate security considerations into routine activity and project delivery;
- Understand how security affects operational performance and organisational continuity.

These contributions are defined in outcome terms rather than technical terms. The Secure Business enables organisations to maintain trust, uphold obligations, and operate confidently, even as their environments grow and evolve.

How This Outcome Area Supports the Intelligent Business

By developing protection, control, and resilience in a structured way, the Secure Business helps organisations build the dependable foundations that support efficiency, insight, and future capability across the wider Framework. It ensures that work carried out within this outcome area is aligned to organisational objectives, contributes to long-term capability, and reinforces the operating conditions an Intelligent Business depends on.

848 Secure Business – Protect

Alignment to The Intelligent Business

The Protect Service Stream strengthens the Intelligent Business by establishing the safeguards required for secure, reliable, and well-governed operation.

It ensures that identity, devices, data, and cloud services operate within clear security boundaries, supporting the organisation's ability to deliver work safely as conditions evolve. Protect provides the controls that underpin stable day-to-day performance and allow teams to operate with confidence.

Within the Intelligent Business Framework, Protect supports operational reliability by ensuring that essential security measures are applied consistently across the environment. This reduces the likelihood of compromise, prevents configuration drift, and maintains the conditions required for dependable performance.

By introducing safeguards in a structured way, Protect improves the flow of value across the Secure Business and supports responsible decision-making.

Protect also supports human-centric operation by providing users with a secure, predictable environment in which to work. Clear access conditions, consistent configuration across devices, and governed collaboration practices reduce friction and enable users to perform tasks safely.

This improves confidence, strengthens accountability, and ensures that protective measures align to how the organisation functions in practice.

Through these contributions, Protect reinforces the operating conditions that support efficiency, insight, and innovation across the Intelligent Business. It ensures that as the organisation introduces new services, modernises platforms, or changes ways of working, the underlying security model remains stable, dependable, and aligned to organisational expectations.

Service Purpose

The Protect Service Stream exists to ensure that an organisation has the safeguards required to operate securely and responsibly every day. It addresses the practical challenge of environments where protective measures are inconsistent, outdated, or applied unevenly across users, platforms, and services.

Without dependable safeguards, organisations experience increased risk, reduced resilience, and uncertainty in how securely their systems are operating.

Protect resolves this by establishing clear, structured controls that govern access, secure devices, protect information, and maintain security across cloud and collaboration platforms. It improves the organisation's capability to prevent compromise, reduce exposure, and maintain stability as environments evolve.

By applying safeguards in a predictable and evidence-led way, the stream ensures that essential protections function reliably and support safe day-to-day operation.

The purpose of Protect is to create a consistent and maintainable protection model that strengthens operational security, supports accountable governance, and enables users to work confidently within defined security boundaries.

This gives leaders and teams a dependable foundation on which to introduce change, adopt modern services, and progress security improvements across the Secure Business outcome area.

What This Service Provides

The Protect Service Stream provides individuals across the organisation with the safeguards required to work securely and confidently. It ensures that controls are applied consistently, that users operate within governed boundaries, and that day-to-day activity is supported by a stable and predictable security environment. Each role group benefits from clearer protection, stronger governance, and reduced operational uncertainty.

Role Group	What They Gain	Why They Matter
Executive Teams & Senior Leaders	Clear assurance that protective measures are in place to support safe and reliable operation. Evidence that safeguards align with organisational priorities and risk expectations. Confidence that the organisation can adopt modern working practices without increasing exposure.	They set strategic direction, approve investment, and hold accountability for organisational resilience.
Governance, Risk & Compliance Stakeholders	Reliable insight into how safeguards are applied across systems and services. Clear conditions for monitoring control effectiveness and validating compliance.	They oversee risk, obligations, and assurance requirements that influence organisational decision-making.

	Structured protection measures that support responsible governance and audit readiness.	
Security & Technology Leaders	A consistent foundation of technical and operational controls that support secure platform management. Clear access boundaries, configuration standards, and behavioural safeguards. Improved ability to plan, prioritise, and coordinate protection across the environment.	They direct how protective controls are applied and ensure that platforms operate securely as conditions change.
Operational & Infrastructure Teams	Defined configuration baselines and governance tasks that support day-to-day security management. Clarity on how controls should be applied and maintained across devices, platforms, and services. Reduced uncertainty caused by drift, inconsistent configuration, or undocumented practices.	They maintain the systems and services through which protective controls operate in practice.
Security Operations & Monitoring Functions	Clear conditions for secure access, device compliance, and collaboration behaviour. Dependable controls that improve the accuracy of detection and alerting. Visibility into protective measures that strengthen operational response capability.	They interpret security signals and respond to events. Consistent safeguards improve the quality and reliability of their work.

How This Service Is Delivered

The Protect Service Stream is delivered through a structured methodology that ensures safeguards are designed, configured, and embedded in a consistent and dependable way.

This approach enables organisations to establish protective controls that operate reliably across identity, devices, data, cloud platforms, and collaboration services.

Each stage of the method builds towards a stable and repeatable protection model that supports secure day-to-day operations.

Method Component	Stage 1: Establish Context & Requirements	Stage 2: Design Safeguards & Control Structures	Stage 3: Configure & Implement Controls	Stage 4: Embed Safeguards into Operations	Stage 5: Transfer Knowledge & Confirm Readiness
Stage Description	This stage confirms the conditions in which protective measures will operate and identifies the factors that influence how safeguards should be applied.	This stage translates organisational requirements into defined technical and operational safeguards that support safe day-to-day operation.	This stage applies the designed safeguards across relevant platforms and services to create a consistent protective environment.	This stage integrates protective measures into everyday working practices so that safeguards remain effective, maintained, and aligned to organisational processes.	This stage ensures the organisation can maintain its protective environment with confidence and clarity.
Purpose of the Stage	To ensure that all protection activity aligns to real operating conditions and reflects organisational priorities.	To create a dependable protection model that supports responsible and secure use of technology.	To ensure safeguards are implemented in a consistent and reliable manner across the environment.	To ensure safeguards operate as part of routine activity rather than as one-off configurations.	To ensure the organisation can sustain safeguards independently or with managed support.
Activities Included	Reviewing organisational objectives, constraints, and operating conditions Understanding user needs, service	Designing control models for identity, devices, collaboration, data, and cloud services	Configuring controls within Microsoft 365, Azure, and related services	Defining governance tasks, monitoring expectations, and operational procedures	Walking through configuration decisions and implemented safeguards

	expectations, and access patterns Identifying dependencies across platforms, roles, and business units Confirming governance structures and operational responsibilities	Defining access boundaries, configuration standards, and behavioural expectations Aligning designs to Zero Trust principles and Microsoft-recommended practices Validating that proposed safeguards support identified operational and governance needs	Applying identity, device, collaboration, and data protection settings Implementing secure baselines and validating initial control behaviour Ensuring controls operate predictably and meet design expectations	Integrating controls into service workflows and administrative processes Providing guidance for teams on how to support and maintain protective measures Reinforcing expected user behaviours through targeted communication or simulation	Providing documentation, governance guidance, and operational instructions Clarifying roles and responsibilities for ongoing control ownership Conducting structured handover sessions to confirm readiness
What This Provides	A clear understanding of the environment being protected and the requirements that safeguard design must support.	A structured and coherent design that defines how protective controls will operate across the environment.	A functioning protection boundary that establishes secure conditions for users, devices, and services.	Established operational practices that sustain protection without introducing friction or additional risk.	A clear understanding of how to operate, oversee, and maintain the organisation's protective environment.

