848

Respond

Service Definition

Secure Business

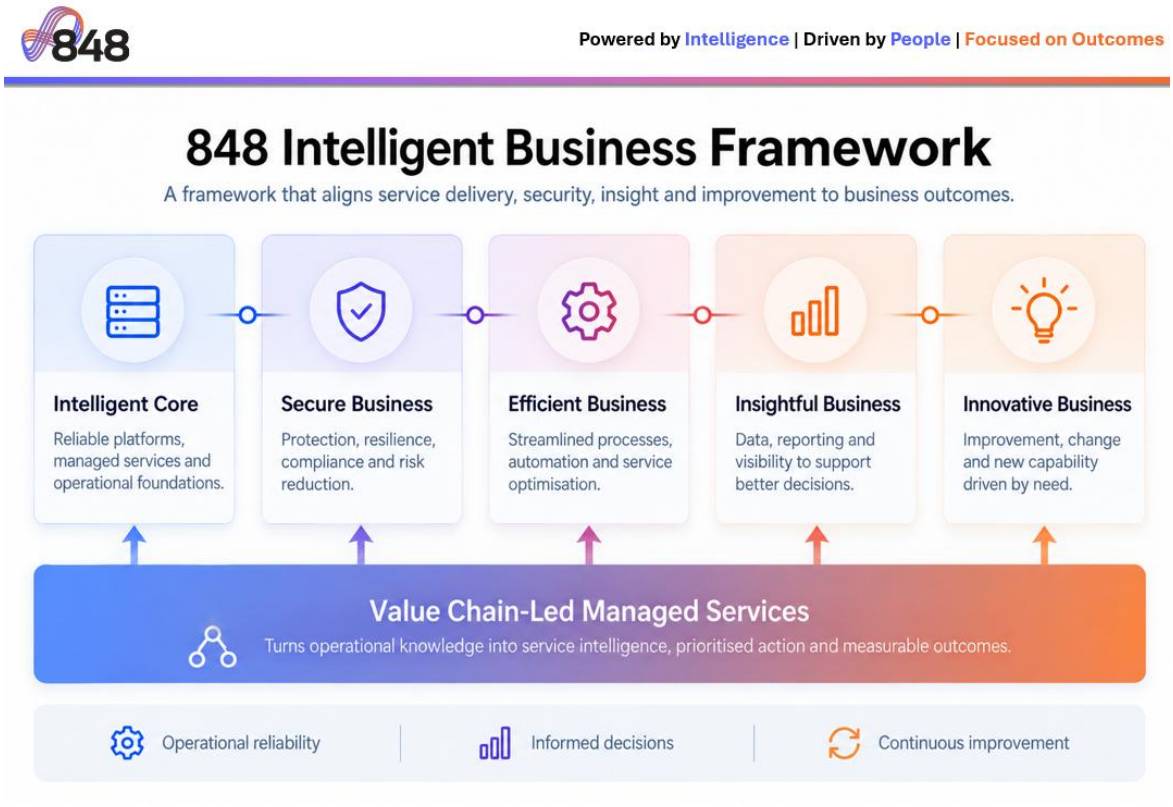
Version 0.6 | September 2026

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

1. Service Overview

A security incident puts pressure on people as much as technology. Decisions about containment, communications and service restoration become harder when responsibilities or response authority are unclear. Respond helps an organisation prepare for incidents and commission the operational response capability appropriate to its needs.

Respond sits within The Secure Business, part of 848's Intelligent Business Framework. The framework connects technology investment to the way the organisation operates, makes decisions and delivers services. Each engagement addresses the selected outcome while considering its place in the wider customer environment.



From business need to usable capability

Readiness work makes the response process usable before an event occurs. Selected automation or managed response can then support action when a threat is detected. Investigation and lessons learned turn an incident record into a practical improvement plan, so the experience strengthens future readiness.

Detect provides the signals that trigger response, while Protect reduces exposure through preventive safeguards. Recover addresses continuity and recovery readiness. Respond connects those capabilities through incident decisions and authorised actions, keeping the effect on business services visible throughout the event.

