



Stiona Managed Service

OPERATE. SECURE. ASSURE

SERVICE DEFINITION DOCUMENT

JANUARY 2026

46 Donegall Pass

Belfast, BT7 1BS

Email Stiona (sales@stiona.com)

Tel: +44 (0) 2890 322011



Contents

1.	Stiona Managed Service Overview	3
1.1.	Why Stiona	3
2.	Service Scope and Inclusions	5
3.	Support Levels and Service Hours	7
4.	Service Level Agreements (SLA).....	8
5.	Incident, Problem and Change Management.....	9
6.	Security, Accessibility and Assurance.....	10
6.1.	Disaster Recovery and Service Continuity.....	11
7.	Service Reporting and Governance	12
8.	Onboarding and Offboarding	13
8.1.	Onboarding	13
8.2.	Offboarding	13
8.2.1.	End of contract data extraction	14
9.	Service Constraints and Exclusions.....	15
10.	Optional Enhanced and Additional Services	16
10.1.	Mobilisation Services	16
10.2.	Enhanced Configuration and Solution Design Services.....	16
10.3.	Data Services	16
10.4.	Payment Services	17
10.5.	Enhanced Support / Extended Hours	17
10.6.	Business Continuity Planning and Support.....	17
10.7.	Business Security Risk Management Support	17
10.8.	Custom Development Services.....	18
10.9.	Hosting Support Services	18

1. Stiona Managed Service Overview

Stiona Managed Service provides structured, ongoing operational support for Stiona-hosted SaaS services and the underlying cloud infrastructure on which they operate. The service is designed to ensure secure, reliable and compliant operation throughout the service lifecycle, from onboarding and live operation through to continuous improvement and assurance.

The Managed Service is delivered by Stiona's experienced cloud, platform and service management teams and operates in accordance with established service management practices and ISO-certified management systems. Stiona holds ISO/IEC 27001 certification for information security management and ISO 9001 certification for quality management, alongside Cyber Essentials and Cyber Essentials Plus accreditation. These credentials underpin the governance, controls and operational processes used to deliver the service.

The Digital Transformation Platform and its services have been successfully operated and supported by Stiona within the Northern Ireland Civil Service for over ten years, supporting mission-critical public sector services at scale. The platform and services undergo regular independent penetration testing and accessibility testing, with identified issues managed and remediated through controlled operational processes aligned to agreed service levels.

1.1. Why Stiona

Stiona is an established public sector technology partner with a proven track record of delivering and operating secure, scalable digital services. With over a decade of experience supporting live services within the Northern Ireland Civil Service, Stiona understands the operational, security and governance requirements of public sector environments.

Stiona's services are delivered on a mature, multi-tenant digital platform that has been designed for reuse, resilience and assurance. This approach reduces duplication, accelerates delivery and lowers total cost of ownership while maintaining consistent security and service standards across customers.

The organisation operates certified management systems, including ISO/IEC 27001 for information security management and ISO 9001 for quality management, supported by Cyber Essentials and Cyber Essentials Plus accreditation. These standards are embedded within Stiona's service delivery model and underpin its approach to risk management, service governance and continual improvement.

Stiona's services undergo regular independent security penetration testing and accessibility testing, with remediation managed through controlled operational processes aligned to agreed service levels. This ensures services remain secure, accessible and compliant throughout their lifecycle.

By combining proven platform capability with a structured managed service, Stiona provides customers with confidence that their services are operated securely, reliably and in line with public sector expectations.

2. Service Scope and Inclusions

The Stiona Managed Service provides ongoing operational support for Stiona-hosted Digital Platform (DTT) SaaS services and the cloud infrastructure on which those services operate. The service covers day-to-day management of service, platform and infrastructure components to ensure services remain secure, available and performant throughout their operational lifecycle.

As part of the standard managed service, Stiona provides service monitoring, incident and problem management, routine maintenance, security patching, backup and recovery operations, and service governance. This includes automated proactive health checks with associated alerting, operational support for service components, and coordination of remedial actions where issues are identified. The service also supports assurance activities, including coordination of annual penetration testing and accessibility testing for Stiona-managed services, and remediation of findings within agreed service scope and service levels.