Service-Level Benefits

The key business-level benefits of the Protect service are:

- Reduces security breaches through consistent, preventative safeguard controls.
- Ensures only trusted users and devices access organisational resources safely.
- Strengthens endpoint resilience with secure, policy-aligned device configuration.
- Enables safe collaboration and communication across email, Teams, and SharePoint.
- Protects sensitive information through structured classification, labelling, and DLP.
- Improves governance of SaaS applications and reduces cloud application risk.
- Establishes stable, secure platform baselines across Microsoft 365 and Azure.
- Reduces human-driven risk through targeted simulation and awareness activities.
- Clarifies operational security responsibilities through defined governance tasks.
- Supports confident technology modernisation with dependable security foundations.

Service Scope

In-Scope Summary

The Protect Service Stream covers the design, configuration, and embedding of safeguards that support secure and responsible operation across identity, devices, data, and cloud services.

It focuses on establishing consistent protective measures, applying defined control structures, and integrating these safeguards into day-to-day operational practice.

The scope includes the technical and operational activities required to introduce protection in a structured and dependable manner, based on the conditions and evidence confirmed during delivery.

Theme	Description
Protective Control Design	Designing identity, device, collaboration, and data protection models that support safe and predictable operation.
Configuration of Safeguards	Applying protective controls, configuration baselines, and access boundaries within Microsoft cloud platforms.
Governed Access and Permissions	Establishing controlled access models and enforcing conditional and risk-based access requirements.
Device and Endpoint Protection	Configuring device compliance, endpoint security policies, and baseline protections for organisational devices.
Secure Collaboration and Workflows	Applying protection to collaboration platforms, content sharing, and service-level behaviours.
Data Protection Measures	Implementing classifications, labels, and protective policies aligned to information handling expectations.
Cloud and Platform Hardening	Configuring secure settings within Microsoft 365 and Azure to reduce exposure and maintain safe operating conditions.
Operational Embedding	Defining governance tasks, user expectations, and procedures required to sustain protective measures.

Knowledge Transfer and Handover	Providing guidance, documentation, and handover required for ongoing operation of the protective environment.

Out-of-Scope Summary

The Protect Service Stream does not include remediation of existing issues, incident response, continuous monitoring, or delivery of services outside the boundaries of safeguard design, configuration, and embedding.

It does not cover custom development, third-party security tooling, or activities that sit within other Secure Business streams such as Identify, Detect, Respond, or Recover.

These clarifications are included to prevent ambiguity and ensure Protect remains focused on establishing dependable protective controls.

Exclusion	Description
Remediation of Pre-Existing Issues	Fixing misconfigurations, vulnerabilities, or operational problems identified before or during delivery.
Security Monitoring or Detection	Providing continuous monitoring, alert triage, or threat detection functions.
Incident Response or Forensics	Investigating events, performing root-cause analysis, or responding to active incidents.
Solution or Architecture Design Beyond Protection	Producing broader architectural designs or models unrelated to safeguard implementation.
Development or Custom Engineering	Building custom applications, scripts, or integrations not required for safeguard configuration.
Third-Party Security Tools	Configuring or integrating tools outside the Microsoft security ecosystem unless explicitly agreed.
Ongoing Operational Management	Running the protective environment on behalf of the customer after implementation.
User Training Beyond Protection Awareness	Delivering full end-user training programmes unrelated to protective behaviours.
Unscoped or Unavailable Systems	Protecting systems, services, or platforms not included in the agreed scope or where access cannot be provided.

Service Element: Identity & Access Management (IAM) Enablement

Description

The Identity & Access Management Enablement element establishes the controls an organisation requires to govern who can access systems, applications, and information. It delivers a structured identity model that enforces secure authentication, adaptive access conditions, and clear lifecycle governance across users, devices, and applications.

The service designs and configures identity safeguards using Microsoft Entra ID and related Microsoft 365 capabilities, applying Conditional Access, MFA, privileged access controls, SSO integration, and joiner–mover–leaver processes. The outcome is a resilient, least-privilege identity environment aligned to Zero Trust principles, enabling users to access services securely and predictably.

Deliverables

Deliverable	Description
IAM Design and Configuration Plan	A validated design document that defines authentication requirements, access conditions, identity governance structures, and Zero Trust alignment for the organisation's identity environment.
Configured Identity Protections	Implemented identity safeguards across Entra ID, including MFA enforcement, Conditional Access policies, session controls, and authentication protections aligned to agreed requirements.
Privileged Access Governance	Configured PIM settings, approval workflows, and elevated access controls that enforce least-privilege access and strengthen governance of privileged accounts.
SSO and Federation Configuration	Configuration of SSO integrations and identity federation with approved applications or platforms, ensuring consistent and secure access boundaries.
Joiner–Mover–Leaver Processes	Defined and implemented identity lifecycle processes and supporting automation to ensure consistent provisioning, change management, and deprovisioning of user access.
Operational and Configuration Documentation	Documentation describing configuration decisions, policy settings, operational requirements, and governance expectations to support ongoing operation.
Handover and Readiness Confirmation	A structured handover session and acceptance summary confirming effectiveness of implemented controls and readiness for transition to operational ownership.
Knowledge Transfer Sessions	Guided walkthroughs of design, configuration, and governance tasks to ensure customer teams understand how to operate and maintain applied identity controls.

Dependencies

Delivery of this Service Element requires the following:

- Active Microsoft licensing that supports the identity features being configured (e.g., Microsoft 365 E5, Entra ID P2).
- Administrative access to Entra ID, Microsoft 365, and any systems required for SSO or directory integration.
- Availability of stakeholder representatives who understand identity governance, access requirements, and current operational processes.
- Where lifecycle automation is included, access to HR or directory data sources required for JML integration.
- Access to Intune or Defender for Endpoint if Conditional Access policies rely on device compliance signals.
- A single primary tenant in scope, unless explicitly agreed otherwise.

Constraints

This Service Element is subject to the following constraints:

- The effectiveness of Conditional Access and MFA enforcement depends on the accuracy and completeness of identity data available in the customer environment.
- JML automation may require additional integration activity where HR or directory systems do not expose required attributes.
- SSO integration depends on the compatibility and capability of the target application or identity provider.
- Only identity-related configurations are included; broader architectural or operational redesigns fall outside this Service Element.
- Delivery is limited to the systems, domains, and identity sources defined at the outset

Benefits

This Service Element improves the organisation's ability to operate as a Secure Business by establishing reliable control over who can access systems and information.

It strengthens resilience by ensuring authentication and access conditions are applied consistently, reduces exposure by enforcing least-privilege principles, and supports accountable governance through structured identity lifecycle management.

This creates a predictable access environment that enables users to work securely and allows the organisation to adopt modern services with greater confidence.

848 Responsibilities

Under this Service Element, 848 will:

- Design the IAM model, including authentication requirements, access conditions, and identity governance structures.
- Configure Entra ID identity controls, including MFA, Conditional Access, session policies, and authentication protections.

- Implement PIM roles, workflows, and governance settings for privileged accounts.
- Configure SSO integrations and identity federation where included in scope.
- Implement defined JML processes and supporting automation.
- Validate the effectiveness of implemented controls and ensure they operate as intended.
- Produce configuration documentation and operational guidance for customer teams.
- Deliver structured knowledge transfer and conduct a formal handover session.

