civica

Transforming the way you work

Service Description

Digital & Biometric Forensics Service

DOCUMENT CONTROL

COPYRIGHT

Any questions regarding this document should be directed to:

Name	Serena Attridge
Address	Civica UK Limited, 2 Burston Road, London, SW15 6AR
Telephone	020 77602800
Email	serena.attridge@civica.co.uk

Digital and Biometric Forensic Services

Summary

A holistic service for the management and processing of Forensic Evidence and Records. Providing a central asset management hub and additional best of breed modules for fingerprint, photo and video analysis and face recognition software. Proven integration with third party applications and hosted in a compliant IL3 environment.

Features

- Civica FileTrail Evidence and Asset Tracking software
- FISH Forensic Image Scanning Hub
- MXServer Face Recognition Software
- Sungard IL3 Compliant Official Assured Zone Managed Cloud Services
- Full end to end Digital Biometric Forensics Management
- Complete Audit Trail and Reporting
- Fully configurable Workflow Dashboards
- Seamless integration
- Best of breed applications and hosting
- Single modular solution

Benefits

- Fully configurable to meet a wide range of requirements
- Significant reduction in staff inputting and processing time
- Demonstrable return on investment
- Automated barcode and RFID tracking
- Simple and intuitive interface
- Faster detection of offenders
- Extends an organisation’s intelligence base
- Secure hosting with full Disaster Recovery
- Relives the strain on existing It infrastructure
- Proven track record in this field

Civica Forensic Asset Tracking software using FileTrail Forensic Asset Tracking Software

Track and manage evidence and assets with full workflow capability and audit trail

Sub-contractors:

Sungard Availability Services (http://www.sungardas.co.uk)

Table of Contents

Filetrail Overview

Civica offers a solution to track and manage forensic assets with high accuracy utilising FILETRAIL.

Hosted on secure PaaS supplied by Sungard Availability Services.

1.1 FileTrail Overview

FileTrail is a powerful web-based Evidence, Forensic and Asset Management Software tool that enables organisations to track and manage an unlimited number of evidence forensic and asset items in an unlimited number of locations and accessed by an unlimited number of users.

By using barcode reading it allows fast and easy recording of item movements, edits, updates and audits by users. It also operates with Radio Frequency Identification (RFID) systems to allow completely automatic logging of asset whereabouts and movement.

FileTrail monitors every item of evidence in its database and informs users of the precise location of evidence at any time and a complete history of their movement to date. It also provides powerful searching and requesting functionality as well as a comprehensive checking-out and checking-in system. Furthermore, it will manage evidence in forensic laboratory, evidence stores right through to their ultimate destruction when they have reached the end of their life cycle period.

FileTrail is a fully comprehensive system that fully meets all organisations requirements for managing evidence and any other items that need to be tracked.

FileTrail is currently used by many large organisations where IT asset and records management is a critical issue and some specific references can be provided. Good examples of this are the DBS (NSV) (Defence Business Services (National Security Vetting), formerly the Defence Vetting Agency at Imphal Barracks in York) and Humberside Police. DBS (NSV) use FileTrail to track and manage around half a million files used by 150 Vetting Staff.

Humberside Police use the system for a wide range of applications including force records, custody suite audio tapes, car and helicopter video media, items of evidence etc. The reason they can do this is because FileTrail can track and manage any item that carries a barcode or RFID tag and users can set up an unlimited number of separate applications from their FileTrail Server licence.

1.2 Proven Deployments

FILETRAIL is being utilised by a number of UK Police Forces and by the FBI

UK customers include the following Forces:

- Humberside Police
- North Yorkshire Police
- GARDA
- MOD

In addition, Civica brings outstanding customer focus, commitment and track record, testimony to which is a history of successful long-term relationships. Providing the technology behind local transactions with more than 25 million citizens and businesses, Civica is delivering to:

- More than 90% of the UK’s police forces and many US Police Departments
- Central Government Organisations such as the MOD
- More than 800 local authorities including 90% of UK councils and more than 300 in Australia & New Zealand

- Over 1,500 schools and libraries, including as IT partner for school modernisation programmes in Sheffield, Luton, Barnsley and Wandsworth and in Singapore
- Almost 200 social housing organisations, managing from 250 to 110,000 units
- Some of the largest health care providers in the UK and Canada

Civica Blue Light Services works with police forces and government agencies in the UK and the USA, delivering software and services that help to bring about safer streets and communities together with greater efficiency, underpinned by leading expertise in secure data communications and mobile working. The Civica Group has a long history in the sector working with customers to support improved policing, and solutions provided are used by 90% of UK police forces together with authorities such as the Vehicle & Operator Services Agency and the Highways Agency.

Civica has a long history of providing widely used software and the broadest range of options for access to the Police National Computer, including direct system interfaces, web browser and mobile access for laptops, tablets and PDAs. Drawing on this experience, the company has built a position as a safe pair of hands for secure data access solutions.

1.3 How FILETRAIL Works

FileTrail sits as a central hub for managing and processing evidence and assets.

Proven integration via web services to most applications including digital asset stores, Force crime management systems, workflow systems and external third parties.

As well as accepting the physical input of data, FileTrail also offers automated tracking utilising a wide range of barcode and RFID technologies.

In essence, any detail of an incident can be monitored and processed from crime number generation and scene of crime all the way through to case completion.

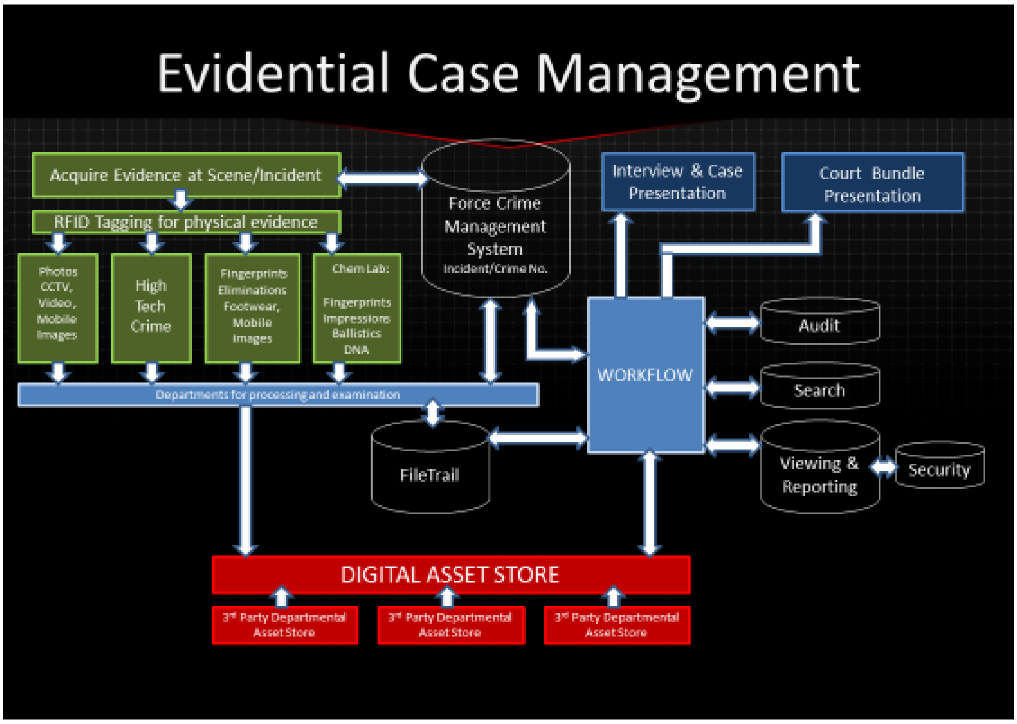
FileTrail is fully configurable to manage processing times, retention schedules and destruction.

Proven to dramatically reduce the time staff spend inputting and managing information.

Key Performance Indicators can be individually configured and displayed via web dashboards.

Full audit suite offers the production of tailored reports on an automated or manual basis and can be interrogated to establish individual amendments to a record on an ad hoc basis.

Example application:



Evidential Case Management

Acquire Evidence at Scene/Incident

RFID Tagging for physical evidence

Photos CCTV, Video, Mobile Images

High Tech Crime

Fingerprints Eliminations Footwear, Mobile Images

Chem Lab: Fingerprints Impressions Ballistics DNA

Departments for processing and examination

Force Crime Management System Incident/Crime No.

Interview & Case Presentation

Court Bundle Presentation

WORKFLOW

Audit

Search

Viewing & Reporting

Security

FileTrail

DIGITAL ASSET STORE

3rd Party Departmental Asset Store

3rd Party Departmental Asset Store

3rd Party Departmental Asset Store

1.4 Benefits of FILETRAIL

- FileTrail is an “industrial strength” Evidence and Forensic Management software tool that will meet the requirements any Police Force requiring the tracking and management of evidence, forensic tests and property stores.

- With the addition of User licences, FileTrail for provides a complete set of configuration, administration and operational features. The server licence includes the rights to configure an unlimited number of fields, screens, labels, search forms, place locations and active storage locations.

- Users will access all the FileTrail functionality through their web interface making training a very quick and simple process.

- There are no limits to the number of evidence items or users (subject to licensing) managed by the system.

- FileTrail accepts item movement instructions from barcode scanners, RFID readers, keyboard input or through its own bulk input tool “FT Connect”.

- FileTrail has a powerful Retention Management module to enable an unlimited number of assets with varying retention periods/service periods and warranties to be managed and reported on.
- Civica has extensive experience in the implementation and support of this system with clients including Global Banks, Pharmaceutical Multinationals, Police Forces, MOD and large corporate bodies.

- Civica has the resources available to configure and fully implement the system as required providing full training and support

Information Assurance

Civica partners with Sungard AS who provides a Managed Cloud Service for UK Government connected and compliant to PSN Code of Connection and Service Provision, the infrastructure platform over which the service will run.

The service can be run either in the Assured or Protected Zones that are connected to PSN Assured and PSN Protected Respectively with additional options of an Internet breakout in the Assured Zone only.

Sungard AS' Government Cloud is hosted in the UK only. The service is supported by a dedicated SC Cleared UK based service operations team with staff background checks in accordance with BS7858:2012,

The service is aligned to the CESG Cloud Security Principles.

Sungard AS has ISO 9001:2008 and ISO/IEC 27001 certification and BS 25999-2:2007 certification.

Back-up / Restore Recovery Level

Details of Sungard AS' Managed Cloud Services for UK Government back-up and recovery service can be found in the service definition and terms and conditions that can be found on the digital market place.

On-Boarding / Off Boarding Process

On-boarding and Off-boarding processes/scope etc.

On-boarding

Details of Sungard AS' Managed Cloud Services for UK Government on-boarding service can be found in the service definition and terms and conditions that can be found on the digital market place.

Off-boarding

Details of Sungard AS' Managed Cloud Services for UK Government off-boarding service can be found in the service definition and terms and conditions that can be found on the digital market place

Pricing

1.5 SaaS Pricing

The service consists of the sale of a non-exclusive license to install and use the FILETRAIL software described herein on a monthly subscription basis, using Sungard AS' Managed Cloud Services for UK Government.