Services are hosted on Microsoft Azure and associated cloud services, including networking and identity services. Service availability and performance are therefore dependent on the underlying cloud platform and third-party services. Planned maintenance is required to apply updates, patches and improvements and is communicated in advance where possible. Emergency maintenance may be required where necessary to address security vulnerabilities or service stability risks.

As part of the managed service, Stiona supports the controlled deployment of platform and service enhancements introduced through the product roadmap. Enhancements and new features are introduced through planned maintenance windows and communicated in advance where possible. The managed service supports the operation of released functionality but does not guarantee delivery of specific features or timelines, which remain subject to product planning and change control processes.

The managed service is delivered during standard support hours unless enhanced or extended support options are purchased separately. The service does not cover

customer-owned environments, end-user devices, local networks, or third-party systems outside the Stiona-managed scope.

The Stiona Managed Service is delivered using a tiered service model to ensure that operational support, assurance and governance activities are proportionate to the scale, complexity and risk profile of each supported service. Managed service tiers reflect factors such as service usage, transaction volumes, availability requirements, integration complexity and assurance effort. The applicable tier is agreed during onboarding and reviewed as part of ongoing service governance.

Tiered pricing is published separately within the G-Cloud pricing documentation. This Service Definition describes the capabilities provided across all tiers, with enhanced or extended support available as optional additional services.

3. Support Levels and Service Hours

Support is provided through the Stiona Managed Service during standard service hours of 08:00–18:00, Monday to Friday, excluding Northern Ireland bank and public holidays.

Standard Support is included as part of the managed service and provides access to the Stiona Service Desk via email or ticketing channels, together with access to user guidance and support documentation. Standard Support covers incident and problem management, routine operational assistance, and service-related queries within the defined service scope.

Support levels may vary by managed service tier, with enhanced or extended support available as an optional additional service.

Enhanced Support is available at additional cost and provides extended service hours, including 24/7 phone and email support, faster response and resolution targets, and access to a dedicated Technical Account Manager or Cloud Support Engineer, where required. Enhanced Support arrangements, including service hours and service levels, are agreed per contract.

Additional support and service management options may be purchased separately to meet specific operational or service assurance requirements. Further details are provided in 10.5 Enhanced Support / Extended Hours.

4. Service Level Agreements (SLA)

Stiona Managed Service support SLAs are outlined below. Response times relate to the acknowledgement of an incident following logging with the Service Desk.

Resolution times reflect restoration of service or provision of an agreed workaround. SLA targets apply during standard support hours unless enhanced support arrangements are in place.

Full definitions of priority levels, escalation processes and service management procedures are provided as part of the Stiona Managed Service documentation and contractual agreements.

Impact on service	Response Time	Resolution Time (Support)	Resolution Time (Defect)
Critical – P1	30 minutes	4 hours or as agreed by problem diagnosis	8 hours
High – P2	1 hour	6 hours or as agreed by problem diagnosis	32 hours
Moderate – P3	2 hours	8 hours or as agreed by problem diagnosis	Next planned release
Minor – P4	4 hours	12 hours or as agreed by problem diagnosis	Next planned release

Table 1 - Managed Service Level Agreements

Enhanced or bespoke SLA targets may be agreed where enhanced support services are purchased.

5. Incident, Problem and Change Management

Incident and problem management support is provided as part of the Stiona Managed Service to ensure service stability, availability and continual improvement.

Incident and problem management includes:

1. **Access to the Stiona Service Desk** for logging incidents during standard support hours.
2. **Incident triage and prioritisation** based on severity, impact and service dependency.
3. **Timely response and resolution of service incidents**, including provision of agreed workarounds where required.
4. **Restoration of normal service** following application, platform or infrastructure issues or outages.
5. **Identification and investigation of recurring or underlying issues** impacting service stability or user experience.
6. **Implementation of permanent fixes or corrective actions to prevent recurrence**, where issues fall within the Stiona-managed service scope.

Change management is used to ensure that updates and changes are introduced in a controlled manner. This includes assessment of change impact, scheduling of planned changes, coordination of releases and communication of planned maintenance where appropriate. Emergency changes may be applied where required to address security vulnerabilities or service stability risks, with retrospective review conducted as part of standard governance processes.

