Q-SOLUTION

Secure Mail as a Service

Service Description

Crown Commercial Service Supplier

ISO 27001 Certified

CYBER ESSENTIALS PLUS

For more information about our services please contact us:

Tel: +44 (07538) 023530 | email: contact@q-solution.co.uk

or write to:

Customer Services, 2 Tallis Street

London, EC4Y 0AB

Disclaimer

Any views, opinions and guidance set out within this document are provided for information purposes only and do not purport to be professional advice. No responsibility or liability is accepted for any errors or omissions in this document or related documents.

Crown Commercial Service Supplier

Information Security Management System ISO 27001 Certified

CYBER ESSENTIALS PLUS

Q-SOLUTION

Table of Contents

1 Overview

The UK Public Sector places a high emphasis on securing communications and safeguarding sensitive data during exchanges among organisations on a need-to-know basis. Q-Solution has been active in this secure domain of the Public Sector for over 20 years, earning trust through our various G-Cloud services to securely transmit highly sensitive data between entities such as the Police, HMCTS, DVLA, CPS, Home Office, and others.

Our Secure Mail service is a closed community relay and hosted webmail service, enabling organisations to safely share protectively marked information up to OFFICAL with sensitive marking.

The service is provided by a resilient and scalable infrastructure hosted in public cloud, protecting against accidental emailing to inappropriate recipients, phishing and malware, while enabling secure connectivity to customers via the Internet and UK Government networks such as the Public Sector Network (PSN) subject to approval from the appropriate Authority.

Q-Solution ensures the necessary security standards are met for authentication and access management, encryption at rest and in transit, protective monitoring, vulnerability management and cloud configuration.

1.1 Key Features

The following features are delivered as part of the Secure Mail as a Service

- Closed community of mail users from authorised organisations
- SMTP connections to and from authorised:
    - On-premise mail server routed via Internet
    - On-premise mail server routed via UK Government network
    - Google Workspace (Gmail) hosted organisation mail service
    - Microsoft 365 (Exchange Online) hosted organisation mail service
- Hosted webmail with delegated administration
- Directory service of users and organisations with opt-in option
- Phishing resistant Multi Factor Authentication (MFA) for webmail users
- Highly scalable anti-malware service
- TLS 1.2 / 1.3 for secure communication in transit with enforced mTLS for SMTP relay customers
- Leverages public cloud services for resilience and capacity at scale
- Data held entirely within UK Sovereign Data Centres
- Continuous vulnerability, cloud configuration and cloud event monitoring with context-based prioritisation
- Fully managed Security Incident and Event Management (SIEM)
- Management reporting
- Certified against Cyber Essentials Plus and ISO27001
- 99.9% availability
- Service desk for customer administrators

1.2 Benefits

- Prevents accidental emails to recipients outside closed community
- Ensures encrypted email delivery between Internet and UK Government networks
- Wide range of mail services supported including cloud and on-premise
- Effective search for organisations and individuals using directory service
- Delegated administration allows organisation self-service
- Protection against phishing and malware
- Resilient and scalable infrastructure hosted in public cloud
- Emails with attachments can be sent reliably

1.3 Monitoring

Monitoring of the infrastructure is performed by Q-Solution as a part of the Managed Service. This includes both System Monitoring and Protective Monitoring.

System Monitoring and Alerting

System Monitoring involves the monitoring of the underlying services supporting the cloud platform. Thresholds are set for these services to generate automated alerts if they are breached. Details of these thresholds and the alerting and communication with customers will be provided during the on-boarding process and are fully customisable.

Management Information

Extensive Management Information (MI) is provided including:

- email volumes
- Total registered organisations
- Breakdown of organisations between SMTP Internet, SMTP PSN, cloud gateway and webmail organisations
- Numbers of webmail users

The MI is provided through a web front end and can be customised to ensure the customer receives the insights relevant to their business.