Customer Responsibilities

The customer must:

- Provide administrative access to Entra ID and relevant Microsoft 365 services.
- Make stakeholders available who can confirm identity requirements, access policies, and lifecycle processes.
- Supply accurate information relating to users, groups, roles, and identity sources.
- Ensure required licensing is active for all users in scope.
- Provide access to HR or directory systems where lifecycle automation is required.
- Maintain system stability during configuration and testing.
- Review and validate deliverables as part of the acceptance process.

Assumptions

This Service Element is delivered on the basis that:

- Identity data provided by the customer is accurate and reflects the current environment.
- Required Microsoft services are deployed and available for configuration.
- Stakeholders are available at agreed times to support design and validation.
- Only one primary tenant or domain is in scope unless explicitly defined otherwise.
- Handover to BAU does not include ongoing operational management, which is delivered through separate services.

Exclusions

This Service Element does not include:

- Continuous operational identity management or ongoing administration of identity controls.
- Incident response, investigation, or remediation of identity-related breaches.
- Development of bespoke automation beyond the JML processes included in scope.

- Configuration of third-party identity platforms unless explicitly agreed.
- Creation of organisation-wide governance frameworks, policies, or risk models.
- Broader architectural redesign outside identity and access services.
- Work on additional tenants, domains, or identity systems not included at the outset.

Success Measures

The IAM Enablement element is successfully delivered when:

- The IAM design is approved and reflects the defined requirements.
- Identity controls are configured and validated as operating correctly.
- PIM, SSO, and JML components (where in scope) are implemented and functioning as intended.
- Documentation and operational guidance are delivered and reviewed with customer stakeholders.
- Knowledge transfer and handover sessions are completed and acknowledged.
- Stakeholders confirm that access governance and authentication controls meet their operational expectations.

Service Element: Endpoint & Device Protection

Description

The Endpoint & Device Protection element establishes the controls and configuration standards required to protect desktops, laptops, mobile devices, and hybrid estate endpoints. It delivers a unified approach to device management by deploying and configuring Microsoft Intune and Microsoft Defender for Endpoint to enforce secure baselines, compliance policies, and threat protection.

The service also establishes structured patch and vulnerability governance for operating systems and applications, and applies mobile device and application management controls to ensure secure use on corporate and personal devices.

The outcome is a resilient, compliant, and centrally governed device environment that reduces device-level security exposure and supports Zero Trust principles across the organisation.

Deliverables

Deliverable	Description
Intune and Defender for Endpoint Deployment	Deployment and configuration of Microsoft Intune and Defender for Endpoint across agreed device types to establish unified device management and protection.
Compliance and Configuration Baselines	Implementation of CIS-aligned, Microsoft-recommended baselines covering device configuration, compliance checks, and minimum security standards.
Endpoint Protection Policies	Configuration of device-level threat protection policies, including antivirus, firewall, attack surface reduction, and device health monitoring.
Patch and Vulnerability Management Process	Defined and established governance process for patching, update deployment, and vulnerability treatment across supported operating systems.
Mobile Device and Application Management Controls	Configuration of MDM/MAM policies to protect mobile devices and corporate data accessed from mobile applications.
Operational Documentation Pack	Documentation covering policy configurations, device governance requirements, monitoring expectations, and operational procedures.
Handover and Readiness Validation	A structured handover confirming correct policy enforcement, telemetry health, and alignment to the defined configuration scope.
Knowledge Transfer Sessions	Walkthroughs of policies, governance tasks, and operational processes to equip customer teams to manage device protections effectively.

Dependencies

Delivery of this Service Element requires:

- Appropriate Microsoft licensing for Intune, Microsoft Defender for Endpoint, and compliance policy enforcement.
- Administrative access to Microsoft Intune, Microsoft 365 Defender, and relevant tenant resources.
- A current and accurate device inventory for all devices in scope.
- Connectivity from managed devices to required Microsoft cloud services for configuration and telemetry.
- Integration with IAM Enablement where Conditional Access relies on device compliance signals.
- Alignment with Secure Configuration and Cloud Security Management where ongoing baseline validation is required.

Constraints

This Service Element is subject to the following constraints:

- Configuration validation may be limited to representative sample devices where full-estate testing is not feasible.
- The effectiveness of compliance policies depends on device enrolment, telemetry flow, and customer-managed operating system conditions.
- Mobile device controls may be limited by device operating system capabilities or restrictions imposed by personal devices.
- Only device and endpoint controls described within the agreed scope are included; broader endpoint management or IT operations activities are not.
- Delivery is restricted to a single primary tenant unless otherwise agreed.

Benefits

This Service Element strengthens the organisation's ability to operate as a Secure Business by ensuring that devices used across the environment function within defined, reliable protection boundaries.

It improves operational resilience by establishing consistent configuration and compliance standards, reduces exposure arising from misconfigured or unprotected endpoints, and provides a stable foundation for secure hybrid and mobile working.

This helps the organisation maintain safe day-to-day operations and supports confident adoption of modern device platforms and services.

848 Responsibilities

Under this Service Element, 848 will:

- Design device protection requirements, configuration standards, and compliance expectations.
- Deploy and configure Intune and Defender for Endpoint across in-scope devices.

- Implement compliance, configuration, and threat protection baselines.
- Establish patch and vulnerability management governance processes.
- Configure MDM/MAM policies for mobile device and application protection.
- Validate configuration effectiveness across representative devices.
- Produce operational documentation and governance guidance.
- Deliver structured knowledge transfer and a formal handover session.

Customer Responsibilities

The customer must:

- Provide administrative access to relevant Microsoft 365, Intune, and Defender for Endpoint services.
- Supply an accurate device inventory and confirm devices in scope.
- Ensure devices can connect to Microsoft cloud services for policy deployment and telemetry.
- Provide stakeholder input relating to device usage, security requirements, and operational constraints.
- Ensure required licensing is active for all devices in scope.
- Review and validate deliverables as part of acceptance.
- Maintain device stability during deployment and configuration.

Assumptions

- Required Microsoft technologies are deployed and functional before configuration begins.
- Device data and inventory information provided by the customer is accurate.
- Stakeholders are available to support design, testing, and validation activities.
- The organisational scope remains stable throughout delivery.
- Ongoing operational management will be performed by the customer or through a separate managed service.

Exclusions

This Service Element does not include:

- Continuous device monitoring, management, or operational administration.
- Remediation of device vulnerabilities or patch deployment outside the defined governance process.
- Incident response, investigation, or device-level forensic analysis.

- Configuration of third-party device management or endpoint protection tools.
- Development of custom scripts, automation, or reporting solutions beyond defined scope.
- Broader IT operations services such as service desk, hardware lifecycle, or device procurement.
- Work on additional tenants, domains, or environments not included in the agreed scope.

Success Measures

This Service Element is successfully delivered when:

- Intune and Defender for Endpoint are deployed and configured as defined.
- Compliance and configuration baselines are implemented and validated.
- Patch and vulnerability governance processes are established and understood.
- MDM/MAM controls are operational across relevant devices.
- Documentation and operational guidance have been delivered and reviewed.
- Knowledge transfer and handover sessions are completed and acknowledged by customer stakeholders.

Service Element: Secure Remote Access

Description

The Secure Remote Access element establishes the controls and connectivity required for users to access organisational resources safely from remote, hybrid, and distributed environments. It delivers a structured access model using Microsoft Conditional Access, Azure VPN, and device compliance integrations to ensure that only trusted users and compliant devices can connect to corporate services.

By enforcing contextual access conditions based on identity, device health, and location, the service enables flexible working while maintaining consistent security across cloud and on-premises environments.

The outcome is a secure, reliable, and governed remote access environment that supports Zero Trust principles and reduces exposure associated with remote connectivity.