We have developed a standard pricing/performance model that can be applied to estimate the cost of an FILETRAIL deployment based upon digital media processing requirements. The pricing model is made up of a base package plus additional scaling units, as required. The base package includes a system meeting the minimum recommended configuration. All additional modules at additional cost

Costs are detailed in the supplied price schedule

1.6 Software Licensing Pricing Variability

Pricing is dependent upon exact client requirements. In the absence of specific client requirements, the above pricing for software licensing is indicative.

Additionally, software licensing pricing may also vary with the number of months the purchaser commits to the service, as well as the number of Additional Scaling Units (if any) subscribed to.

An exact quote can be provided after an initial consultation with the purchaser.

1.7 Required Professional Services

The stated software licensing prices exclude any required professional services for:

- Software installation, configuration and commissioning.
- Bespoke development required to adhere to specific and agreed customer requirements.
- Integration with external and 3rd party systems.
- Training on use of the FILETRAIL.

1.8 Annual Support and Maintenance

Support and Maintenance and help desk is included in the service price.

1.9 Support and Maintenance

The monthly subscription includes support and maintenance.

Support and maintenance includes:

- Free software upgrades (including patches and updates).
- Fault / bug reporting and resolution. (via email)
- Logging of enhancement requests. (via email)
- Access to 1st line Help Desk
  - Telephone: Mon-Fri 9-5 excluding holidays
  - email

Support and maintenance excludes:

- Customer side Installation, integration and configuration services (can be covered by Additional Services)
- Training (can be covered by Additional Services)
- Product use instructions (can be covered by Additional Services)

Service Constraints

“Planned Maintenance” means any pre-planned maintenance of any infrastructure relating to the Services. Civica shall provide the Customer with at least twenty-four (24) hours’ advance notice of any such planned maintenance:

Planned maintenance of Sungard's infrastructure relating to the Services shall happen between the hours of 00:00 and 06:00 (UK local time) Monday to Sunday and/or between the hours of 08:00 and 12:00 (UK local time) on a Saturday and/or Sunday. No planned maintenance will take place on a Saturday unless agreed in advance by both parties;

Planned Maintenance shall be excluded from any availability calculation in regard to service credits but shall be included in the monthly service reporting;

"Emergency Maintenance" means any emergency maintenance of any of the infrastructure relating to the Services. Whenever possible, Sungard shall provide the Client with at least six (6) hours' advance notice:

Whenever possible Emergency Maintenance of Sungard's infrastructure will happen between the hours of 00:00 and 06:00 (UK local time) Monday to Sunday and/or between the hours of 08:00 and 12:00 (UK local time) on Saturday and/or Sunday unless there is an identified and demonstrable immediate risk to a Clients environment;

Emergency Maintenance shall be excluded from any availability calculation in regard to service credits but shall be included in the monthly service reporting.

This is from page 6 of Sungard AS' Managed Cloud Services for UK Government Terms and Conditions.

9. VDC Infrastructure and Maintenance

From time to time, Sungard AS may need to perform maintenance on or make adjustments to the infrastructure (including without limitation, any Sungard AS provided telecommunications links, Sungard AS Equipment and Sungard AS Software, on which the Customer VDC(s) relies and shall be entitled to do so at its discretion, without incurring liability for so doing. In the event of any such maintenance or adjustment being needed, then except in the case of emergency maintenance, Sungard AS will give the Customer reasonable prior notice and shall use all reasonable endeavours to limit the interruption. If emergency maintenance is needed, Sungard AS shall be entitled to interrupt services without prior notice.

Service Levels

- The Service is based on a Service Level Availability (SLA) of 99.95%
- Civica will endeavour to respond to all incidents within 4 Hours
- Service Credits are not offered against this Service offering

Details of Sungard AS' Managed Cloud Services for UK Government infrastructure/platform SLA can be found in the service definition and terms and conditions that can be found on the digital market place

Termination Terms

Terms

The Customer and Civica agree to a monthly subscription.

Customer and Civica will also agree to a minimum number of month's commitment. The agreement will terminate on the last day of the agreement, unless a request to extend the agreement is received within 7 working days in advance.

Either party may terminate at any time if the other party is in material breach of agreement.

At the point of termination, all consumer data, accounts and access will be permanently deleted, and will not be able to be subsequently recovered or restored.

Costs

There are no termination costs for this Service. Consumers are responsible for extracting their own data from the platform if required.

Sungard may make an additional charge for transferring data out of the service.

Data Restoration / Service Migration

- Data will be restored following a data restore request within 24 hours.
- No Service Migration capability is offered as part of this Service offering

Details of Sungard AS' Managed Cloud Services for UK Government RPO/RTO SLA. can be found in the service definition and terms and conditions that can be found on the digital market place

Customer Responsibilities

The control and management of access and responsibilities for end users including appropriate connectivity, security and accreditation if required. Where access is required over PSN, the Customer is responsible for adhering to the Code of Connection and assigning appropriate IP addresses from their own allocation to their services hosted on the Sungard platform.

Details of Sungard AS' Managed Cloud Services for UK Government customer responsibilities are in the terms and conditions that can be found on the digital market place.

Technical Requirements

Customers will require appropriate network connectivity such as internet access (IL0-IL2) or accredited connectivity such as a government secure network (IL3) to the Sungard Cloud Platforms.

Connectivity via the internet, a government secure network (PSN,) or private leased line is available but may incur additional charges.

Where required, Customers are responsible for procuring and managing appropriate devices or software to meet the requirement for data security over the various forms of connectivity.

IL2

- Standard Internet connectivity over common protocols (HTTP, HTTPS, SSH, etc.)
- Secure commercial grade VPN
  - Self-managed Site-to-Site IPSEC VPN to the compute environment
  - Self-managed SSL VPN to the compute environment
- PSN - You might need to assign part of your PSN IP allocation to your services
- CAS(T) using CPA/PEPAS overlay encryption

IL3

- Preferred connectivity is over a Government Secure Network such as GSI or PSN
- PSN/GSI - You might need to assign part of your PSN/GSI IP allocation to your services
- PSN or CAS(T) Leased Line (IL3 over IL2)
  - CPA/PEPAS approved solution providing overlay encryption (e.g. Cisco ISR/ASR)
- IL0 (e.g. Internet or non CAS(T) circuit) to IL3 VPN
  - Site-to-Site VPN using CAPS approved solutions (e.g. Ultra AEP Xcryptor)
  - CPA assured solution where Foundation Grade assurance is appropriate (e.g. Cisco ISR/ASR)
- IL3 Leased Line (assured network connection)

Trial Services

Civica may, on a case-by-case basis, agree to allow the purchaser a limited trial use of the software on their own facilities before purchasing, consisting of a time limited license to use the software in a non-production environment.

Additional Services

Reference to our G-Cloud Specialist Services Service Description

In order to enable the successful delivery and commissioning of the FILETRAIL solution, we can provide consultancy support to the customer in the following areas:

- Customer side Installation, integration and configuration services
- Customer side testing
- Training
- Product use instructions
- Enhanced DR Capability
- Project Management and Business Change consultancy relating to the SaaS service

Civica Cloud-based photo and video forensic analysis using MXSERVER:

...in partnership with Allevate and SUNGARD® AVAILABILITY SERVICES™

Find People Fast in Videos and Photos Using Cloud-Enabled Media Analysis Incorporating Face Recognition

Photo and Video Forensic Analysis Service Definition

Sub-contractors:

Allevate Limited

(http://allevate.com)

Sungard Availability Services

(http://www.sungardas.co.uk)

Table of Contents

Photo and Video Forensic Analysis Service Overview

Civica offers a solution to Find People Fast in Videos and Photos Using Cloud-Enabled Media Analysis Incorporating Face Recognition, build on MXSERVER offered by Allevate hosted on secure PaaS supplied by Sungard Availability Services.

1.10 The Need

Growing security concerns arising from increasing terrorist attacks, racial and ethnic disturbances, organised civil unrest, random violence, riots, burglary and physical assaults are necessitating solutions to unlock intelligence from multimedia.

The quantity of digital media has massively increased due to the ubiquity of CCTV, smart phones and other portable devices. Law enforcement and intelligence agencies have amassed large collections of video and photographs from sources such as:

- Digital Forensics:
  - Computer hard drives
  - Mobile phones and portable cameras
  - Flash memory devices
- Online sources on the Internet such as Facebook and YouTube
- CCTV
- Body Worn Video
- Members of the Public

However, there is no easy and cost-effective way to access the potential intelligence bonanza this multimedia contains; experienced and expensive human capital must be assigned to rote tasks of watching countless of hours of media in the hope of finding useful information.

A solution to automate this processing to quickly and efficiently unlock actionable intelligence from this staggering amount of data is required. The potential to improve public safety whilst simultaneously enabling more efficient use of public finances is significant.

1.11 MXSERVER Overview

MXSERVER processes vast amounts of textual, video and photo collections quickly – automatically discovering, grouping and extracting segments depicting people. Using face recognition technology, this solution searches media archives to find other assets which depict individuals of interest. It also enables digital media content to be efficiently searched, previewed and analysed via an intuitive web-based user interface. Results become available in minutes rather than hours or days because the digital media files are processed in parallel over a distributed cloud architecture.

MXSERVER applies data mining principles to digital media:

- Automatically find and match faces from huge stores of videos and photos
- Identify individuals from watchlists and track them across multiple videos
- Extract faces from video and automatically cross-reference with all other video
- Associate multiple videos and photos based upon their active content and the individuals they contain

- Apply enhanced link analysis to identity an individual across multiple video sources
- Automatically build links between different individuals based on their associations in media, whether they are known or unknown
- Automatically and graphically display web-based drill down link analysis diagrams
- Determine "Pattern of Life" analysis for specific individuals and flag deviations from the norm
- Manage and access your entire video and photo repository from a single web interface. (automatically transforming multiple video formats)
- Apply powerful analytical tools to your digital media content

Work more efficiently. Connect the dots. Get more results. Exploit the masses of raw media from multiple sources to create actionable intelligence with less manpower.

Additionally, MXSERVER can process live video in real-time to raise alerts if individuals in the video are matched against a watchlist of persons of interest.

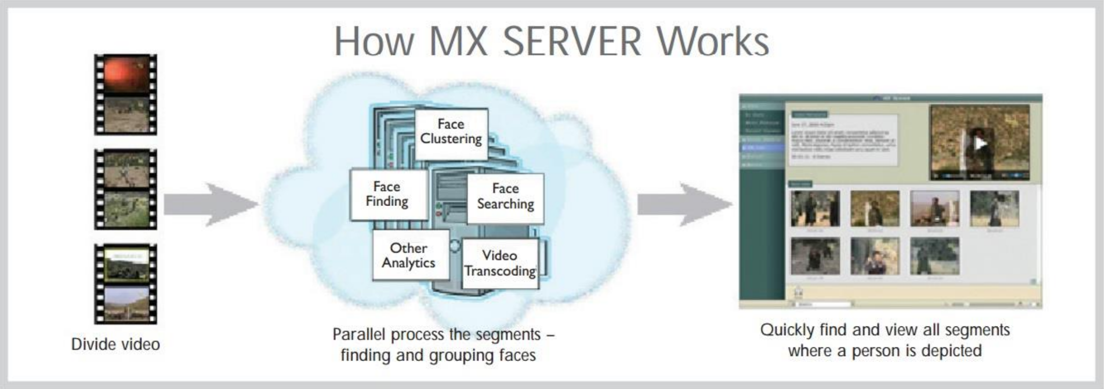
1.12 Proven Deployments with US Federal Agencies

MXSERVER is being utilised by Defence, Intelligence and Law Enforcement organisations and has proven its ROI to these customers over the past many years. MXSERVER's Cloud and Web-based architecture has been operationally proven to scale from small dual-server configurations to as large as thirty-two server installations. MXSERVER can be right-sized to meet an organisation's current processing needs and is flexible to be incrementally scaled to meet future demand.