Protective Monitoring

The service is governed by a fully managed Protective Monitoring regime supported by our internal security operations team. The service:

- Ensures all systems and services are patched to the latest supported versions
- Measures our technical controls against NIST and ISO27001
- Protects against phishing and malware
- Monitors user activity, alerting suspicious behaviour based in the MITRE ATT&CK knowledge base

1.4 Security and Information Assurance

Q-Solution operate a comprehensive Cyber Assurance process across all our cloud and corporate IT. Our Assurance Document Set (ADS) aligns with the following HMG & Corporate Policies:

- HMG Security Policy Framework
- NCSC Cloud Security Principles
- NCSC Architectural Patterns
- NCSC Cyber Assessment Framework
- Q-Solution Information Security Policy and sub policies
- ISO/IEC27001 standard
- NIST Cybersecurity Framework
- Government Secure by Design Principles

The following documents support our ADS and can be provided to the customer during the onboarding process

- Information Risk Assessment Report (IRAR) overview document
- Risk Assessment Methodology and Risk Treatment documentation
- ISO/IEC 27001 certification, SoA and audit findings
- Audit Policy
- AWS Well Architected Review
- NCSC Cloud Security Principles
- NCSC Cyber Assessment Framework
- NIST Cybersecurity Framework (Mapped to ISO27001)
- CHECK ITHC report and vulnerability management/mitigation
- Cyber Essentials reports and Action Plan

1.5 Limitations

The following are the current limitations of the service.

- Mail Server compliance with RFC5321 and RFC5322 (only applies to on-premise customers)

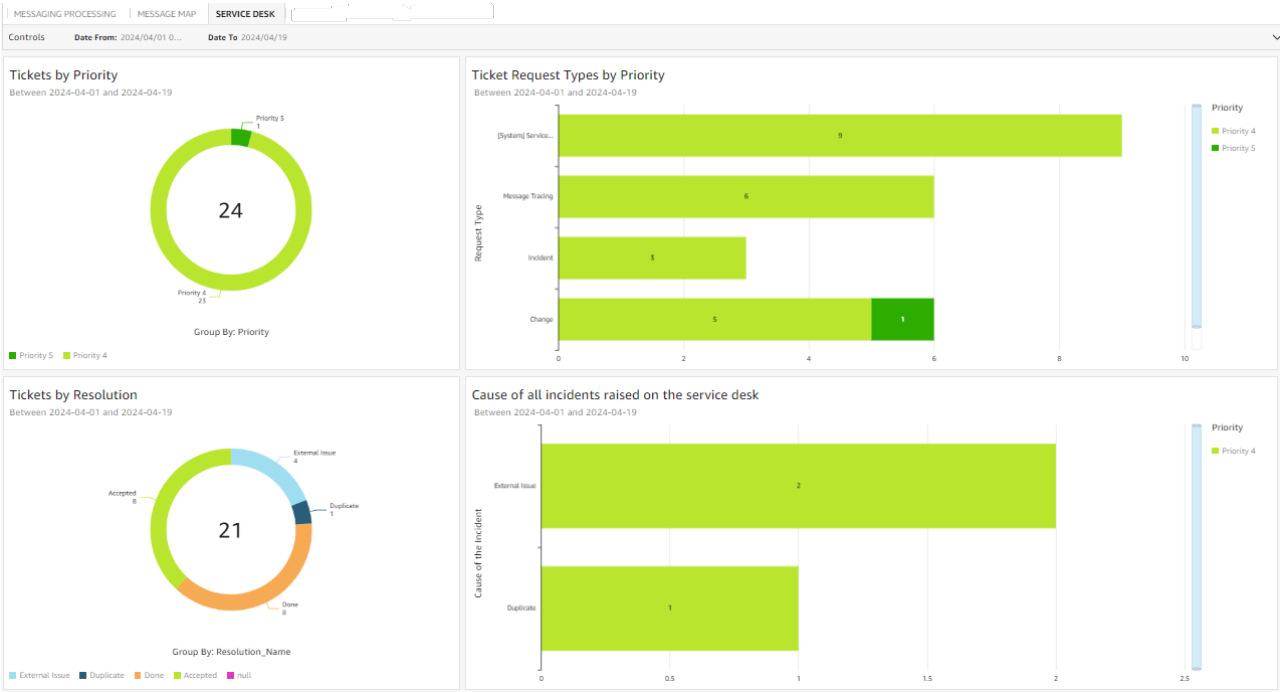
2 Secure Mail Service Management

2.1 Overview

Q-Solution provide the overall service management wrap for the secure email service, providing monthly service reports including but not limited to:

- Tickets raised
- Performance against SLA's
- Incident trend types
- Change Management
- Continuous Improvement initiatives

Whilst this is reviewed monthly, our Management Reporting is dynamic and online allowing the customer to view these and other metrics in real time through and online portal.