Deliverables

Deliverable	Description
Secure Remote Access Design and Configuration Plan	A validated design document defining access methods, authentication requirements, Conditional Access conditions, VPN configurations, and Zero Trust alignment.
Conditional Access Policy Deployment	Implemented Conditional Access controls that govern access based on identity, device compliance, location, and session requirements.
Azure VPN Configuration	Deployment and configuration of Azure VPN or Azure VPN Gateway to support secure remote connectivity for approved users and devices.
Compliance-Based Access Controls	Enforced access policies that restrict connectivity to compliant, trusted devices using integrated device health and compliance signals.
Operational Documentation Pack	Documentation outlining configured policies, VPN settings, governance tasks, troubleshooting steps, and operational responsibilities.
Handover and Readiness Validation	A structured handover that confirms access policy effectiveness, connectivity resilience, and readiness to transition into operational ownership.
Knowledge Transfer Sessions	Guided walkthroughs of access configurations, operational tasks, and governance expectations to enable effective oversight by customer teams.

Dependencies

Delivery of this Service Element requires:

- Active Microsoft licensing that includes Conditional Access and Azure VPN capabilities.
- Administrative access to Microsoft Entra ID, Microsoft 365, Azure networking components, and relevant infrastructure.
- Connectivity and network routing that support Azure VPN deployment and testing.

- Device compliance signals sourced from the Endpoint & Device Protection element where Conditional Access relies on device health.
- Integration with IAM Enablement for identity authentication, policy structure, and access governance.
- A single primary identity provider (Microsoft Entra ID) unless otherwise scoped.

Constraints

This Service Element is subject to the following constraints:

- Access scenarios outside the Microsoft ecosystem may require separate scoping or may not be supported.
- Conditional Access enforcement depends on accurate identity information and reliable device compliance telemetry.
- VPN performance and reliability depend on customer-managed network conditions and connectivity.
- Complex multi-tenant, multi-identity, or multi-network scenarios require explicit agreement during design.
- Only secure access methods defined within the agreed scope are included; broader network redesign or firewall changes are not.

Benefits

This Service Element strengthens the organisation's ability to operate as a Secure Business by ensuring that remote access is governed, resilient, and restricted to trusted users and devices. It reduces exposure associated with distributed working by applying consistent access conditions and enforcing control over how and from where resources are accessed. This supports flexible working without compromising security, contributes to stable day-to-day operations, and provides a dependable foundation for secure modern working practices.

848 Responsibilities

Under this Service Element, 848 will:

- Design the secure remote access model aligned to organisational needs and Zero Trust principles.
- Configure Conditional Access policies, Azure VPN, and compliance-based access controls.
- Validate access scenarios, connectivity, and policy effectiveness across representative user groups.
- Document all configurations, governance expectations, and operational requirements.
- Deliver structured knowledge transfer sessions to customer teams.
- Conduct a formal handover and confirm readiness for operational management.

Customer Responsibilities

The customer must:

- Provide administrative access to required Microsoft 365, Entra ID, and Azure components.
- Supply accurate information relating to access requirements, user groups, and network architecture.
- Ensure that devices used for remote access meet compliance requirements and can connect to Microsoft cloud services.
- Provide relevant network configuration inputs and ensure routing supports VPN deployment.
- Maintain required licensing for all users in scope.
- Make stakeholders available to support design, testing, and validation.
- Review and accept deliverables as part of handover.

Assumptions

This Service Element is delivered on the basis that:

- Required Microsoft services and Azure networking capabilities are deployed and available.
- Identity governance structures are in place through IAM Enablement.
- Device compliance signals are available through the Endpoint & Device Protection element.
- Stakeholders are available for design workshops, validation, and acceptance stages.
- The environment remains stable throughout delivery.
- Ongoing remote access management will be performed by the customer or through a separate managed service.

Exclusions

This Service Element does not include:

- Continuous monitoring or management of remote access controls.
- Incident response, investigation, or remediation of access-related security issues.
- Configuration of third-party VPN clients, gateways, or non-Microsoft access solutions.
- Broader network infrastructure redesign or firewall rule development.
- Custom automation or integrations outside Microsoft technologies.
- Multi-tenant or multi-identity provider deployments beyond the agreed scope.

Success Measures

This Service Element is successfully delivered when:

- The secure remote access design is validated and approved.
- Conditional Access policies and Azure VPN configurations are implemented and tested.
- Compliance-based access controls operate as intended across representative users and devices.
- Documentation and operational guidance have been delivered and reviewed.
- Knowledge transfer and handover sessions have been completed.
- Stakeholders confirm the remote access model meets their operational and security expectations.

Service Element: Email & Collaboration Security

Description

The Email & Collaboration Security element establishes the protections required to secure email, messaging, and collaborative workloads across Microsoft 365. It delivers a structured configuration of Microsoft Defender for Office 365 and related collaboration safeguards to protect users against phishing, malicious links, harmful attachments, impersonation attempts, and unsafe sharing practices.

The service applies policies and controls across Exchange Online, Teams, SharePoint, and OneDrive to ensure that communication and collaboration take place within governed, secure, and predictable boundaries. It provides visibility into message hygiene, threat activity, and collaboration risk so the organisation can support modern working without increasing exposure.

The outcome is a safer, more resilient communication and collaboration environment that operates in line with Secure Business principles.

Deliverables

Deliverable	Description
Defender for Office 365 Configuration Plan	A validated design document defining email and collaboration protection requirements, policy scope, and Zero Trust alignment for Microsoft 365 workloads.
Anti-Phishing and Anti-Spam Protections	Configuration of policies that detect and prevent phishing attempts, impersonation risks, spam, and malicious email behaviours.
Safe Links Policy Configuration	Implemented Safe Links protections that scan and validate URLs to prevent malicious link access across email, Teams, and other supported workloads.
Safe Attachments Policy Configuration	Configured Safe Attachments policies that analyse and detonate suspicious files to prevent harmful content reaching users.
Collaboration Platform Security Controls	Security configurations applied across Teams, SharePoint, and OneDrive to govern sharing, restrict risky behaviours, and protect organisational data.
Operational Documentation Pack	Documentation covering policy configurations, collaboration safeguards, governance tasks, monitoring expectations, and operational procedures.
Handover and Readiness Validation	A structured handover confirming policy effectiveness, threat protection coverage, and readiness for operational ownership.
Knowledge Transfer Sessions	Guided walkthroughs of policy sets, operational governance, monitoring tasks, and configuration decisions for customer administrators.

Dependencies

Delivery of this Service Element requires:

- Active Microsoft licensing supporting Defender for Office 365 protections.
- Administrative access to Microsoft 365 security and compliance portals.
- Access to mail flow configurations, accepted domains, and any relevant routing details.
- Integration with Information Protection & Governance where DLP or sensitivity labelling interacts with collaboration policies.
- Alignment with IAM Enablement for identity-based protection logic (e.g., spoofing protections, authentication context).
- Connectivity and access for Teams, SharePoint, and OneDrive to apply collaboration policies.

Constraints

This Service Element is subject to the following constraints:

- Protections apply only to workloads within Microsoft 365; third-party mail gateways, archives, or security tools are excluded unless explicitly scoped.
- The effectiveness of phishing and impersonation protection depends on accurate identity information and reliable mail flow configuration.
- Advanced policy features may require additional licensing.
- Multi-tenant or cross-domain configurations require explicit agreement during design.
- Only collaboration security settings defined in scope are included; broader information governance or compliance programmes are not.