2. Scope and Service Boundaries

Customers select the elements that support their intended outcome. The scope identifies what 848 will deliver and the work retained by customer teams or suppliers.

Service	Outcome
Preparedness assessment	Existing policies and response practices are reviewed to identify gaps in readiness. The customer receives a baseline and prioritised recommendations; writing new plans or handling a live incident is separate.
Response plans and playbooks	An incident response plan and selected scenario playbooks define severity, responsibilities and communication routes. The work establishes usable response guidance, with live response separately commissioned.
Automation and orchestration	Sentinel, Logic Apps and Defender XDR support selected response workflows. Agreed approval steps and safe-use boundaries govern actions; custom connectors and ongoing maintenance require separate scope.
Managed detection and response	The selected MDR service combines monitoring and investigation with authorised initial containment and eradication actions in the supported Microsoft environment. Wider remediation, long-term forensics and disaster recovery execution are separate.
Investigation and lessons learned	Available telemetry and stakeholder evidence establish the incident timeline, cause and impact. A review workshop develops corrective actions; forensic imaging and evidential investigation are outside this element.

Dependencies and exclusions

An assessment or playbook engagement does not include live incident handling. MDR activity is limited to the agreed environment and authorised actions. Forensic acquisition, legal representation and business continuity execution need separate arrangements. Initial containment and wider remediation have distinct responsibilities, which must be clear before operational response starts.

3. How 848 Delivers the Service

Delivery follows the selected scope, using the customer's operating context to guide the work. The sequence below explains how evidence and decisions progress towards the agreed outputs. Customer review and knowledge transfer form part of that progression.

Establish readiness and authority

848 reviews the response arrangements and the services that could be affected. The customer identifies decision makers and confirms containment authority. For planning work, this becomes the basis for the selected design or preparedness recommendations.

Assess and prioritise the event

Where operational response is commissioned, analysts review detection information and available context to establish significance. The incident is classified and escalated through the agreed routes. Customer teams provide business impact and environment information to support prioritisation.

Coordinate authorised action

848 investigates and undertakes the initial actions included in the response scope. Automation follows the approved workflow and guardrails. Customer teams coordinate work on retained systems and wider remediation, with the incident record preserving the decisions and activity undertaken.

Review the findings and next steps

The selected investigation or review consolidates chronology and contributing factors. 848 explains limitations in the available evidence and agrees improvement priorities with stakeholders. Planning and automation engagements validate their outputs and transfer them to the receiving team.

4. Service Delivery and Management

4.1. Deliverables and Outcomes

The outputs give the customer a usable record of the work and the information needed to act on it. The selected elements determine which deliverables apply; findings and limitations remain visible alongside the results.

Deliverable	Use for the customer
Readiness findings or response guidance	Provides the assessment, plan or selected playbooks needed to strengthen incident preparation.
Validated response capability	Documents commissioned automation or the operational response arrangements and authorised actions.
Incident findings and improvement actions	Preserves the available incident evidence and lessons learned for customer decisions about remediation and readiness.

4.2. Working with 848

Customer leadership retains business decisions and approves response authority. Technical owners provide access and undertake retained remediation. Communication and regulatory responsibilities remain with the customer's nominated functions.

Participant	Responsibility
848 delivery team	Performs the selected work, explains findings and documents the relevant outputs. Coordinates review and knowledge transfer with the customer.
Customer service owner	Confirms the intended outcome and scope. Makes customer decisions and identifies who can resolve dependencies or approve changes.
Customer specialists and suppliers	Provide relevant information and agreed access. Complete retained activity and participate in review or validation where their systems or processes are involved.
Receiving team	Reviews the relevant outputs and takes ownership of the activities that continue after handover.

4.3. Service Assurance

Planning outputs are reviewed for practical use and role clarity. Automation is validated against the approved logic and guardrails. Operational response records distinguish authorised actions, findings and work that remains with the customer.