Our Service Management tooling has a number of APIs available for customers to use to feed service management information into their own analytics platform if required.

2.2 Support Hours

Support hours for the service desk is between 8am and 6pm, Monday to Friday excluding UK Public Holidays. Our Protective Monitoring and System Monitoring however operates 24/7/365 and will generate alerts throughout this period in the event of any priority incidents occurring.

2.3 SLA Targets

Measure	SLA Component	Target Value	SLA Value
Incident Response time	P1 Response time	10 minutes	100%
	P2 Response time	30 minutes	100%
	P3 Response time	1 Hour	100%
	P4 Response time	8 Hours	100%
Incident Restoration time	P1 Restoration time	1 Hour	98%
	P2 Restoration time	4 Hours	100%
	P3 Restoration time	24 Hours	100%
	P4 Restoration time	3 Days	100%
Incident Resolution time	P1 Resolution time	4 Hours	98%
	P2 Resolution time	8 Hours	98%
	P3 Resolution time	3 Days	98%
	P4 Resolution time	7 Days	98%
Change Management	Emergency Change	12 Hours	100%
	Standard Change	2 Days	100%
	Planned Maintenance Notification	14 Days	100%
Problem Management	Root Cause Analysis Delivery	1 Day	98%
Availability	Monthly Availability	99.95%	100%
Business Continuity	Recovery Point Objective	Zero hours	100%

Measure	SLA Component	Target Value	SLA Value
	Recovery Time Objective	30 minutes	100%

2.4 Availability Targets

Type	Measurement	SLA (over month)
Availability	Availability of the service during working hours (8am to 6pm, Monday to Friday excluding Bank Holidays)	99.9%
	Availability of the service outside of working hours.	99.5%
Service Desk	Monday to Friday, 8am to 6pm excluding UK Public Holidays	See Secure Messaging Incident Management

The service availability outside of core hours allows for patches, change requests and enhancements to be made to the service. When necessary, a scheduled maintenance window will operate with notification of changes published to the Service Desk Portal as well as communicated via the customers preferred channel.

By design, the services provides the necessary resilience to allow patching to occur without service interruption.

3 Secure Mail Incident Management

Users of the service have two channels for raising incidents on the service:

- Email
- Online Portal

Emails can be sent to a centralised email address that will generate a ticket to be triaged and raised with the support desk. Alternatively, a portal is available that allows users to raise specific service requests directly, ensuring the information required by the service desk is provided and therefore a quick response to the incident can be achieved.

3.1 Incident Response

Incident Management and the response to incidents is defined through a combination of two factors:

- Urgency of the incident
- Impact of the incident

Incident Urgency

The *urgency* of the incident is defined as how quickly a resolution to an incident is required.

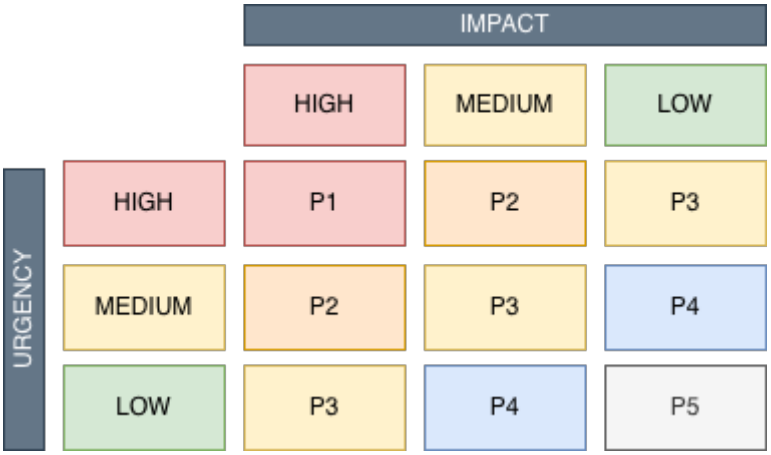
Category	Description
High (H)	• The damage caused by the Incident increases rapidly. • Work that cannot be completed by staff is highly time sensitive. • A minor Incident can be prevented from becoming a major Incident by acting immediately.
Medium (M)	• The damage caused by the Incident increases considerably over time.
Low (L)	• The damage caused by the Incident only marginally increases over time. • Work that cannot be completed by staff is not time sensitive.