Benefits

This Service Element strengthens the organisation's ability to operate as a Secure Business by safeguarding communication and collaboration channels against threats that commonly disrupt operations or compromise sensitive information. It reduces exposure to phishing, malicious content, and unsafe sharing, and ensures that users can work confidently across email, Teams, SharePoint, and OneDrive within clear protective boundaries. This contributes to stable operations, safer information handling, and a more resilient modern workplace.

848 Responsibilities

Under this Service Element, 848 will:

- Design the email and collaboration protection model based on organisational requirements.
- Configure Defender for Office 365 policies, including anti-phishing, Safe Links, Safe Attachments, and anti-spam protections.

- Apply collaboration security controls across Teams, SharePoint, and OneDrive.
- Validate protection effectiveness through sample testing and policy review.
- Produce operational documentation and policy reference material.
- Deliver structured knowledge transfer and conduct a formal handover session.

Customer Responsibilities

The customer must:

- Provide administrative access to Microsoft 365 Defender and collaboration platforms.
- Supply accurate mail flow information, accepted domains, and routing details.
- Make security, IT, and collaboration stakeholders available for design and validation.
- Ensure required licensing is active for all users in scope.
- Review policies and configurations as part of acceptance.
- Maintain stable mail flow and collaboration platform environments during delivery.

Assumptions

This Service Element assumes:

- Microsoft 365 workloads (Exchange Online, Teams, SharePoint, OneDrive) are deployed and operational.
- Identity structures and authentication controls are established through IAM Enablement.
- Information Protection & Governance is available where data handling policies interact with collaboration safeguards.
- Stakeholders are available for workshops, reviews, and acceptance processes.
- The organisational scope remains consistent throughout delivery.

Exclusions

This Service Element does not include:

- Ongoing monitoring or administration of mail or collaboration security policies.
- Investigation of phishing incidents, compromised accounts, or other security events.
- Configuration of third-party mail gateways, routing platforms, or security tools.
- End-user training outside defined knowledge transfer sessions.
- Broader compliance or governance frameworks beyond collaboration safeguards.
- Multi-tenant orchestration unless explicitly defined.
- Custom scripting, automation, or reporting beyond agreed scope.

Success Measures

This Service Element is successfully delivered when:

- The Defender for Office 365 configuration plan is validated and approved.
- Policies for anti-phishing, Safe Links, Safe Attachments, and collaboration safeguards are configured and functioning as intended.
- Collaboration platforms enforce security controls aligned with organisational requirements.
- Documentation and operational guidance are delivered and reviewed.
- Knowledge transfer and handover sessions are completed.
- Stakeholders confirm that email and collaboration protections meet their operational expectations.

Service Element: Information Protection & Governance

Description

The Information Protection & Governance element establishes the controls required to manage sensitive information responsibly throughout its lifecycle. It delivers a structured implementation of Microsoft Purview and related Microsoft 365 capabilities, combining data loss prevention (DLP), sensitivity labelling, encryption, retention, and deletion policies into a coherent protection model.

The service ensures that data is governed consistently across email, collaboration platforms, and storage locations so that information is protected when in use, in motion, and at rest. This enables the organisation to handle sensitive information safely, meet regulatory expectations, and embed reliable data governance into daily operations.

The outcome is a clearly defined, well-governed data environment that reduces information-handling risk and supports secure, compliant business operations.

Deliverables

Deliverable	Description
Information Classification and Sensitivity Label Model	A defined classification structure and label set tailored to the organisation's data types, handling needs, and governance priorities.
Configured Sensitivity Labels and Label Policies	Implemented sensitivity labels, protection settings, and labelling policies that govern how data is accessed, shared, and stored across Microsoft 365.
Data Loss Prevention Policies	DLP policies configured for Exchange, SharePoint, OneDrive, and Teams to detect, prevent, and govern risky or non-compliant data activity.
Encryption and Protection Rules	Applied encryption, access restrictions, and content protection rules aligned to organisational needs and label definitions.
Retention and Lifecycle Policies	Implemented retention, deletion, and lifecycle rules that ensure information is held and disposed of in accordance with organisational and regulatory requirements.
Purview Dashboards and Monitoring Views	Configured visibility dashboards for reviewing data movement, policy matches, governance, and compliance behaviours.
Operational Documentation Pack	Documentation covering classification models, policy configurations, governance expectations, and operational tasks required for effective data protection.

Handover and Readiness Validation	A structured handover confirming policy function, governance alignment, and readiness for operational ownership.
Knowledge Transfer Sessions	Walkthroughs of classification, labelling, DLP, and retention logic to equip customer teams to maintain data governance confidently.

Dependencies

Delivery of this Service Element requires:

- Appropriate Microsoft Purview and Microsoft 365 licensing that supports information protection, DLP, and retention capabilities.
- Administrative access to Microsoft Purview, Microsoft 365 compliance portals, and relevant data sources.
- A clear and accurate inventory of data sources (e.g., Exchange, SharePoint, OneDrive, Teams).
- Approved classification taxonomy and data-handling principles during the design phase.
- Integration with Email & Collaboration Security where labelling or DLP intersects with communication policies.
- Alignment with IAM Enablement and Endpoint & Device Protection where protection depends on authentication context or device compliance.

Constraints

This Service Element is subject to the following constraints:

- Policy effectiveness depends on accurate classification decisions and the availability of data inventory information.
- Retention and deletion rules must align to legal and regulatory requirements provided by the customer.
- Complex or multi-entity environments may require extended design activity and additional scoping.
- Configuration applies only to Microsoft 365 data sources included in scope; third-party repositories are excluded unless explicitly agreed.
- Automated lifecycle rules may be limited by the customer's existing information architecture or data quality.

Benefits

This Service Element supports the organisation's ability to operate as a Secure Business by establishing clear and consistent controls over how sensitive information is handled, stored, and shared.

It reduces the likelihood of data loss or unauthorised disclosure, strengthens compliance readiness, and ensures that information is governed responsibly throughout its lifecycle. This contributes to more predictable operations, safer collaboration, and greater confidence in the organisation's ability to meet regulatory and business obligations.

848 Responsibilities

Under this Service Element, 848 will:

- Design the information classification model, governance approach, and policy structure.
- Configure sensitivity labels, label policies, DLP rules, encryption settings, and retention policies.
- Establish access restrictions and governance conditions aligned to classification outcomes.
- Configure Purview dashboards and monitoring capabilities.
- Validate policy behaviour and ensure controls function as intended.
- Produce operational documentation and governance guidance.
- Deliver structured knowledge transfer and conduct a formal handover session.

Customer Responsibilities

The customer must:

- Provide administrative access to Microsoft Purview and relevant Microsoft 365 services.
- Supply accurate information about data sources, handling requirements, and regulatory obligations.
- Approve the classification taxonomy and label structure during design.
- Ensure required licensing is active for all users in scope.
- Make data governance, compliance, and IT stakeholders available for workshops and validation.
- Review and validate deliverables as part of the acceptance process.
- Maintain stable data environments during configuration and testing.

Assumptions

This Service Element assumes:

- Required Microsoft 365 and Purview services are deployed and accessible.
- Stakeholders with data governance and compliance responsibility are available for design and review.
- Information provided by the customer is accurate and represents current data usage.
- The organisational scope remains consistent throughout delivery.

- Ongoing governance or enforcement activity will be delivered by the customer or through a separate managed service.