Customers include:

- United States Department of Defence (multiple) – due to confidentiality agreements the names of these organisations who are operationally using MXSERVER cannot be publically disclosed. Government-to-government communications can be facilitated on a case-by-case basis
- West Virginia Fusion Centre – The West Virginia Intelligence Fusion Centre facilitates the collaboration of local, state, and federal law enforcement, public safety agencies, and the private sector in order to protect citizens. It is currently using MXSERVER to create a searchable repository utilizing mug shots and faces extracted from photographs and videos

1.13 How MXSERVER Works


How MX SERVER Works
Face Clustering
Face Finding
Face Searching
Other Analytics
Video Transcoding
Divide video
Parallel process the segments – finding and grouping faces
Quickly find and view all segments where a person is depicted

1.14 Benefits of MXSERVER

Expand on Available Intelligence

Extends an organization’s intelligence-base by transforming video, audio and photograph collections into searchable resources.

Increase Productivity

60:1 force-multiplier – saving countless man hours by:

- Searching the contents of digital media collections in an automated fashion
- Eliminating the need to manually view video and photo collections to locate the segment(s) of interest
- Automatically finding and saving occurrences of people in video and photos
- Sharing the results of previous analysis across the enterprise

Cloud Computing Power

Running on Sungard AS PaaS Assured or Protected Zone, MXSERVER’s powerful processing engine enables greater speed, capacity and scalability to process ever larger repositories of media.

Integrate Open Platforms and Increase Information Sharing

Integrate MXSERVER into your digital media and identification systems architecture and greatly add value to your analytical and media management platforms.

Learn more at: http://allevate.com/index.php/2013/08/01/intelligence-and-efficiency-through-on-demand-media-analysis-using-face-recognition/

Information Assurance

Civica partners with Sungard AS who provides a Managed Cloud Service for UK Government connected and compliant to PSN Code of Connection and Service Provision, the infrastructure platform over which the service will run.

The service can be run either in the Assured or Protected Zones that are connected to PSN Assured and PSN Protected Respectively with additional options of an Internet breakout in the Assured Zone only.

Sungard AS’ Government Cloud is hosted in the UK only. The service is supported by a dedicated SC Cleared UK based service operations team with staff background checks in accordance with BS7858:2012,

The service is aligned to the CESG Cloud Security Principles.

Sungard AS has ISO 9001:2008 and ISO/IEC 27001 certification and BS 25999-2:2007 certification.

Back-up / Restore Recovery Level

Details of Sungard AS' Managed Cloud Services for UK Government back-up and recovery service can be found in the service definition and terms and conditions that can be found on the digital market place.

On-Boarding / Off Boarding Process

On-boarding and Off-boarding processes/scope etc.

On-boarding

Details of Sungard AS' Managed Cloud Services for UK Government on-boarding service can be found in the service definition and terms and conditions that can be found on the digital market place

.Off-boarding

Details of Sungard AS' Managed Cloud Services for UK Government off-boarding service can be found in the service definition and terms and conditions that can be found on the digital market place

Pricing

1.15 SaaS Pricing

The service consists of the sale of a non-exclusive license to install and use the MXSERVER software described herein on a monthly subscription basis, using Sungard AS' Managed Cloud Services for UK Government.

We have developed a standard pricing/performance model that can be applied to estimate the cost of an MXSERVER deployment based upon digital media processing requirements. The pricing model is made up of a base package plus additional scaling units, as required. The base package includes a system meeting the minimum recommended configuration and the incremental expansion unit includes the components necessary to add additional MXSERVER Workers to meet projected processing workloads.

Full costs can be found in the pricing schedule.

1.16 Software Licensing Pricing Variability

Pricing is dependent upon exact client requirements. In the absence of specific client requirements, the above pricing for software licensing is indicative.

For example, software licensing can vary with licensing of alternative or additional 3rd party software components, such as face recognition matching SDKs or additional matching capability such a logo detection.

Additionally, software licensing pricing may also vary with the number of months the purchaser commits to the service, as well as the number of Additional Scaling Units (if any) subscribed to.

An exact quote can be provided after an initial consultation with the purchaser.

1.17 Required Professional Services

The stated software licensing prices exclude any required professional services for:

- Software installation, configuration and commissioning.
- Bespoke development required to adhere to specific and agreed customer requirements.
- Integration with external and 3rd party systems.
- Training on use of the MXSERVER.

Refer to Section 0 - Additional Services.

Cost / Benefit Considerations

The cost / benefit of this monthly expenditure can easily be quantified.

- Each employed human can watch realistically approx. 5-6 hours of video per day on the days which they are working
- The base-package can process 100 hours of video per day, each and every day, thereby freeing up human beings to analyse the system's reported results

1.18 Annual Support and Maintenance

Support and Maintenance and help desk is included in the service price.

Service Management Details

1.19 Support and Maintenance

The monthly subscription includes support and maintenance.

Support and maintenance includes:

- Free software upgrades (including patches and updates).
- Fault / bug reporting and resolution. (via email)
- Logging of enhancement requests. (via email)
- Access to 1st line Help Desk
    - Telephone: Mon-Fri 9-5 excluding holidays

Support and maintenance excludes:

- Customer side Installation, integration and configuration services (can be covered by Additional Services)
- Training (can be covered by Additional Services)
- Product use instructions (can be covered by Additional Services)

Service Constraints

“Planned Maintenance” means any pre-planned maintenance of any infrastructure relating to the Services. Civica shall provide the Customer with at least twenty-four (24) hours’ advance notice of any such planned maintenance:

Planned maintenance of Sungard’s infrastructure relating to the Services shall happen between the hours of 00:00 and 06:00 (UK local time) Monday to Sunday and/or between the hours of 08:00 and 12:00 (UK local time) on a Saturday and/or Sunday. No planned maintenance will take place on a Saturday unless agreed in advance by both parties;

Planned Maintenance shall be excluded from any availability calculation in regard to service credits but shall be included in the monthly service reporting;

“Emergency Maintenance” means any emergency maintenance of any of the infrastructure relating to the Services. Whenever possible, Sungard shall provide the Client with at least six (6) hours’ advance notice:

Whenever possible Emergency Maintenance of Sungard’s infrastructure will happen between the hours of 00:00 and 06:00 (UK local time) Monday to Sunday and/or between the hours of 08:00 and 12:00 (UK local time) on Saturday and/or Sunday unless there is an identified and demonstrable immediate risk to a Clients environment;

Emergency Maintenance shall be excluded from any availability calculation in regard to service credits but shall be included in the monthly service reporting.

This is from page 6 of Sungard AS’ Managed Cloud Services for UK Government Terms and Conditions.

9. VDC Infrastructure and Maintenance

From time to time, Sungard AS may need to perform maintenance on or make adjustments to the infrastructure (including without limitation, any Sungard AS provided telecommunications links, Sungard AS Equipment and Sungard AS Software, on which the Customer VDC(s) relies and shall be entitled to do so at its discretion, without incurring liability for so doing. In the event of any such maintenance or adjustment being needed, then except in the case of emergency maintenance, Sungard AS will give the Customer reasonable prior notice and shall use all reasonable endeavours to limit the interruption. If emergency maintenance is needed, Sungard AS shall be entitled to interrupt services without prior notice.

Service Levels

- The Service is based on a Service Level Availability (SLA) of 99.95%
- Civica will endeavour to respond to all incidents within 4 Hours
- Service Credits are not offered against this Service offering

Details of Sungard AS’ Managed Cloud Services for UK Government infrastructure/platform SLA can be found in the service definition and terms and conditions that can be found on the digital market place

.

Termination Terms

Terms

The Customer and Civica agree to a monthly subscription.

Customer and Civica will also agree to a minimum number of month's commitment. The agreement will terminate on the last day of the agreement, unless a request to extend the agreement is received within 7 working days in advance.

Either party may terminate at any time if the other party is in material breach of agreement.

At the point of termination, all consumer data, accounts and access will be permanently deleted, and will not be able to be subsequently recovered or restored.

Costs

There are no termination costs for this Service. Consumers are responsible for extracting their own data from the platform if required.

Sungard may make an additional charge for transferring data out of the service.

Data Restoration / Service Migration

- Data will be restored following a data restore request within 24 hours.
- No Service Migration capability is offered as part of this Service offering

Details of Sungard AS' Managed Cloud Services for UK Government RPO/RTO SLA. can be found in the service definition and terms and conditions that can be found on

Customer Responsibilities

The control and management of access and responsibilities for end users including appropriate connectivity, security and accreditation if required. Where access is required over PSN, the Customer is responsible for adhering to the Code of Connection and assigning appropriate IP addresses from their own allocation to their services hosted on the Sungard platform.

Details of Sungard AS' Managed Cloud Services for UK Government customer responsibilities are in the terms and conditions that can be found on the digital market place

Technical Requirements

Customers will require appropriate network connectivity such as internet access (IL0-IL2) or accredited connectivity such as a government secure network (IL3) to the Sungard Cloud Platforms.

Connectivity via the internet, a government secure network (PSN,) or private leased line is available but may incur additional charges.

Where required, Customers are responsible for procuring and managing appropriate devices or software to meet the requirement for data security over the various forms of connectivity.

IL2

- Standard Internet connectivity over common protocols (HTTP, HTTPS, SSH, etc.)
- Secure commercial grade VPN
  - Self-managed Site-to-Site IPSEC VPN to the compute environment
  - Self-managed SSL VPN to the compute environment
- PSN - You might need to assign part of your PSN IP allocation to your services
- CAS(T) using CPA/PEPAS overlay encryption

IL3

- Preferred connectivity is over a Government Secure Network such as GSI or PSN
- PSN/GSI - You might need to assign part of your PSN/GSI IP allocation to your services
- PSN or CAS(T) Leased Line (IL3 over IL2)
  - CPA/PEPAS approved solution providing overlay encryption (e.g. Cisco ISR/ASR)
- IL0 (e.g. Internet or non CAS(T) circuit) to IL3 VPN
  - Site-to-Site VPN using CAPS approved solutions (e.g. Ultra AEP Xcryptor)
  - CPA assured solution where Foundation Grade assurance is appropriate (e.g. Cisco ISR/ASR)
- IL3 Leased Line (assured network connection)

Trial Services

Civica may, on a case-by-case basis, agree to allow the purchaser a limited trial use of the software on their own facilities before purchasing, consisting of a time limited license to use the software in a non-production environment.