Review focus	What is checked
Scope alignment	The delivered work and outputs address the agreed requirements and selected service elements.
Evidence and validation	Findings or test results show the basis for conclusions, including known limitations and unresolved dependencies.

Review focus	What is checked
Customer acceptance	Relevant owners review the outputs and understand any open actions before accepting the commissioned work.

4.4. Onboarding

Onboarding establishes the conditions needed for useful delivery. The customer and 848 confirm what the engagement should achieve and check that the people and information needed for the selected work will be available.

Preparation	What needs to be established
Outcome and scope	Confirm the selected elements, boundaries and expected outputs, together with the customer's priorities.
Information and access	Relevant telemetry and licensed Microsoft capabilities must be available for technical work. Customer teams provide existing plans, contact routes and the permissions needed for agreed response actions.
Participants and decisions	Identify the service owner, relevant specialists and receiving team. Confirm review participants and escalation routes.
Delivery readiness	Agree the applicable schedule and customer prerequisites. Confirm any operational constraints affecting access, validation or handover.

4.5. Operating and Improving

Lessons learned identify changes to plans, detection coverage or safeguards. Owners prioritise those actions and commission implementation where required. The improvement record helps the customer revisit readiness after material incidents or environment changes.

4.6. Handover and Exit

The receiving team is briefed on response guidance, workflow operation and outstanding actions. For managed response exit, the customer confirms the future monitoring and incident owner and the transfer of available service records.

Handover item	Purpose
Agreed outputs	Provide the final documents or configuration material relevant to the selected service.
Findings and open actions	Preserve the evidence, limitations and remaining work for the customer or receiving provider.
Knowledge and ownership	Explain how the outputs should be used and confirm who owns the next operational or improvement activity.

5. Why 848

848 helps organisations improve how technology supports the way they operate, make decisions and deliver services. Our focus is not on deploying technology for its own sake, but on connecting technology investment to measurable business outcomes.

Our services are aligned through The Intelligent Business Framework, which brings together five outcome areas: The Intelligent Core, The Secure Business, The Efficient Business, The Insightful Business and The Innovative Business. This provides a consistent way to move from technology foundations and security through to operational efficiency, data-led decision-making and innovation, without treating each requirement as an isolated project.

848 combines consulting, engineering and managed service capability within one UK-based team. That matters because the people who design and implement change understand how technology must operate once it enters live service. Architecture, cloud, security, data, Power Platform, Dynamics 365, Microsoft 365 and managed services can therefore be considered as connected parts of the customer environment rather than separate technical towers.

Our Microsoft capability is supported by established partner credentials and practical delivery experience across Microsoft Azure, Microsoft 365, Power Platform, Dynamics 365, Fabric, Sentinel, Defender, Intune, Entra ID and Purview. 848 is a Microsoft Solutions Partner for Security and a Microsoft Direct CSP, giving our teams direct access to Microsoft technologies, programmes and commercial capability.

Service quality and security are supported by recognised organisational standards. 848 holds ISO/IEC 27001, ISO 9001, Cyber Essentials and Cyber Essentials Plus, with security-cleared capability available where required. These controls sit behind the way we manage information, quality, access, risk and service delivery across customer engagements.

What differentiates 848 is the connection between delivery and improvement. Through Value Chain-Led Managed Services, service information is converted into practical intelligence about how technology and services perform across users, teams, suppliers, systems and hand-offs. Service Flow Analysis extends that view by identifying friction, delay, rework, unclear ownership and recurring service issues across end-to-end journeys. The result is a clear improvement backlog based on real operational evidence rather than assumption.

We also place a strong emphasis on internal capability. Knowledge transfer, clear ownership and practical handover are built into our services so that customers understand what has been delivered, how it works and how it should evolve. Where 848 remains involved, improvement continues through review, prioritisation and measurable service outcomes rather than static support.

For customers, the result is a partner able to move from strategy through design, implementation, validation, operation and improvement while maintaining a consistent view of the wider business outcome. 848 brings together the people, Microsoft capability and service intelligence needed to make technology easier to operate, easier to improve and more valuable over time.