Exclusions

This Service Element does not include:

- Ongoing monitoring or management of DLP, labelling, or retention controls.
- Investigation of data loss incidents or breaches.
- Configuration of third-party DLP or information protection platforms.
- End-to-end compliance, policy authoring, or regulatory framework development.
- Custom automation or integration beyond Microsoft Purview capabilities.
- Broader enterprise information governance programmes or data governance operating models.
- Work on additional tenants, entities, or regulatory scopes not included at the outset.

Success Measures

This Service Element is successfully delivered when:

- The classification and sensitivity label model is approved and applied.
- DLP, encryption, and retention policies are configured and validated.
- Purview dashboards and monitoring views are operational.
- Documentation and governance guidance have been delivered and reviewed.
- Knowledge transfer and handover sessions are completed.
- Stakeholders confirm that information protection and governance controls meet organisational and regulatory expectations.

Service Element: Application & Cloud Access Security (CASB)

Description

The Application & Cloud Access Security element establishes the visibility and control required to govern how cloud applications are accessed and used across the organisation. It delivers a structured deployment of Microsoft Defender for Cloud Apps to identify sanctioned and unsanctioned cloud services, enforce access and session policies, and apply data protection controls that prevent unauthorised sharing or exfiltration.

The service integrates signals from SaaS, IaaS, and PaaS environments to provide a single, coherent view of cloud activity and risk. Through continuous monitoring, policy enforcement, and automated response actions, it strengthens cloud security and ensures that cloud usage aligns with organisational expectations and governance requirements.

The outcome is a safer, more controlled cloud application environment that reduces operational risk and supports the organisation's ability to work flexibly without compromising security.

Deliverables

Deliverable	Description
Cloud Application Security Design and Configuration Plan	A validated design defining cloud application governance objectives, policy scope, access controls, and integration requirements across SaaS, IaaS, and PaaS services.
Connected Cloud Applications	Configuration of API and connector integrations to onboard sanctioned and monitored applications and enable visibility across cloud services.
Discovery and Visibility Enablement	Activated discovery capabilities that identify unsanctioned or unmanaged applications, including normalised reporting on usage patterns and associated risks.
Access and Session Control Policies	Implemented Conditional Access and session control rules that enforce safe access, govern risky activity, and prevent unauthorised data movement.
Data Protection and Compliance Policies	Custom policies for data governance, including rules that identify risky behaviours, enforce organisational standards, and restrict high-risk actions.
Monitoring Dashboards and Alerts	Configured dashboards, analytics, and alerting views that provide visibility into cloud usage, risk exposure, and policy impact.
Operational Documentation Pack	Documentation covering application integrations, policy sets, governance tasks, monitoring procedures, and operational responsibilities.

Handover and Readiness Validation	A structured handover confirming that cloud visibility, policy coverage, and controls operate as intended.
Knowledge Transfer Sessions	Guided walkthroughs of policies, dashboards, and operational tasks to enable customer teams to manage cloud access and governance effectively.

Dependencies

Delivery of this Service Element requires:

- Appropriate Microsoft licensing supporting Defender for Cloud Apps.
- Administrative access to Microsoft 365, Azure AD, and application APIs required for integration.
- A validated list of applications to be monitored or onboarded.
- Identity architecture and Conditional Access policies established through IAM enablement.
- Integration with Information Protection & Governance where DLP or labelling policies apply to cloud activity.
- Device compliance telemetry from Endpoint & Device Protection where applicable.

Constraints

This Service Element is subject to the following constraints:

- Cloud visibility is dependent on the availability and accuracy of discovery data and application API integrations.
- Some cloud applications may have limited or restricted API support, affecting depth of control.
- Advanced automation or remediation workflows may require additional scoping.
- Multi-tenant or multi-cloud environments may require extended design activity.
- Only Microsoft Defender for Cloud Apps is configured; third-party CASB tools are excluded unless explicitly scoped.

Benefits

This Service Element supports the organisation's ability to operate as a Secure Business by providing clear oversight and control of cloud application usage.

It reduces exposure arising from unmanaged, unsanctioned, or high-risk cloud behaviours and ensures that cloud access is governed in a consistent and predictable way.

This strengthens operational resilience, improves accountability for cloud usage, and enables the organisation to adopt SaaS and cloud services safely and with confidence.

848 Responsibilities

Under this Service Element, 848 will:

- Design the cloud application governance model and policy structure.
- Configure Defender for Cloud Apps connectors, discovery capabilities, and monitoring features.
- Implement access, session, and data protection policies aligned to organisational requirements.
- Establish dashboards and alerting to support operational oversight.
- Validate policy behaviour and confirm visibility across in-scope applications.
- Provide operational documentation and governance guidance.
- Deliver structured knowledge transfer and conduct a formal handover session.

Customer Responsibilities

The customer must:

- Provide administrative access to Microsoft 365, Entra ID, and relevant cloud applications.
- Supply accurate information about sanctioned applications, user groups, and cloud usage patterns.
- Ensure required licensing is active across all users in scope.
- Make stakeholders available for design workshops, testing, and acceptance.
- Provide API permissions and approvals needed to integrate cloud services.
- Review and validate deliverables as part of the acceptance process.

Assumptions

This Service Element assumes:

- Microsoft Defender for Cloud Apps is available and licenced for the environment.
- Application API access and permissions required for integration are available.
- Stakeholders with responsibility for cloud governance and IT operations are available.
- Information supplied by the customer reflects current cloud usage.
- The defined scope remains stable throughout the engagement.
- Ongoing cloud governance is delivered by the customer or through a separate managed service.

Exclusions

This Service Element does not include:

- Continuous monitoring or ongoing administration of cloud access policies.
- Incident response, investigation, or forensic analysis of cloud security events.
- Configuration of third-party CASB tools or non-Microsoft cloud security platforms.
- Development of custom integrations or automation outside core Defender for Cloud Apps capabilities.
- Broader cloud architecture redesign or IaaS/PaaS hardening not defined in the scope.
- Multi-tenant or multi-entity deployments beyond the agreed engagement.

Success Measures

This Service Element is successfully delivered when:

- Cloud application integrations are configured and operational.
- Discovery and visibility functions provide accurate insight into cloud usage.
- Access, session, and data protection policies operate as intended.
- Monitoring dashboards and alert views are functioning and reviewed with stakeholders.
- Documentation and governance guidance have been delivered.
- Knowledge transfer and handover sessions are completed.
- Stakeholders confirm that cloud access governance meets operational and security expectations.

Service Element: Zero Trust Architecture Design

Description

The Zero Trust Architecture Design element defines and implements the controls required to establish a unified, adaptive security model across identity, endpoints, networks, applications, infrastructure, and data. The service applies the core Zero Trust principles of verify explicitly, use least privilege access, and assume breach to design the organisation's trust boundaries and control model.

It translates policy, operational context, and risk insights into technical design and configuration guidance that aligns Microsoft 365, Azure, and relevant third-party systems into a coherent architecture.

The outcome is a well-defined Zero Trust framework that strengthens organisational security, improves control consistency, and enables predictable, secure operation across the enterprise ecosystem.

Deliverables

Deliverable	Description
Zero Trust Reference Architecture	A documented reference architecture defining the target Zero Trust model across identity, devices, applications, networks, infrastructure, and data.
Zero Trust Design Principles and Control Model	A structured set of design principles, control expectations, and trust boundary definitions tailored to the organisation's environment and business requirements.
Control Mapping Across Zero Trust Pillars	Documentation mapping required controls to the Zero Trust pillars, showing how identity, device, application, network, data, and governance controls will be applied.
Validated Proof-of-Concept Configurations	Configured and tested PoCs demonstrating application of Zero Trust controls across Microsoft 365, Azure, and selected third-party technologies.
Zero Trust Maturity Assessment	A high-level assessment of the organisation's current Zero Trust maturity and readiness, identifying capability gaps and priority areas.
Zero Trust Improvement Roadmap	A prioritised roadmap detailing recommended actions, dependencies, and expected outcomes required to progress toward the target Zero Trust state.
Operational Documentation Pack	Documentation covering architectural decisions, control integrations, governance considerations, and operational expectations.
Handover and Readiness Validation	A structured review confirming understanding of the Zero Trust design, control model, and roadmap, and readiness to progress to implementation.