Additional Services

Reference to our G-Cloud Specialist Services Service Description

In order to enable the successful delivery and commissioning of the MXSERVER solution, we can provide consultancy support to the customer in the following areas:

- Customer side Installation, integration and configuration services
- Customer side testing
- Training
- Product use instructions
- Enhanced DR Capability
- Project Management and Business Change consultancy relating to the SaaS service

Appendix: About Allevate and Tygart Technology

About Allevate

Allevate Limited (http://allevate.com) was founded in 2007 in England. Allevate's mission is to enhance public safety and improve public sector efficiency through the sale and implementation of biometric identification solutions, focusing on government, law enforcement, border control and transport.

Allevate seeks to improve society by building and selling propositions to government agencies to ensure a more efficient use of public finances whilst making society safer and more secure.

Alevites' Partner: Tygart Technology

Tygart Technology Inc. (http://www.tygart.com) was founded in 1992 in West Virginia. Tygart designs and develops commercial software products and provides an array of Information Technology (IT) consulting services for state and federal government clients.

Tygart is the developer of MXSERVER, a solution for automated face finding and matching. It transforms video, audio & photo collections into actionable intelligence for law enforcement agencies.

Tygart's existing customers include:

- US Department of Defence
- US FBI
- Various (confidential) US Intelligence Agencies
- US General Services Administration
- US Department of State
- US Army
- State of West Virginia

Forensic Image Scanning Hub

Civica Cloud-based forensic image scanning hub using FISH:

Gather, transmit and process fingerprints, photographs and videos with accuracy and full audit trail

Sub-contractors:

Sungard Availability Services (http://www.sungardas.co.uk)

Table of Contents

2. Photo and Video Forensic Analysis Service Overview

Civica offers a solution to gather, transmit and process fingerprints, photographs and video with high accuracy utilising FISH.

Hosted on secure PaaS supplied by Sungard Availability Services.

2.1 The Need

Growing security concerns arising from increasing terrorist attacks, racial and ethnic disturbances, organised civil unrest, random violence, riots, burglary and physical assaults are necessitating solutions to unlock intelligence from multimedia.

The quantity of digital media has massively increased due to the ubiquity of CCTV, smart phones and other portable devices. Law enforcement and intelligence agencies have amassed large collections of video and photographs from sources such as:

- Digital Forensics:
- Computer hard drives
- Mobile phones and portable cameras
- Flash memory devices
- Online sources on the Internet such as Facebook and YouTube
- CCTV
- Body Worn Video
- Members of the Public

However, there is no easy and cost-effective way to access the potential intelligence bonanza this multimedia contains; experienced and expensive human capital must be assigned to rote tasks of watching countless of hours of media in the hope of finding useful information.

A solution to automate this processing to quickly and efficiently unlock actionable intelligence from this staggering amount of data is required. The potential to improve public safety whilst simultaneously enabling more efficient use of public finances is significant.

2.2 FISH Overview

FISH Digital Forensics (DF) is a suite of applications to enable fingerprints and other images to be gathered, transmitted and processed in a highly accurate scientific and audited manner. FISH DF manages the capture of images at the scene of crime using mobile phones, laptops, tablets or digital cameras, and then allows the transmission back to the forensics departments for experts to make determinations whilst complying with the new standard ISO 17025. FISH DF has a comprehensive reporting tool that can visually (displayed on wallboards) inform both management and experts who either choose or be allocated work determined by real time operational priorities. Innovative tools like the Comparator enable experts to make faster determinations and can be integrated with force/agency systems including AFIS and Case Management.

FISH DF is a transformational technology enabling the drivers of regional collaboration to be achieved whilst providing the mechanisms of achieving cost reductions, increasing efficiency and effectiveness within the forensic environment.

FISH DF technology has enabled and supported regional collaborations within the East Midlands and Yorkshires and has been adopted by the FBI, USA, the Italian Ministry of Interior and a large number of UK forces.

FISH DF has a unique pedigree in managing images having evolved from software developed for FujiFilm worldwide for harvesting, processing and printing digital photos in the photo finishing industry, processing over 1.5 billion photographs in 2006 for companies such as Walmart, Walgreens and Boots.

2.3 Proven Deployments

FISH is being utilised by a number of UK Police Forces and by the FBI

UK customers include the following Forces:

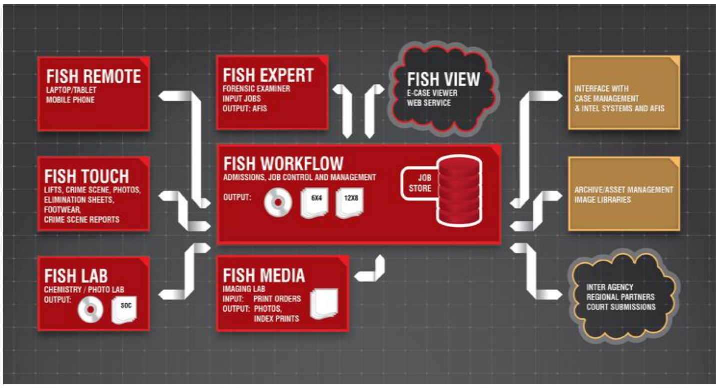
- West Yorkshire
- Cheshire
- South Wales
- West Midlands
- EMSOU

2.4 How FISH Works

- **FISH Modules**

FISH is split into a number of modules providing functionality around submission, processing and reporting.

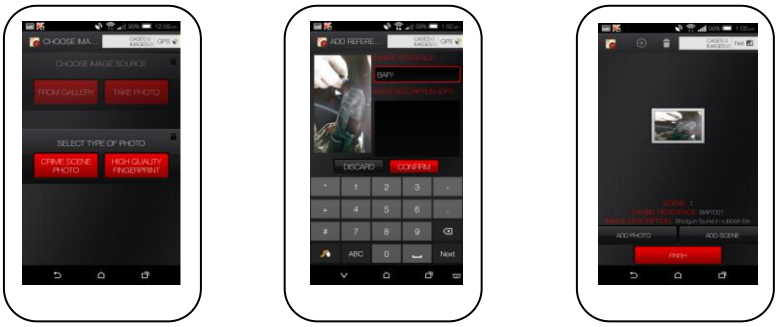
The main functions are displayed opposite and include FISH Remote, Touch and Lab for submissions, FISH Expert, Workflow and Media for processing, web based FISH View for eForensics and Image Management, various interfaces to case management and other force applications. Inter-agency interaction includes reporting and sharing of evidence.



- **FISH Remote/Mobile**

FISH Remote enables the capture and transmission of scene photographs and fingerprints straight from the scene allowing the fast track of cases and assisting in early detection of offenders and recovery of property.

Scene of crime and exhibit details are logged, fingerprint lifts, scene and entirety photo's captured using either tablet or mobile phone and transmitted directly to the FISH Workflow for processing.



Mobile screen examples showing mark capture from the scene to

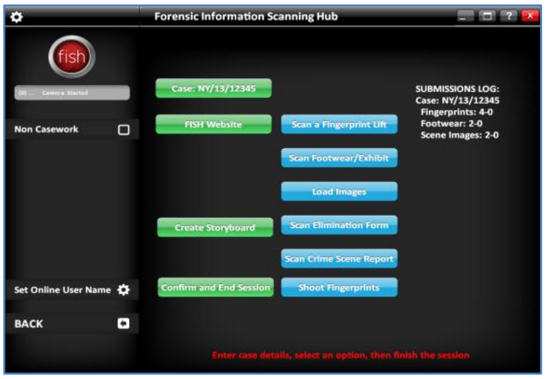
- **FISH Touch**

FISH Touch enables the capture and transmission of high quality scene photographs, fingerprint lifts, elimination fingerprint forms, footwear images and documents from CSI bases.

Photographs can be imported directly from camera cards. Fingerprints, footwear and documents can be scanned using high quality scanners or captured via tethered camera work stations for high speed input.

Submissions are transmitted directly into the FISH Workflow for processing from any CSI base or designated location.

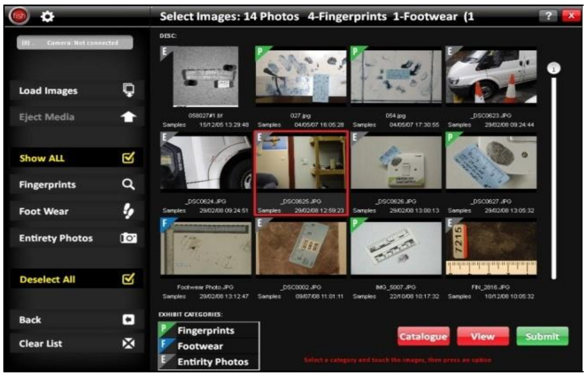
Supports any number of CSI bases regardless of location and is ideal for collaboration and regionalisation projects. Submissions can be sent as master and working copies to one or any number of locations determined by the force or agency requirements.



Forensic Information Scanning Hub

SUBMISSIONS LOG:
Case: NY/13/12345
Fingerprints: 4-0
Footwear: 2-0
Scene Images: 2-0

Enter case details, select an option, then finish the session



Select Images: 14 Photos 4-Fingerprints 1-Footwear (1

Select a category and touch the images, then press an option

fish
(0) ... Camera: Not connected
DESC
Load Images
Eject Media
Show ALL ☑
Fingerprints
Foot Wear
Entirety Photos
Deselect All ☑
Back
Clear List
058027#1.tif Samples 15/12/05 13:29:48
027.jpg Samples 04/05/07 16:05:28
054.jpg Samples 04/05/07 17:30:55
_DSC0623.JPG Samples 29/02/08 09:24:44
_DSC0624.JPG Samples 29/02/08 09:24:51
_DSC0625.JPG Samples 29/02/08 12:59:23
_DSC0626.JPG Samples 29/02/08 13:00:13
_DSC0627.JPG Samples 29/02/08 13:05:32
Footwear Photo.JPG Samples 29/02/08 13:12:47
_DSC0002.JPG Samples 09/07/08 11:01:11
IMG_5007.JPG Samples 22/10/08 10:17:32
FN_2816.JPG Samples 10/12/08 10:05:32
EXHIBIT CATEGORIES:
P Fingerprints
F Footwear
E Entirity Photos
Catalogue
View
Submit

FISH Touch Submission Screens

- **FISH Lab**

FISH Lab enables the capture and transmission of photographed fingerprint exhibits or can be integrated with lab systems such as Syntronics RUVIS cameras and Foster+Freeman DCS for the submission of images to the FISH Workflow for processing. Alternatively images can be printed at 1:1 scaling.

Supports single or regional collaborations regardless of location.

- **FISH Workflow/Workflow Server**

FISH Workflow is the heart of processing and reporting within FISH. For single workflow installations it can be run on a desktop but to fully utilise its functionality the FISH Workflow Server is recommended typically running on a secure robust server.

The FISH Workflow Server enables the users to access a full suite of functions including complete image management, full interactive reporting functionality and is strongly recommended for any collaboration projects.