Incident Impact

The *impact* of the incident is defined by what impact this incident is having on live operations and specifically the number of users and/or systems affected.

Category	Description
High (H)	• A large number of staff are affected and/or not able to do their job. • A large number of customers are affected and/or acutely disadvantaged in some way. • The damage to the reputation of the business is likely to be high. • Someone has been injured.
Medium (M)	• A moderate number of staff are affected and/or not able to do their job properly. • A moderate number of customers are affected and/or inconvenienced in some way. • The damage to the reputation of the business is likely to be moderate.
Low (L)	• A minimal number of staff are affected and/or able to deliver an acceptable service but this requires extra effort. • A minimal number of customers are affected and/or inconvenienced but not in a significant way. • The damage to the reputation of the business is likely to be minimal.

The diagram below defines the Priority assigned to incidents raised.

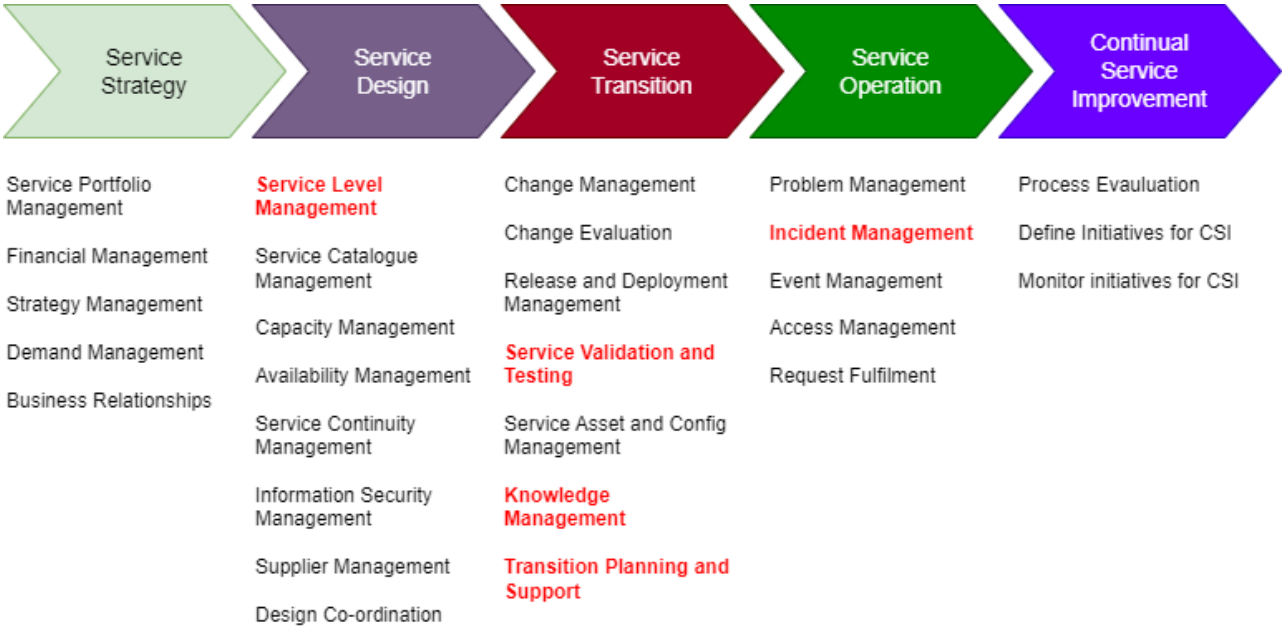


Response times for Priority incidents are defined in the Service Level Agreement Target section

Please note that as part of the On Boarding process, our Incident Management as well as our Problem Management processes will be shared with the customer and integrated into their own operating model as necessary.

4 Acceptance Into Service

By offering a SaaS service, the supplier assumes the majority of the overhead linked to a complete ITIL-based AIS, thus relieving the customer of this burden and associated costs.



The above diagram highlights the key processes our Service Transition Manager will work on with the customer, ensuring our internal services integrate seamlessly with the customers.

4.1 Service Level Management

We ensure our Service Levels for all incidents and requests are aligned to the customers own Service Management Model and ITSM tooling.