Knowledge Transfer Sessions	Workshops with architecture, security, and IT stakeholders explaining the design approach, control mapping, and Zero Trust operating considerations.

Dependencies

Delivery of this Service Element requires:

- Existing Microsoft 365 and Azure environments with appropriate capabilities available for Zero Trust control integration.
- Administrative access to relevant Microsoft services and any agreed third-party systems (e.g., firewalls, identity providers, security tools).
- Availability of architecture, security, and IT stakeholders to participate in design workshops and validation sessions.
- Inputs from IAM Enablement, Endpoint & Device Protection, Information Protection & Governance, and Secure Configuration & Cloud Security Management to ensure architectural alignment.
- If third-party systems are included, required documentation and access must be available for integration design.

Constraints

This Service Element is subject to the following constraints:

- Implementation is limited to design and pilot or proof-of-concept configurations unless otherwise scoped.
- Integration capabilities may vary depending on the features of third-party systems or existing technical constraints.
- Zero Trust adoption across all pillars may require phased implementation based on organisational readiness.
- Multi-tenant or multi-entity environments may require additional design effort and must be defined at the outset.
- This Service Element does not replace full enterprise architecture or IT operating model design.

Benefits

This Service Element supports the organisation's ability to operate as a Secure Business by establishing a coherent and consistent security model that reduces reliance on perimeter-based controls and strengthens defence across all layers of the environment.

It helps the organisation apply safeguards in a predictable and coordinated manner, improves resilience against modern threats, and ensures that access, data handling, and platform behaviour operate within clearly defined trust boundaries.

This creates a strong foundation for secure digital transformation and enables the organisation to adopt new technologies with confidence.

848 Responsibilities

Under this Service Element, 848 will:

- Conduct discovery workshops to understand the current environment, controls, risks, and constraints.
- Define the Zero Trust architecture, including principles, trust boundaries, and target-state design.
- Map required controls across the Zero Trust pillars and align them with the organisation's operating context.
- Configure and validate proof-of-concept integrations across Microsoft 365, Azure, and agreed third-party systems.
- Assess Zero Trust maturity and identify capability gaps.
- Produce the Zero Trust roadmap and operational documentation.
- Deliver knowledge transfer and a structured handover session.
- Provide design-level guidance on future implementation phas

Customer Responsibilities

The customer must:

- Provide administrative access to relevant Microsoft and third-party systems required for assessment and PoC configuration.
- Make key architecture, security, and IT stakeholders available for workshops and design validation.
- Supply accurate information on current network, identity, data, and platform architectures.
- Ensure required Microsoft licensing is active and available for all in-scope services.
- Approve design decisions, control models, and the Zero Trust roadmap.
- Maintain environment stability during assessment and PoC work.
- Review all deliverables and participate in handover sessions.

Assumptions

This Service Element assumes:

- Microsoft 365 and Azure environments are already deployed and accessible.
- Stakeholders responsible for architecture, governance, and operations will provide timely input.

- Existing controls and configuration documentation are available for review.
- Scope remains consistent throughout engagement.
- Any ongoing implementation or operationalisation beyond PoC is delivered separately.

Exclusions

This Service Element does not include:

- Full-scale implementation of Zero Trust controls beyond PoC configuration.
- Continuous monitoring, management, or enforcement of Zero Trust controls.
- Incident response or remediation of architectural issues.
- Development of enterprise-wide governance frameworks or operating models outside Zero Trust context.
- Configuration of third-party security platforms beyond what is explicitly scoped.
- Integration with SIEM, SASE, or firewall platforms unless included during design.
- Redesign of broader network or infrastructure architecture outside Zero Trust requirements.

Success Measures

This Service Element is successfully delivered when:

- The Zero Trust reference architecture is completed, validated, and approved.
- Control mappings across Zero Trust pillars are documented and understood.
- PoC configurations demonstrate expected Zero Trust behaviour and integration.
- A maturity assessment and prioritised improvement roadmap are delivered.
- Documentation and architectural guidance are reviewed with stakeholders.
- Knowledge transfer and handover sessions are completed.
- Stakeholders confirm that the Zero Trust model aligns with organisational needs and is ready for further implementation.

Service Element: Secure Configuration & Cloud Security Management

Description

The Secure Configuration & Cloud Security Management element establishes and validates the configuration baselines required to maintain secure, resilient Microsoft 365, Windows, and Azure environments. It delivers a structured design and implementation of secure configuration standards aligned to recognised frameworks such as CIS, NCSC, and Microsoft Defender for Cloud benchmarks.

The service applies Cloud Security Management (CSM) capabilities to monitor configuration drift, assess compliance, and support remediation activities across cloud and hybrid infrastructure. This ensures that platforms operate within defined security parameters and remain aligned with organisational governance requirements.

The outcome is a consistently hardened environment that maintains strong security, reduces configuration-related risk, and supports safe and predictable business operations.

Deliverables

Deliverable	Description
Secure Configuration Baseline Documentation	A defined set of configuration standards aligned to CIS, NCSC, and Microsoft recommendations covering Microsoft 365, Windows, and Azure environments.
Baseline Configuration and Remediation Activities	Assessment and implementation of baseline settings across in-scope environments, including remediation of deviations to establish a consistent security foundation.
Microsoft Defender for Cloud Configuration	Configuration of Microsoft Defender for Cloud policies, compliance assessments, recommendations, and security controls.
Security Monitoring and Alerting Setup	Configuration of security dashboards, alerts, and compliance views to support ongoing monitoring of configuration drift and control application.
Final Compliance and Security Report	A summarised report detailing baseline alignment, identified gaps, remediation actions taken, and residual risks requiring future attention.
Operational Documentation Pack	Documentation covering configuration standards, monitoring steps, alert handling, and governance tasks required for ongoing security maintenance.

Handover and Readiness Validation	A structured handover confirming configuration status, baseline coverage, and readiness for operational governance.
Knowledge Transfer Sessions	Walkthroughs of baselines, security dashboards, and operational responsibilities to enable effective management by customer teams.

Dependencies

Delivery of this Service Element requires:

- Active Microsoft licensing supporting Microsoft Defender for Cloud and relevant compliance features.
- Administrative access to Microsoft 365, Azure, and any systems required for configuration assessment.
- Visibility of in-scope Azure subscriptions, resource groups, and Microsoft 365 workloads.
- Existing baseline configuration or architecture documentation where available.
- Inputs from Identify services (Security Assessment, GRC Alignment) for risk prioritisation and compliance mapping.
- Integration with Zero Trust Architecture Design where alignment of baselines and trust boundaries is required.

Constraints

This Service Element is subject to the following constraints:

- Configuration coverage is limited to the environments, subscriptions, and workloads included in the agreed scope.
- Effectiveness of security monitoring depends on the accuracy and completeness of telemetry and configuration data.
- Advanced automation or remediation workflows may require additional scoping.
- Multi-tenant or large multi-subscription environments may require extended configuration cycles.
- Mapping to specific regulatory frameworks depends on customer-provided requirements and legal guidance.