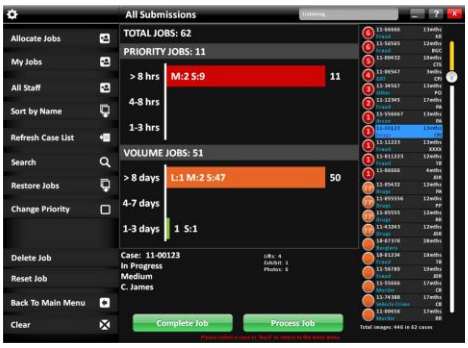
FISH Workflow can be configured to suit any force or agency requirements. Regional areas and teams can be created with overall or individual management. Jobs can be allocated by team leaders/management or left for the individuals to pick and self-allocate the next case for processing.

Multiple sub workflows can be configured to automatically control specific submissions to different departments such as footwear, fingerprints, imaging and eForensics.

Cases can be prioritised in line with force or agency priorities such as serious/major crime and volume crime.

Additional submissions are automatically associated with existing case submissions. Once the case work is complete the submissions are archived and can subsequently be restored into the workflow as required.

Integration with existing force case management and asset management systems is actively encouraged.

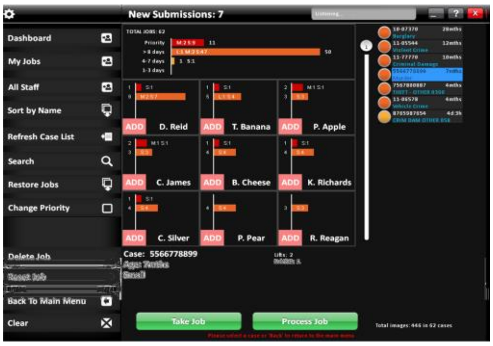


Case: 11-00123
In Progress
Medium
C. James

Lifts: 4
Exhibit: 1
Photos: 6

Total images: 446 in 62 cases

Workflow Dashboard All Cases

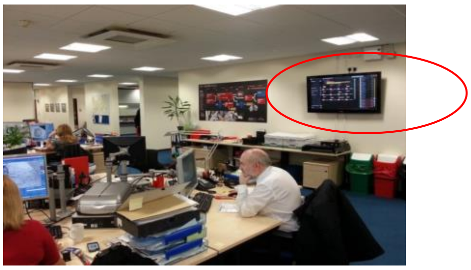


Case: 5566778899

Lifts: 2

Total images: 446 in 62 cases

Workflow Dashboard Allocated Cases

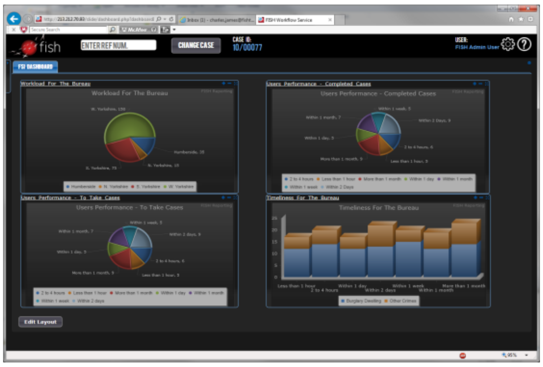


Dashboards

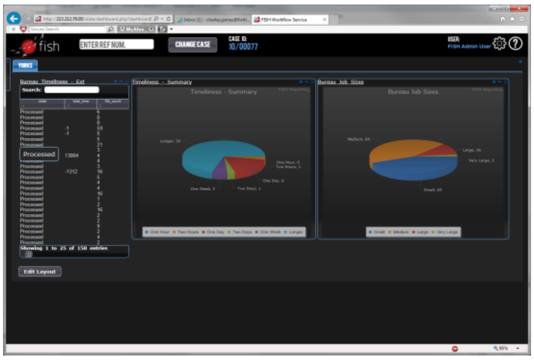
The Dashboard enables the workflow to be displayed on large screens within a bureau or designated area, to give users and managers a quick live view around the overall status of the incoming work.

Reports

A suite of reports are available through the Workflow Server which can be created and structured around force/agency requirements and associated to different levels of user permissions through to senior user or management requirements.



Generated Report Examples



- **FISH Expert/Comparator**

  FISH Expert enables examiners to access cases in the workflow for processing. With the addition of the FISH Comparator, images can be assessed, analysed, compared, evaluated and reported to officers and the Courts.

  Cases are selected for processing utilising a suite enhancement tools and direct submission to AFIS for searching or printed out for comparison if required.

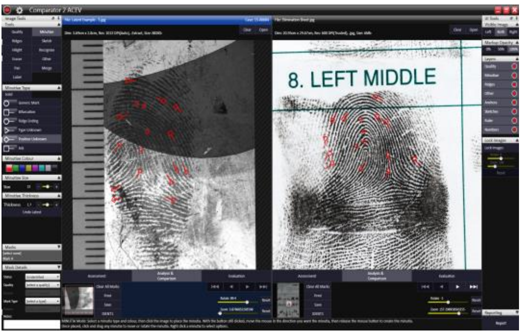
  With the use of Comparator ACE/V, cases and images can be processed in line with ISO 17025 requirements. This can be incorporated within FISH Expert or be provided as a standalone solution.

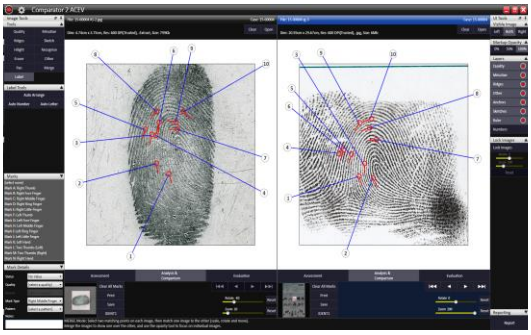
  A full range of enhancement and comparison tools are available within the Comparator which includes image colour manipulation, marking up of features, note taking, recording fingerprint characteristics and enabling full side by side comparison of latent's against elimination forms or digitally captured fingerprint forms from a database.

  Streamlined Forensic Reports can be tailored to the force/agency requirements and can be either printed out, emailed or used as an automated visual report around the image comparison sequence, for court presentations.

  FISH Expert enables the processing of cases from one location which can be sighted anywhere within a region or country as required. Ideal for single force/agency processing or regional and collaboration projects.

Side by Side Comparison





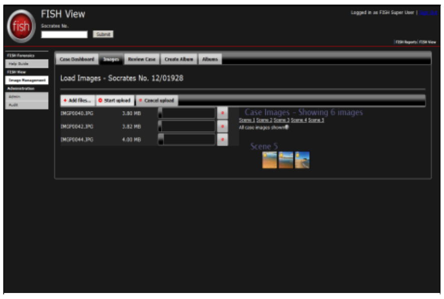
Comparison Chart/Report

- **FISH View and FISH Media**

FISH View and FISH Media are both designed to support the submission, viewing, printing and management of digital imagery.

FISH View works in conjunction with the FISH Workflow Server providing browser based viewing, uploading, asset management and printing of images. It supports multiple image formats displayed in multiple resolutions which can be viewed according to assigned permissions and access rights. The printing service allows CSIs and officers to request remote printing as albums from a central imaging department.

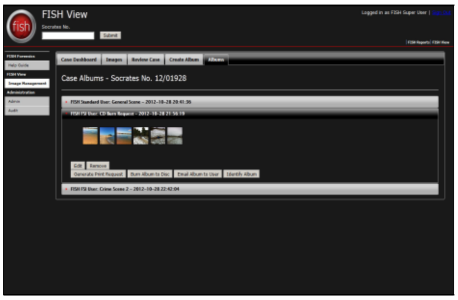
Bulk uploading of images using a browser or a FISH submission module such as FISH Photo provides a quick and efficient solution while meeting the auditing and continuity requirements of a forensic lab.



Load Images - Socrates No. 12/01928

IMGP0040.JPG 3.80 MB
IMGP0042.JPG 3.82 MB
IMGP0044.JPG 4.00 MB

Case Images – Showing 6 images
Scene 1 Scene 2 Scene 3 Scene 4 Scene 5
All case images shown
Scene 5



Case Albums - Socrates No. 12/01928

FISH Standard User: General Scene – 2012-10-28 20:41:36
FISH FSI User: CD Burn Request – 2012-10-28 21:56:19
FISH FSI User: Crime Scene 2 – 2012-10-28 22:42:04

Case Detail View

Images Selected for Court Album

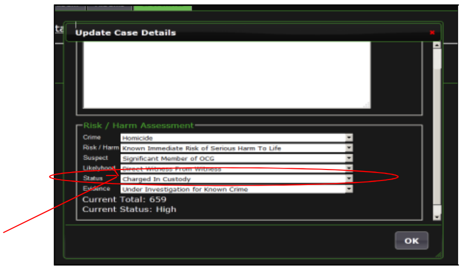
- **FISH eForensics**

The FISH eForensics functionality is designed to manage the submission and triage of items and images for analysis through to result reporting to officers. This is typically used for analysing mobile phones and computers.

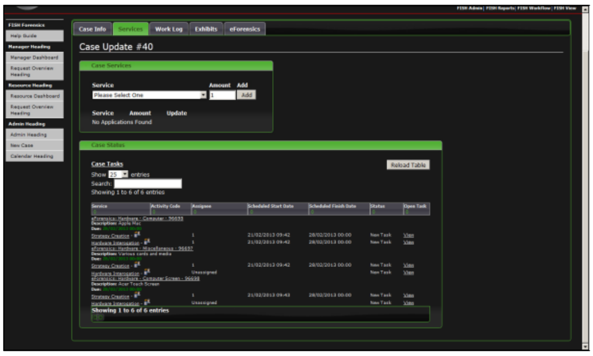
The authorising officer completes a request for submission which includes a prioritisation matrix ensuring the evidential value and priority of the case. A risk/harm assessment also takes place giving the submission a score rating determining the time investment and examination approach.

Images can be uploaded or recorded at every stage of the examination which is particularly useful at the triage stage. There are two workflow dashboards available for technicians and managers providing the ability to track cases and tasks in progress

Images can be viewed by the investigating officers and reports can be generated on completion



Risk / Harm Assessment
Crime: Homicide
Risk / Harm: Known Immediate Risk of Serious Harm To Life
Suspect: Significant Member of OCG
Likelihood: Direct Witness From Witness
Status: Charged In Custody
Evidence: Under Investigation for Known Crime
Current Total: 659
Current Status: High



Case Update #40

Case Services

Service: Please Select One Amount: 1

Service Amount Update
No Applications Found

Case Status

Case Tasks
Show 25 entries
Search:
Showing 1 to 6 of 6 entries

Service	Activity Code	Assignee	Scheduled Start Date	Scheduled Finish Date	Status	Open Task
eForensics: Hardware - Computer - 96693 Description: Apple Mac Due: 28/02/2013 00:00						
Strategy Creation -		1	21/02/2013 09:42	28/02/2013 00:00	New Task	View
Hardware Interrogation -		1	21/02/2013 09:42	28/02/2013 00:00	New Task	View
eForensics: Hardware - Miscellaneous - 96697 Description: Various cards and media Due: 28/02/2013 00:00						
Strategy Creation -		1	21/02/2013 09:42	28/02/2013 00:00	New Task	View
Hardware Interrogation -		Unassigned			New Task	View
eForensics: Hardware - Computer Screen - 96698 Description: Acer Touch Screen Due: 28/02/2013 00:00						
Strategy Creation -		1	21/02/2013 09:43	28/02/2013 00:00	New Task	View
Hardware Interrogation -		Unassigned			New Task	View

Showing 1 to 6 of 6 entries

Prioritisation Matrix and Risk/Harm Assessment

2.5 Benefits of FISH

FISH DF enables costs to be reduced and benefits realised around single or regional solutions for CSI, Lab and Scene Mobile submissions, speedier fingerprint, footwear, documents, photographs, video and CCTV analysis and reporting, tracking, management and reporting for forensic and multi-media submissions.