6. Security, Accessibility and Assurance

Security, accessibility and assurance activities are delivered as part of the Stiona Managed Service to ensure services remain secure, resilient and compliant throughout their operational lifecycle.

For services operating on the Stiona-Managed instance of the platform, Stiona provides ongoing security management and assurance. This includes management of hosting, network, identity and access controls, application security and data protection controls in line with established operational procedures and certified management systems. Security controls are actively monitored, maintained and reviewed as part of day-to-day service operations.

Stiona **coordinates and funds annual independent security assurance testing (ITHC)** for the Stiona-managed platform. Identified security findings are assessed, prioritised and remediated in line with published service level agreements and incident management processes, for example, Critical security findings are treated as equivalent to Priority 1 (P1) incidents and managed through the standard incident and problem management process.

The managed service also **supports accessibility assurance**, including coordination of periodic accessibility testing and remediation of identified issues within the managed service scope and agreed service levels.

Security monitoring, logging and alerting are in place to support detection of incidents, investigation of issues and auditability of security-relevant events. Data is protected using encryption in transit and at rest, with access controlled through managed identity and access controls.

Where a customer requires a dedicated or customer-managed platform instance, coordination and funding of security or accessibility testing and remediation activities **are not included as standard**. These activities may be supported through additional services, subject to separate agreement.

6.1. Disaster Recovery and Service Continuity

Disaster Recovery capabilities are built into the Digital Toolkit platform as part of the **standard service**. The platform is hosted within Microsoft Azure UK regions using a resilient architecture designed to maintain availability in the event of a component or site-level failure. The standard DR capability includes:

1. **Resilient, multi-zone architecture**
2. **Encrypted, automated backups**
3. **Defined recovery objectives (RTO/RPO)**
4. **Platform-level failover processes** - Infrastructure and core platform services are configured with automated failover or rapid redeployment processes to minimise downtime in the event of failure.
5. **Regular (annual) testing and validation** - DR processes are periodically tested as part of ISO platform assurance activities to ensure recovery procedures remain effective
6. **Secure data restoration**

These Disaster Recovery capabilities relate to the resilience and recoverability of the Digital Toolkit platform itself. Stiona's support for customer-specific Business Continuity planning, operational continuity processes, or wider organisational risk management is not included as part of the standard service and is available as an optional, additional-cost professional service.

7. Service Reporting and Governance

As part of the Stiona Managed Service, quarterly service review and steering meetings are typically held to support effective governance and ongoing service improvement. These meetings provide a structured forum to review service performance, operational activity and forward planning.

A typical service review agenda includes a delivery summary covering activity and performance from the previous quarter and planned activity for the upcoming quarter. Financial matters relevant to the managed service are reviewed where applicable. Service management reporting is discussed, including service availability, incident metrics and trends, and any change requests raised during the period.

The review also covers current risks and issues, progress against previously agreed action points, and any additional items raised by either party. Outcomes, actions and decisions from service review meetings are recorded and tracked through agreed governance processes to ensure accountability and follow-through.

The structure and frequency of service review meetings may be tailored to customer requirements by agreement.

8. Onboarding and Offboarding

8.1. Onboarding

As part of standard service delivery, Stiona provides structured onboarding to enable supported services to operate within the Stiona Managed Service. Standard onboarding activities include:

1. ***Publish the service to the target user groups*** (e.g. Citizen Portal, Authenticated citizen etc)
2. ***Configure the chosen authentication mechanism*** (if already supported by the platform identity service)
3. ***Configure the service user roles*** applicable to each user group.
4. ***Create the initial administrative ('super-admin') users.***

Additional onboarding and mobilisation services are available at additional cost. These may include support with service and organisational configuration, message or workflow configuration, business process mapping, form or configuration design, data migration, and remote or onsite user training. Stiona can also support user testing preparation and execution to support a controlled rollout. For complex implementations, mobilisation and configuration design services are recommended.

8.2. Offboarding

At the end of the contract, we provide a structured offboarding process to ensure a smooth transition. Included as part of the managed service are:

1. ***Export of customer data*** in a supported format,
2. ***Closure of service accounts***
3. ***Revocation of user access*** for all user groups which may be phased if required.