Benefits

This Service Element supports the organisation's ability to operate as a Secure Business by ensuring that platforms remain consistently hardened and aligned with recognised security standards.

It reduces exposure caused by configuration drift, strengthens compliance readiness, and provides clear insight into secure configuration across cloud and hybrid environments.

This contributes to more predictable operations, improved governance, and a resilient foundation for secure growth and transformation.

848 Responsibilities

Under this Service Element, 848 will:

- Define secure configuration baselines aligned to applicable frameworks.
- Assess current security configuration and identify deviations requiring remediation.
- Implement and validate baseline configurations across in-scope environments.
- Configure Microsoft Defender for Cloud to support security monitoring and compliance assessment.
- Produce security reports, configuration documentation, and operational guidance.
- Deliver structured knowledge transfer and complete a formal handover session.
- Provide recommendations for ongoing security maintenance and improvement.

Customer Responsibilities

The customer must:

- Provide administrative access to Microsoft 365, Azure, and any in-scope platforms.
- Supply accurate information for all subscriptions, resource groups, and workloads included in the engagement.
- Ensure required licensing is active for in-scope services.
- Make relevant stakeholders available for design, validation, and acceptance sessions.
- Approve baseline standards and remediation priorities.
- Maintain environment stability during configuration and validation activities.
- Review and validate all deliverables as part of the acceptance process.

Assumptions

This Service Element assumes:

- Microsoft 365 and Azure environments are deployed and accessible.
- Compliance priorities and regulatory requirements are defined by the customer.
- Stakeholders responsible for platform governance and cloud operations are available.
- Scope remains stable throughout the engagement.
- Ongoing monitoring, remediation, or operational security management will be delivered separately.

Exclusions

This Service Element does not include:

- Continuous monitoring or operational administration of Microsoft Defender for Cloud.
- Remediation of issues outside secure baseline scope (e.g., workload redesign, network restructuring).
- Incident response, forensics, or threat investigations.
- Configuration or hardening of third-party cloud platforms unless explicitly scoped.
- Development of custom automation, scripts, or integrations beyond defined requirements.
- Full compliance certification, audit preparation, or regulatory submissions.
- Work on additional tenants, subscriptions, or environments not included at the outset.

Success Measures

This Service Element is successfully delivered when:

- Secure configuration baselines are defined and approved.
- Baseline configuration is implemented and validated across in-scope environments.
- Security monitoring dashboards and alerts are configured and operational.
- A final compliance and security report is delivered and reviewed.
- Documentation and governance guidance have been provided.
- Knowledge transfer and handover sessions are completed.
- Stakeholders confirm that configuration and security controls meet organisational expectations.

Service Element: Phishing Simulation & User Awareness Campaigns

Description

The Phishing Simulation & User Awareness Campaigns element establishes the behavioural safeguards required to reduce user-driven security risk. It delivers the configuration and execution of simulated phishing campaigns and targeted awareness activities using approved training platforms. The service measures user susceptibility to phishing and social engineering, identifies behavioural patterns, and provides structured reinforcement to help users recognise and avoid common attack techniques.

By combining campaign execution with awareness briefings, insights, and recommendations, the service supports the development of a security-conscious culture and strengthens the organisation's ability to prevent user-initiated compromise.

The outcome is improved security awareness, supported by measurable behavioural insight and consistent reinforcement over time.

Deliverables

Deliverable	Description
Phishing Platform Configuration	Configuration of the agreed training and phishing simulation platform, including tenant setup, user onboarding, and routing checks.
Campaign Design and Scheduling	Definition of campaign themes, targeting approach, scheduling, and delivery structure aligned to organisational needs.
Phishing Simulation Execution	Delivery of one or more phishing simulations across the defined user population, including staged or segmented deployment as required.
Awareness Briefing Sessions	Pre-campaign or post-campaign briefings to explain objectives, expected behaviours, and organisational security expectations.
Campaign Metrics and Dashboard	Access to a metrics dashboard showing user actions, click rates, reporting rates, and indicators of behavioural susceptibility.
Results and Behavioural Insights Report	A summarised report providing behavioural trends, observations, and recommendations for ongoing awareness reinforcement.
Operational Documentation Pack	Documentation covering campaign structure, user groups, frequency expectations, and recommended next steps.
Handover and Knowledge Transfer	A structured debrief and knowledge transfer session enabling customer teams to run future campaigns independently if required.

Dependencies

Delivery of this Service Element requires:

- An active licence for the selected phishing and awareness platform.
- User directory information and permissions necessary for campaign setup.
- Coordination with the organisation's communications or HR teams for scheduling.
- Integration with Email & Collaboration Security where routing or Safe Links policies may affect delivery.
- Access to relevant stakeholders to validate user groups and campaign scope.

Constraints

This Service Element is subject to the following constraints:

- Campaign delivery depends on platform capability and mail flow configuration.
- Multi-language content or multi-region scheduling requires additional scoping.
- Behavioural insights and trend analysis depend on the availability of historic data.
- Only campaigns and awareness activities defined at project outset are included.
- Follow-up or recurring campaigns fall outside this engagement unless explicitly scoped.

Benefits

This Service Element supports the organisation's ability to operate as a Secure Business by improving user awareness and strengthening the organisation's resilience to social engineering.

It provides insight into behavioural risk, reinforces responsible security practices, and reduces the likelihood of successful phishing attacks by ensuring users better understand how to identify and report suspicious activity.

This helps the organisation maintain safer day-to-day operations and strengthens overall security through informed, engaged, and accountable users.

848 Responsibilities

Under this Service Element, 848 will:

- Configure the phishing simulation and awareness platform.
- Design and schedule campaigns aligned to organisational context and user groups.
- Deliver phishing simulations and awareness briefings.
- Provide metrics, behavioural insights, and recommendations.
- Produce documentation and operational guidance.
- Deliver a structured handover and knowledge transfer session.
- Support campaign delivery through agreed communication and coordination processes.

Customer Responsibilities

The customer must:

- Provide user information and ensure permissions required for campaign setup are available.
- Confirm campaign timing, audience, and any internal communication requirements.
- Notify users of high-level awareness expectations, where required by policy.
- Provide access to relevant HR or communications representatives for coordination.
- Maintain stable mail flow and ensure organisational routing does not block campaign messages.
- Review and validate campaign outputs and recommendations during handover.

Assumptions

This Service Element assumes:

- The chosen phishing and awareness platform is licenced and accessible.
- User data is accurate and up to date.
- Stakeholders are available for design, briefing, and review sessions.
- Campaign scope and user population remain stable throughout the engagement.
- Ongoing campaign cycles beyond this engagement will be managed by the customer or through separate services.

Exclusions

This Service Element does not include:

- Development of custom phishing templates beyond those available within the platform.
- End-to-end organisational training programmes or broader security culture initiatives.
- Continuous behavioural monitoring or long-term KPI tracking.
- Remediation of user or process issues identified during campaigns.
- Investigation of security incidents triggered by real phishing threats.
- Custom content creation unless explicitly scoped.

Success Measures

This Service Element is successfully delivered when:

- The platform is configured and validated for campaign delivery.
- A phishing simulation is executed as per the agreed scope.
- Awareness briefings and supporting materials are delivered.

- Metrics and behavioural insights are produced and reviewed with stakeholders.
- Documentation and handover materials are provided.
- Knowledge transfer is completed, enabling customer teams to operate future campaigns.
- Stakeholders confirm the service improved visibility of user behaviours and awareness needs.