The main benefits include:-

- Simple to use, intuitive “big buttons” and drag and drop technology
- Speedy CSI fingerprint submissions from the scene of crime using mobile technology.
- Quality submissions from CSI bases and chemical treatment labs for latent fingerprints, photo's, fingerprint forms and documents.
- Reduction in the printing out of images by enabling on screen comparisons.
- Efficient speedy processing within Fingerprint Bureaux, including individual or allocated case processing, on screen analysis, comparison and verification, direct submission to AFIS and reporting to Police Officers and the Courts.
- Enabling quicker detection of offenders and potential recovery of property.
- Supporting ISO 17025 through specifically designed Comparator.
- Easy case tracking and management using dashboard technology.
- Easy management and processing of digital evidence and creation of albums for court.
- On line secure eForensics submissions, tracking, processing including triage and reporting.
- Auditable eForensic submissions including a prioritisation matrix incorporating a risk/harm assessment.

FISH also encourages Users to Improve Productivity

- Prevents the conflicts that can occur through the 'cherry picking' of jobs, yet supports self-allocation of work and allows users to plan personal workload for the shift
- Reduces demand on general computer skills from workforce, for example file handling and navigation around the application; complements the newer IT skill sets and experience whilst supporting the more experienced fingerprint experts
- Automates repetitive steps and reduces human errors

3. Information Assurance

Civica partners with Sungard AS who provides a Managed Cloud Service for UK Government connected and compliant to PSN Code of Connection and Service Provision, the infrastructure platform over which the service will run.

The service can be run either in the Assured or Protected Zones that are connected to PSN Assured and PSN Protected Respectively with additional options of an Internet breakout in the Assured Zone only.

Sungard AS' Government Cloud is hosted in the UK only. The service is supported by a dedicated SC Cleared UK based service operations team with staff background checks in accordance with BS7858:2012,

The service is aligned to the CESG Cloud Security Principles.

Sungard AS has ISO 9001:2008 and ISO/IEC 27001 certification and BS 25999-2:2007 certification.

4. Back-up / Restore Recovery Level

Details of Sungard AS’ Managed Cloud Services for UK Government back-up and recovery service can be found in the service definition and terms and conditions that can be found on the digital market place.

5. On-Boarding / Off Boarding Process

On-boarding and Off-boarding processes/scope etc.

On-boarding

Details of Sungard AS' Managed Cloud Services for UK Government on-boarding service can be found in the service definition and terms and conditions that can be found on the digital market place.

Off-boarding

Details of Sungard AS' Managed Cloud Services for UK Government off-boarding service can be found in the service definition and terms and conditions that can be found on the digital market place

6. Pricing

6.1 SaaS Pricing

The service consists of the sale of a non-exclusive license to install and use the FISH software described herein on a monthly subscription basis, using Sungard AS' Managed Cloud Services for UK Government.

We have developed a standard pricing/performance model that can be applied to estimate the cost of an FISH deployment based upon digital media processing requirements. The pricing model is made up of a base package plus additional scaling units, as required. The base package includes a system meeting the minimum recommended configuration. All additional modules at additional cost

Costs are detailed in the supplied price schedule

6.2 Software Licensing Pricing Variability

Pricing is dependent upon exact client requirements. In the absence of specific client requirements, the above pricing for software licensing is indicative.

Additionally, software licensing pricing may also vary with the number of months the purchaser commits to the service, as well as the number of Additional Scaling Units (if any) subscribed to.

An exact quote can be provided after an initial consultation with the purchaser.

6.3 Required Professional Services

The stated software licensing prices exclude any required professional services for:

- Software installation, configuration and commissioning.
- Bespoke development required to adhere to specific and agreed customer requirements.
- Integration with external and 3rd party systems.
- Training on use of the FISH.

6.4 Annual Support and Maintenance

Support and Maintenance and help desk is included in the service price.

6.5 Support and Maintenance

The monthly subscription includes support and maintenance.

Support and maintenance includes:

- Free software upgrades (including patches and updates).
- Fault / bug reporting and resolution. (via email)
- Logging of enhancement requests. (via email)
- Access to 1st line Help Desk
  - Telephone: Mon-Fri 9-5 excluding holidays
  - email

Support and maintenance excludes:

- Customer side Installation, integration and configuration services (can be covered by Additional Services)
- Training (can be covered by Additional Services)
- Product use instructions (can be covered by Additional Services)

7. Service Constraints

“Planned Maintenance” means any pre-planned maintenance of any infrastructure relating to the Services. Civica shall provide the Customer with at least twenty-four (24) hours’ advance notice of any such planned maintenance:

Planned maintenance of Sungard’s infrastructure relating to the Services shall happen between the hours of 00:00 and 06:00 (UK local time) Monday to Sunday and/or between the hours of 08:00 and 12:00 (UK local time) on a Saturday and/or Sunday. No planned maintenance will take place on a Saturday unless agreed in advance by both parties;

Planned Maintenance shall be excluded from any availability calculation in regard to service credits but shall be included in the monthly service reporting;

“Emergency Maintenance” means any emergency maintenance of any of the infrastructure relating to the Services. Whenever possible, Sungard shall provide the Client with at least six (6) hours’ advance notice:

Whenever possible Emergency Maintenance of Sungard’s infrastructure will happen between the hours of 00:00 and 06:00 (UK local time) Monday to Sunday and/or between the hours of 08:00 and 12:00 (UK local time) on Saturday and/or Sunday unless there is an identified and demonstrable immediate risk to a Clients environment;

Emergency Maintenance shall be excluded from any availability calculation in regard to service credits but shall be included in the monthly service reporting.

This is from page 6 of Sungard AS’ Managed Cloud Services for UK Government Terms and Conditions.

9. VDC Infrastructure and Maintenance

From time to time, Sungard AS may need to perform maintenance on or make adjustments to the infrastructure (including without limitation, any Sungard AS provided telecommunications links, Sungard AS Equipment and Sungard AS Software, on which the Customer VDC(s) relies and shall be entitled to do so at its discretion, without incurring liability for so doing. In the event of any such maintenance or adjustment being needed, then except in the case of emergency maintenance, Sungard AS will give the Customer reasonable prior notice and shall use all reasonable endeavours to limit the interruption. If emergency maintenance is needed, Sungard AS shall be entitled to interrupt services without prior notice.

8. Service Levels

- The Service is based on a Service Level Availability (SLA) of 99.95%
- Civica will endeavour to respond to all incidents within 4 Hours
- Service Credits are not offered against this Service offering

Details of Sungard AS' Managed Cloud Services for UK Government infrastructure/platform SLA can be found in the service definition and terms and conditions that can be found on the digital market place

.

9. Termination Terms

Terms

The Customer and Civica agree to a monthly subscription.

Customer and Civica will also agree to a minimum number of month’s commitment. The agreement will terminate on the last day of the agreement, unless a request to extend the agreement is received within 7 working days in advance.

Either party may terminate at any time if the other party is in material breach of agreement.

At the point of termination, all consumer data, accounts and access will be permanently deleted, and will not be able to be subsequently recovered or restored.

Costs

There are no termination costs for this Service. Consumers are responsible for extracting their own data from the platform if required.

Sungard may make an additional charge for transferring data out of the service.

10. Data Restoration / Service Migration

- Data will be restored following a data restore request within 24 hours.
- No Service Migration capability is offered as part of this Service offering

Details of Sungard AS' Managed Cloud Services for UK Government RPO/RTO SLA. can be found in the service definition and terms and conditions that can be found on the digital market place

11. Customer Responsibilities

The control and management of access and responsibilities for end users including appropriate connectivity, security and accreditation if required. Where access is required over PSN, the Customer is responsible for adhering to the Code of Connection and assigning appropriate IP addresses from their own allocation to their services hosted on the Sungard platform.

Details of Sungard AS' Managed Cloud Services for UK Government customer responsibilities are in the terms and conditions that can be found on the digital market place

.

12. Technical Requirements

Customers will require appropriate network connectivity such as internet access (IL0-IL2) or accredited connectivity such as a government secure network (IL3) to the Sungard Cloud Platforms.

Connectivity via the internet, a government secure network (PSN,) or private leased line is available but may incur additional charges.

Where required, Customers are responsible for procuring and managing appropriate devices or software to meet the requirement for data security over the various forms of connectivity.

IL2

- Standard Internet connectivity over common protocols (HTTP, HTTPS, SSH, etc.)
- Secure commercial grade VPN
  - Self-managed Site-to-Site IPSEC VPN to the compute environment
  - Self-managed SSL VPN to the compute environment
- PSN - You might need to assign part of your PSN IP allocation to your services
- CAS(T) using CPA/PEPAS overlay encryption

IL3

- Preferred connectivity is over a Government Secure Network such as GSI or PSN
- PSN/GSI - You might need to assign part of your PSN/GSI IP allocation to your services
- PSN or CAS(T) Leased Line (IL3 over IL2)
  - CPA/PEPAS approved solution providing overlay encryption (e.g. Cisco ISR/ASR)
- IL0 (e.g. Internet or non CAS(T) circuit) to IL3 VPN
  - Site-to-Site VPN using CAPS approved solutions (e.g. Ultra AEP Xcryptor)
  - CPA assured solution where Foundation Grade assurance is appropriate (e.g. Cisco ISR/ASR)
- IL3 Leased Line (assured network connection)

13. Trial Services

Civica may, on a case-by-case basis, agree to allow the purchaser a limited trial use of the software on their own facilities before purchasing, consisting of a time limited license to use the software in a non-production environment.

14. Additional Services

Reference to our G-Cloud Specialist Services Service Description

In order to enable the successful delivery and commissioning of the FISH solution, we can provide consultancy support to the customer in the following areas:

- Customer side Installation, integration and configuration services
- Customer side testing
- Training
- Product use instructions
- Enhanced DR Capability
- Project Management and Business Change consultancy relating to the SaaS service

Managed Cloud Services
Official – Assured Zone
Platform-as-a-Service

In Partnership with

(http://allevate.com)

Sungard Availability Services (http://www.sungardas.co.uk)

Table of Contents

1. Service Description

Platform-as-a-Service is part of Sungard AS Managed Cloud Services for UK Government. This offering is specifically designed and available only for use by UK public sector organisations, or providers delivering services to the UK Public Sector to process data marked as Official (including Official-Sensitive).

Compliant PSN connectivity to the service is offered over the Public Services Network (PSN) ‘Assured’ WAN and the Internet for consumption of the services offered.