Customers retain full ownership of their data. Additional offboarding services, including assisted data migration, bespoke export formats, extended access beyond contract end, or transition support to another supplier, are available at additional cost. All offboarding activities follow agreed security and data-retention requirements.

8.2.1. End of contract data extraction

Customer data is encrypted in transit and at rest and stored within managed databases. As standard, Stiona provides a complete export of customer data in CSV format at contract end at no additional cost. Service configuration data can be exported in JSON format on request. Additional export formats or structured migration support may be provided subject to technical feasibility and may incur additional cost. All data extractions are delivered securely and in line with agreed timelines and retention requirements.

9. Service Constraints and Exclusions

The Stiona Managed Service supports Stiona-hosted SaaS services and the cloud infrastructure operated and managed by Stiona. Service availability and performance are dependent on the underlying cloud platform and third-party services, including Microsoft Azure and associated networking and identity services.

Planned maintenance is required to apply updates, patches and service improvements and is communicated in advance where possible. Emergency maintenance may be required to address security vulnerabilities or service stability risks and may be undertaken outside planned maintenance windows. Standard support hours apply unless enhanced or extended support services are purchased.

The managed service does **not** cover customer-owned or customer-managed environments, end-user devices, local networks, on-premises infrastructure, or third-party systems and integrations outside the Stiona-managed service scope. Support for bespoke configurations, customer-specific platform instances, or third-party services may be provided through optional additional services where agreed.

10. Optional Enhanced and Additional Services

Stiona can also offer the following optional service and customer delivery support services at additional cost:

(All optional services are delivered subject to separate agreement, scope definition and pricing, and are not included within the standard Stiona Managed Service.)

10.1. Mobilisation Services

Stiona can provide customers with additional support throughout the delivery period from contract award to the point the service becomes operational and under Managed service scope. This includes

1. Project/Programme planning and co-ordination
2. Planning and guided User Acceptance Testing
3. Implementation planning
4. Data migration support
5. Customer engagement support
6. Training materials and delivery via multiple channels
7. Change Management activities

10.2. Enhanced Configuration and Solution Design Services

We offer additional design services that go beyond standard onboarding into deeper implementation work including:

1. Advanced workflow design and optimisation
2. Advanced Form design and configuration services
3. Integration and design workshops
4. Requirements gathering / discovery sessions
5. Process mapping and business process re-engineering

10.3. Data Services

We offer additional data management services including:

1. Complex data migration support (multiple sources, data transformations and complex cleansing)
2. Legacy system extraction consultancy
3. Data modelling and design

10.4. Payment Services

We offer additional payment management services including:

1. Assistance in establishing the payment product catalogue configuration
2. Integration to payment provider(s) other than Worldpay or Gov.UK Pay
3. Additional payment reporting

10.5. Enhanced Support / Extended Hours

We can offer enhanced or extended support on request including:

1. Extended service desk hours
2. Out of hours incident response
3. Priority Service levels with faster SLAs
4. Scheduled Evening/ Weekend maintenance windows
5. Extended proactive monitoring and notifications
6. Regular service review reporting and meetings

10.6. Business Continuity Planning and Support

We offer additional business continuity planning and support services including:

1. Helping the customer write or update their BC plan
2. Running BC workshops with stakeholders
3. Scenario modelling and impact assessments
4. Establishing customer playbooks or continuity checklists

10.7. Business Security Risk Management Support

We offer additional business security risk management services including:

1. Threat and risk assessments
2. Security policy development
3. Governance and compliance reviews
4. Support in meeting internal audit requirements

10.8. Custom Development Services

We offer additional custom development and enhancement services to support customer-specific requirements for Stiona-hosted services. These services extend beyond standard managed service scope and are delivered subject to separate agreement. Examples include:

1. Bespoke feature or module enhancements aligned to supported services
2. Custom reporting or dashboard development
3. Configuration-led user experience or branding enhancements
4. Document management, bundling or export enhancements
5. Reporting enhancements integrated with service dashboards

10.9. Hosting Support Services

As standard, supported services are operated on the Stiona-managed Digital Toolkit platform. Where required, Stiona can support the deployment and operation of services within a customer-managed Azure subscription as an additional service. This includes platform setup, configuration and operational support. Custom URLs, DNS configuration or customer-specific networking requirements may incur additional cost and are subject to technical feasibility.