4.2 Service Validation and Testing

We define all elements of testing including UAT and Service Management Acceptance Testing (SMAT) that are required for live running. All collateral will be made available to the customer online and in real-time. Our Testing products typically following industry standard best practice

4.3 Knowledge Management

A dedicated wiki is maintained throughout the lifetime of the contract. This contains all the knowledge base articles required for 1st line support to efficiently operate the service. These will also be subject to SMAT testing.

4.4 Transition Planning and Support

A dedicated Service Transition Manager will assigned to work in partnership with the Authority to define both the Transition plan and step by step transition processes.

During first weeks of early life support, the delivery team will be centrally located to support the Authority.

4.5 Incident Management

Extensive testing will be conducted through SMAT to ensure that all incident types, Change Requests, and Service Requests are integrated between our ITSM systems and that SLAs can be automatically extracted from these tools.

4.6 Delivery Team

The project delivery team may consists of one or more of the following roles

Role	Responsibilities
Technical Delivery Management	Responsible for managing the technical aspects of the service during AIS, this role involves liaising with the customer and Q-Solution to ensure that the service's technical requirements are implemented and adhere to the required standards.
Service Transition Manager	Responsible to aligning our Service Management processes with those of the customer. Agreeing service reporting processes against SLA and ultimate responsibility for AIS
Security Architect	Works with the customer to ensure all cyber security requirements are being delivered by the service and ongoing cyber assurance processes are in place throughout the life of the contracts
DevOps engineer	Providing technical engineering to implement customisations required by the customer

5 Secure Mail Pricing

5.1 Billing and Charging

Our charging model for the Secure Mail as a Service is designed to be simple and cost effective. The charges for the platform consist of

- On-Boarding Acceptance Into Service (AIS) setup charge
- Monthly charge based on total users by group
- Initial Organisation setup fee

5.2 Onboarding Charge

The initial onboarding charge is associated with working alongside the customer to either setup the solution from scratch or support the migration of existing users and mailboxes onto the service including customisations as necessary. The charges associated with this will be for Professional Services and typically involve one or more of the following roles:

- Technical Delivery Management
- Service Management
- Security Architect
- DevOps engineer

Rates can be found in the supporting Q-Solution SFIA Rate Card.

5.3 Commodity Charging

The secure email service is charged on a per user/organisation commodity basis.

Web Users

Web User volumes	Per user/year
up to 9,999	£22.50
10,000 to 49,000	£15.75
50,000 to 99,999	£12.40
100,000 to 149,999	£9.00
150,000 to 249,000	£7.90
Above 250,000	£7.90

Charges for web users are applied on a staggered basis as detailed in the table above. For example, customers requiring 12,000 web users, will be charge at £22.50 per user/year for the initial 9,999 users and £15.75 per user/year for the additional 2,001 users.

There is a minimum purchase of 1,000 web users of the service

5.4 Organisation

An Organisation is an enterprise set up to route email to certain domains through the system without user action. This will typically be an on-premise mail server or relay, a Microsoft 365 Exchange Online cloud gateway, or a Google Workspace cloud gateway.

Organisation volumes	Per Organisation/year
up to 149	£220.00
150 to 499	£187.00
500 to 999	£165.00
1,000 to 4,999	£121.00
5000 to 9,999	£99.00
Above 10,000	£88.00

Charges for Organisations are applied on a staggered basis as detailed in the table above. For example, customers requiring 200 Organisation, will be charge at £220.00 per org/year for the initial 149 organisations and £187.00 per org/year for the additional 51 organisations.

There is a minimum purchase of 10 organisations of the service

5.5 Education pricing

We do not offer separate pricing for educational bodies.

5.6 Sector Pricing

We do not differentiate our pricing across different sectors or bodies.

5.7 VAT

All prices within this document are exclusive of VAT, which will be applied at the prevailing rate.

5.8 Indexation

The Supplier may increase the Charges on an annual basis with effect from each anniversary of the contract start date in line with the percentage increase in the Consumer Prices Index (CPI) in the preceding 12-month period.

> "Consumer Prices Index" means the Consumer Prices Index as published by the Office for National Statistics from time to time, or failing such publication, such other index as the parties may agree most closely resembles such index.

Other Charges

Q-Solution reserves the right to apply additional charges based on the standard SFIA rate card in support of customers requirements outside the scope of the Secure Email as a Service offering. Any such requirement will be agreed with the customers during the onboarding process.