Sungard AS assigns each customer with one or more Virtual Data Centre(s) (VDC) comprising of the requisite compute, network and storage resources in resource pool(s) separate from other tenants. The VDCs are created in ‘zones’. The zones are:

- PSN ‘Assured’ zone which is connected to the PSN ‘Assured’ WAN
- Internet ‘Assured’ zone.

The PSN ‘Assured’ zone supports VDC’s deployed to this zone and VDC’s deployed to Internet ‘Assured’ zones. However, VDC’s cannot be connected to more than one of the aforementioned zones at any one time. Connectivity between zones can be offered via Connection Gateways.

Within the VDC(s) individual server instances are defined to run the operating system and application(s). These instances are on a Sungard AS dedicated, geographical and locally resilient UK Public Sector cloud infrastructure. Protection and separation between customers is enforced through virtualisation and the configuration of firewalls and other security management systems.

Sungard AS Security Cleared personnel manage the service using ISO 27001 assured processes and procedures from within our UK service operations centre.

Key Features include:

- Hosted within Sungard Availability Services operated UK data centres;
- Fully redundant multi-tenancy multi-site enterprise infrastructure;
- Supported by a dedicated UK-based Sungard AS Secure Cloud service operations team;
- Diverse connectivity to the Assured and Internet connectivity services at both sites;
- Reserved Public Services Network (PSN) bandwidth;
- Up to 99.99% Availability Service Level Agreement (SLA);
- Security Domain connection gateway;
- A range of virtual machine sizes;
- Managed Operating Systems;
- Dedicated physical server options;
- Flexible pricing options;
- Reduced Total Cost of Ownership and minimum commitments.

Example use cases:

Public Sector organisations or service providers seeking to offer application services to public sector organisations:

- requiring hosted environments for data classified as “Official including “Official-Sensitive” throughout the application lifecycle;
- requiring responsive deployments that provide scalable builds, release templates and cloning of environments;
- that require a fully Managed Service;
- seeking to reduce their overall costs and compliance risks;
- already using a UK government cloud service and looking to mitigate risks by diversifying and avoiding single supplier lock-in;
- Individual departments who use hosted applications that have peaks in computing demands and need a level of flexibility;
- looking to consume and pay for their infrastructure within an OPEX-based financial model and seeking greater efficiency and scalability to meet the growing needs of Public Sector departments.

2. Service Features and Options Summary

Service	Dev & Test. (Alpha/Beta)	Standard (Live)	High Availability (Live)	Managed Physical Host - Single Server	Managed Physical Host - Cold Standby	Managed Physical Host – Warm Standby
Availability SLA	99.5%	99.95%	99.99%	N/A	99.5%	99.5%
Site Failover	Optional	Optional	Yes	N/A	Optional	Optional
4hr RTO	No	No	Yes	N/A	Yes	Yes
RPO down to 1 hour	Yes	Yes	Yes	N/A	Yes	Yes
VM Performance	Contended	Uncontended	Uncontended	N/A	N/A	N/A
Secondary Site Compute Reservation	No	No	Yes	N/A	N/A	N/A
Storage Included (Tier 2)	80GB	80GB	80GB	80GB	80GB	80GB
Additional Storage Tier 0, 2,3	Optional	Optional	Optional	Optional	Optional	Optional
Storage Snapshot	Yes	Yes	Yes	Yes	Yes	Yes
Storage Replication	Optional	Optional	Yes	N/A	Optional	Optional
Managed Firewall	Yes	Yes	Yes	Yes	Yes	Yes
Managed Load Balancing & PSN Traffic Management	Optional	Optional	Optional	Optional	Optional	Optional
Managed Operating Systems	Yes	Yes	Yes	Yes	Yes	Yes
Managed MS Apps (AD,IIS, SQL)	Yes	Yes	Yes	Yes	Yes	Yes
Customer Asset Protective Monitoring & HIDS	Optional	Optional	Optional	Optional	Optional	Optional

PSN ‘Assured’ Connectivity	Yes	Yes	Yes	Yes	Yes	Yes
Reserved PSN bandwidth	Yes	Yes	Yes	Yes	Yes	Yes
Internet Connectivity (Assured Zones Only)	Yes	Yes	Yes	Yes	Yes	Yes
Security Domain Connection Gateway	Optional	Optional	Optional	Optional	Optional	Optional
Typical Use	Development App Server	Active Directory Server	Clustered Production App			

Note: Sungard AS offers Customer Asset Protective Monitoring and Host Based IDS as an optional service; however, for those who choose not to take this service from Sungard AS, the customer must provide adequate Protective Monitoring themselves or via a third party to meet the requirements for HMG ICT systems. Failure to do so could result in the suspension of one or more services.

3. Compute Services

3.1. Virtual Machine Sizes

Sungard AS offers a range of virtual machine sizes on the shared platform. You may select from the following range of predefined virtual machines (VM).

VM Instance (Size)	vCPU	Memory (GB)	Storage (GB)
X-Small	1	2	80
Small	2	4	80
Medium	4	8	80
Medium (High Memory)	4	16	80
Large	8	16	80
Large (High Memory)	8	32	80
Tier 1 Apps Small	8	48	80
Tier 1 Apps Medium	8	64	80
Tier 1 Apps Large	8	96	80

Your VMs can be provisioned within one or more VDC(s) and up to five vLAN's per VDC.

3.2. Virtual Machine Resource Types

Contention refers to how committed a particular resource is, typically if the Virtual CPU is oversubscribed. In non-production workloads, oversubscription can be a suitable compromise between performance and cost.

Sungard AS offers three virtual machine types on the shared platform:

- **Dev and Test (Alpha/ Beta)** virtual machines are provisioned in contended mode, this mode uses unreserved resources for all virtual machines, which at peak times, may result in reduced performance levels of the virtual machine workload.
- **Standard (Live)** virtual machines are provisioned in uncontended mode; this mode ensures that the CPU and RAM resources for each VM are available to each VM at all times.
  High Availability (Live) virtual machines are provisioned in both uncontended mode and the compute resources are reserved at the secondary site, though the VM is only active at the primary site in normal operation.

3.3. Virtual Machine Availability

All virtual machines operate with high availability built in at a single site to provide 99.5% availability for Dev/ Test (Alpha/ Beta) machines and 99.95% availability for Standard (Live) virtual machines.

For High Availability (Live) virtual machines, as well as single site virtual machines with optional replicated storage, all data is replicated to the second site to support an additional level of availability to provide a 99.99% SLA. Replication frequencies are based on the RPO you choose as part of your Storage Services. These typically vary from 1 hour to 12 hours.

3.4. Virtual Machine Cloning

Virtual Machine cloning creates a duplicate of a virtual machine with the same configuration and installed software as the original virtual machine. Virtual machine clones are additional virtual machines and are charged for accordingly based on storage and, if powered on, then Virtual Machine charges will apply.

Cloning can be undertaken on any Virtual Machine as an optional service, cloning is available via a service request, and is a chargeable service request catalogue item.

3.5. Managed Physical Hosts

For workloads that require physical servers, for example, performance or licencing reasons, Sungard AS can provide Managed Physical Hosts. All server images and all other data for Managed Physical Hosts will be stored on data store(s) per customer on shared Tier 2 storage arrays, as is provided for our standard shared platform virtual Machine instances.

We will not provision local storage for Managed Physical Hosts or attach customer provided peripherals or interfaces to the devices. Sungard AS will work with you to determine the server(s) specification you require to meet your application performance demands. Managed Physical Hosts can be deployed in Single Site or Dual Site configurations. Sungard AS offers 3 Managed Physical Hosts types:

- Small Server: Single Socket 4 Core with 32 GB RAM
- Medium Server: Dual Socket 6 core with 64 GB RAM
- Large Server: Dual Socket 10 Core with 128 GB RAM

Note: Managed Physical Hosts can only be ordered as part of a solution that includes standard shared platform virtual machines as detailed in Section 3.1 and are available for a minimum committed period of 12 months.

3.6. Operating System Templates

Sungard AS will provide pre-hardened Operating System templates from which Sungard AS will deploy your virtual machines and physical hosts. The template builds are in accordance with Communications Electronic Security Group (CESG) guidelines and Public Service Network (PSN) requirements. We provide templates for the following operating systems.

OS Type	Version	Edition

Microsoft Windows Server	2008 R2 64 bit	Standard, Enterprise
Microsoft Windows Server	2012 R2 64 bit	Standard, Datacentre Edition
Linux	5 64 bit	Redhat Enterprise Linux
Linux	6 64 bit	Redhat Enterprise Linux

Sungard AS will maintain the supported operating system templates. From time to time Sungard AS will add new operating system templates.

3.7. Managed Operating Systems

Sungard AS will deploy, monitor and manage the supported operating system(s) as well as deploying agents to monitor the platform's continued health. Sungard AS will maintain the patch state of the operating system, deploy anti-virus/ malware software, and monitor uptime and performance. Sungard AS is not responsible for the management of additional Windows Server Services, for example DHCP Servers, Certificate Services that the customer may introduce on to the server. This also applies to Linux operating systems. Please refer to section 9.5 "Managed Operating System Services" for more detailed information.

Sungard AS provides all operating system licences for use on this platform. We may also need to provide other software licences; Sungard AS will work with you to understand the overall licencing requirements for each customer solution.

3.8. Microsoft Application Services

Sungard AS provides the following supported Microsoft application services in addition to supporting the operating systems mentioned above:

- Microsoft Active Directory;
- Microsoft SQL Server;
- Microsoft IIS;
- Microsoft Exchange Server

The managed services include:

- Service monitoring and management

The scope for the design, build and service take-on (where the service build is undertaken by a 3rd party) for Microsoft Applications Services will be agreed between Sungard AS and the customer and will be formulated into work packages within one or more fixed price statement of works in order to deliver the requirements.

3.9. Customer Asset Protective Monitoring

Sungard AS, working with our Protective Monitoring partner can provide a protective monitoring service for customer assets. The definition of an asset is any device, appliance, operating system, application from which security events need to be collected, monitored and reported on by Sungard AS and its partner.

The service captures and alerts on events commensurate to the data processing requirements of each environment, as stipulated by the PSN Code of Connection and the recommendations laid out in the CESG (Communications Electronic Security Group) Good Practice Guide (GPG) 13 - Protective Monitoring for ICT Systems and the CESG Architectural Pattern (AP) 1 - Audit & Monitoring across Security Domains.

Aligned to these recommendations, the Protective Monitoring service comprises of a set of business processes and procedures operated under an ITIL aligned framework with ISO27001 certified policies and processes. These are managed and supported by Security Cleared staff.

Sungard AS are able to log, track, and analyse user and system activity, taking away the need for the customer to build, configure, maintain, and monitor using an in-house data collection solution. The service offers:

- Event generation;
- Alert generation;
- Event filtering;
- Event normalization;
- Event parsing;
- Secure event relay and collection;
- Event correlation;
- Event analysis.

Our Host-Based Intrusion Detection System (HIDS) service monitors the state of the operating system to detect malicious changes or activities. Agents are deployed which feedback events and alerts to a central monitoring server via a secure connection.

Sungard AS offers the following Protective Monitoring and Host-Based IDS services.

3.9.1. Standard without HIDS

This service will deliver Protective Monitoring against the following customer assets for each customer service[1] running on the platform.

- Software appliance or device where the software appliance or device is in the “known list” e.g. a plug-in exists for that the device or appliance so that it can be monitored by the service
- Application, where the application is in the “known list” egg. a plug-in exists for that applications so that it can be supported by the service, providing there is a single data output per application

3.9.2. Standard with HIDS

This service will deliver Protective Monitoring and Host Based IDS against the following customer assets for each customer service[1] running on the platform.

- Sungard AS supported operating systems
- Appliances\Devices that support the installation of an agent and the appliances are on the "known list" of appliances/devices e.g. a plug-in exists

Note: Although the underlying operating system of a software appliance or device may be in the "known list", not all appliances\devices support the installation of an agent; therefore, it will not be possible to provide the HIDS service against these types of assets.

Where no plug-in exists. Our consultants and Protective Monitoring partner(s) will engage with the customer to understand the Protective Monitoring requirements for each "unknown" asset for each customer service[1] and produce one or more fixed price statements of work in order to deliver the Protective Monitoring e.g. write a plug-in to support the monitoring of the asset(s).

[1] A customer service is defined as the assets that are running to provide the application service, for example a production service, or development and test service comprising of one or more VDC's with one or more assets providing resources to provide the production and/or development and test customer application services.

4. Network Services

4.1. PSN Connectivity

The platform has dual site dual path connectivity to the Public Services Network (PSN) 'Assured' WAN. The platform service interfaces to the PSN are via dedicated customer virtual firewalls and optional traffic management/ load balancing services per customer VDC.

Customers and user communities will require access to the PSN and must comply with the PSN Code of Connection (CoCo) in order to access the services hosted on the Managed Cloud Services for UK Government platform. Sungard AS supports access via the PSN shared user groups.

Customers must reserve the bandwidth for each PSN connected VDC. This is available in 1Mbps increments, charges apply. Customers must obtain their own IP Address Blocks for PSN use from the Cabinet Office.

4.2. Managed Internet Access

Sungard AS Managed Internet Access provides highly available IP access to the Internet. The following elements make up the service.

- Provision of Internet access to accommodate Customer contracted bandwidth:
  - Capped
  - Burstable
  - Limited Burstable (DDOS Mitigation Service)

- Provide registered IP addresses;
- Primary and Secondary DNS Zone/Records administration for ten (10) domains;
- Up to five (5) DNS changes with up to ten (10) records per change per month, for Customer-registered domain names;
- Monitor and manage Sungard AS Internet distribution infrastructure;
- Monitor Internet availability;
- Provide monthly Internet bandwidth utilisation report

The following bandwidth options can be ordered:

Type	Bandwidth
Capped	1-1000 Mbps
Burstable	4 x bandwidth up to 999 Mbps
DDoS Mitigation Service	1 Mbps Burstable Limit
DDoS Mitigation Service	2-4 Mbps Burstable Limit
DDoS Mitigation Service	5-9 Mbps Burstable Limit
DDoS Mitigation Service	10-19 Mbps Burstable Limit
DDoS Mitigation Service	20-29 Mbps Burstable Limit
DDoS Mitigation Service	30-39 Mbps Burstable Limit
DDoS Mitigation Service	40-49 Mbps Burstable Limit
DDoS Mitigation Service	50-59 Mbps Burstable Limit
DDoS Mitigation Service	60-69 Mbps Burstable Limit
DDoS Mitigation Service	70-79 Mbps Burstable Limit
DDoS Mitigation Service	80-89 Mbps Burstable Limit
DDoS Mitigation Service	90-99 Mbps Burstable Limit
DDoS Mitigation Service	100+ Mbps Burstable Limit

The following IP Address allocations can be ordered, charges apply:

- Block of 8 IP Address (3 usable)
- Block of 16 IP Address (11 usable)
- Block of 32 IP Address (27 usable)
- Block of 64 IP Address (59 usable)
- Additional Block of 8 IP Address (3 usable)

Note: Customer can bring their own Public IP Address Range. Charges apply for provisioning Internet Access for use with these addresses.

4.3. DDoS Mitigation Service

As an optional service, Sungard AS offers a DDoS Mitigation Service, via third party scrubbing centres. For resilience, Sungard AS is connected to 2 scrubbing centres. These are staffed 24/7 with a 15-minute response SLA from their Security Operations Centre.

4.3.1. Features

- Up to 20Gbs scrubbed traffic throughput;
- Fixed subscription price – no additional mitigation costs which scale with attacks;
- Advance warning of potential threats;
- Whitelisting;
- Blacklists

4.3.2. Benefits

- Dedicated specialist team with 100% mitigation record;
- Reporting of all level attacks to inform your security posture;
- Legitimate traffic flows continue

4.4. Inter-Site Connectivity

Customers can deploy virtual machines on the shared platform and Managed Physical Hosts across both sites to give higher levels of application availability. For dual site design services, you will need to order inter-site connectivity with the appropriate amount of bandwidth reserved across the inter-site link. Bandwidth is available in 1Mbps increments, charges apply.

4.5. Connection Gateway

This optional service provides a technical architecture that will allow secure connectivity between zones, typically for those VDCs connected to two or more zones, for example VDC's running in an Internet 'Assured' zone that needs to communicate with a VDC in a PSN 'Assured' zone.

During the discovery and design phase, our solution and security architects, from our professional services team, will discuss your requirements and agree the controls (people, process and technologies) required to meet the additional accreditation requirements of this service. Professional services charges will apply for this optional service.

4.6. Managed Load Balancing

A Managed Load Balancing service is available as a chargeable option. There are two load balancing service types:

- Standard – A single or multiple load balancing instance(s) that will load balance traffic to virtual machines and/ or Managed Physical Hosts in a single site or across sites with basic load balancing rule sets e.g. round robin, percentage traffic share and least connection.

- Advanced – A single or multiple load balancing instance(s) that will load balance traffic to virtual machines and/ or Managed Physical Hosts in a single site or across sites with complex load balancing rule sets using F5's event driven scripting language, iRules. Setup charges will apply for advanced load balancing configurations.

Standard and Advanced services include up to five rule set changes per month, via service request, with a maximum of 5 rules per request. Additional rule set change requests can be made and will be charged at the current rates.

4.7. Public Services Network (PSN) Traffic Management

An optional and chargeable service, PSN Traffic Management allows the distribution of inbound IP traffic across our two sites. PSN traffic management is only available for customers who connect to the platform with the following PSN connectivity services:

- One or more shared user group PSN connections:
- PSN Registered DNS Zone(s);
- 1 PSN IP Address block per site per PSN 'Assured' connection

4.8. Managed Firewall Service

The Managed Firewall Service consists of a virtual firewall instance and the initial context(s) configuration as standard. Also included in the Managed Firewall Service are up to five rule set changes per month per context, via service request, with a maximum of five rules per request. Additional rule set change requests can be made and will be charged at the current rates.

5. Storage and Back-up Services

Each customer is allocated one or more data store(s) which can be provisioned from the following storage performance tiers:

- Tier 0 Standard Storage - entirely comprised of Solid State Drives (SSD) with a target performance of 2000 IOPS per terabyte with a single off site daily recovery point (this is overwritten every 24 hours)

- Tier 0 Replicated Storage – entirely comprised of Solid State Drives (SSD) with a target performance of 2000 IOPS per terabyte, asynchronously replicated to the second site. Multiple recovery points can be provided in both data centres as defined in section 5.3Tier 2 Standard Storage – comprised of Serial Attached SCSI (SAS) Hard Disk Drives with a target performance of 250 IOPS per terabyte with a single off site daily recovery point (this is overwritten every 24 hours)

- Tier 2 Replicated Storage – comprised of Serial Attached SCSI (SAS) Hard Disk Drives with a target performance of 250 IOPS per terabyte, asynchronously replicated to the second site. Multiple recovery points can be provided in both data centres as defined in section 5.3

- Tier 3 Standard Storage– comprised of Serial ATA (SATA) Hard Disk Drives with a target performance of 50 IOPS per terabyte with a single off site daily recovery point (this is overwritten every 24 hours)

- Tier 3 Replicated Storage – comprised of Serial ATA (SATA) Hard Disk Drives with a target performance of 50 IOPS per terabyte, asynchronously replicated to the second site. Multiple recovery points can be provided in both data centres as defined in section 5.3

Data stores cannot span multiple storage tiers. One or more data stores can be provisioned for each VDC. Data stores do not span multiple VDC's.

5.1 Virtual Machine and Managed Physical Host Storage

All shared platform virtual machines and Managed Physical Hosts include 80GB of storage as a single drive. Further storage can be ordered and will be provisioned to one or more of your virtual machines or Managed Physical Hosts to facilitate additional drive partitions. Storage consumed by your shared platform virtual machines and Managed Physical Hosts within each data store will be charged per GB on a monthly basis. All Virtual Machines types and Managed Physical Hosts are unable to share virtual disks.

5.2 Storage Snapshots

Sungard AS will take scheduled storage snapshots for all shared platform virtual machines and Managed Physical Hosts to facilitate recovery to a point in time, down to a Recovery Point Objective (RPO) of one hour.

To support the One Hour RPO Sungard AS's standard recommended Snapshot intervals are as follows:

- one hour snapshots are maintained for no longer than 5 days

- daily snapshots will be maintained for a further 26 days
-

The snapshot parameters will be set during the design phase so that the frequency and retention times you require can be supported to match your requirements. Changes to your snapshot regime(s) can be made via a service request and will be charged accordingly, at the published rate at that time. The storage required for snapshots must be accounted for when calculating your total storage pool, taking into account the number of snapshots retained and the frequency of snapshots taken.

Restoration of data from a snapshot is initiated via a Service Request and is a chargeable item.

5.3 Storage Replication

Secondary site storage replication is available to support recovery of shared platform virtual machines and Dual Site Managed Physical Host deployments only.

For Dev and Test (Alpha/ Beta) and Standard (Live) virtual machines on the shared platform you can choose between non-replicated storage and replicated storage. If you choose replicated storage for these virtual machine types, Sungard AS will provide an RPO SLA down to 1 hour at the secondary site. However, Sungard AS will not provide a secondary site Recovery Time Objective (RTO) SLA, we will recover your virtual machines under reasonable endeavours.

Storage replication is included for all High Availability (Live) virtual machines. For Dual Site Managed Physical Host deployments, storage replication must be ordered for each Managed Physical Host on the Primary Site deployed in a Dual Site configuration. Sungard AS will provide a four hour RTO SLA for the aforementioned virtual machine and Managed Physical Hosts types.

Your storage replication policies (frequencies and retention) will be set during the on-boarding process, see table 5.4 below for supported schedules.

Table 5.4

Retention	1 day	7 days	14 days	21 days	31 days
Frequency	Down to every hour				

Changes to the replication policies can be made in service by raising a service request and will be charged accordingly, at the published rate at that time.

6. Availability and Disaster Recovery

6.1. Shared Platform Virtual Machines

Our standard shared platform virtual machines can be deployed in the following ways.

6.1.1. Dev and Test (Alpha/Beta) and Standard (Live) Virtual Machines

- Option 1: Primary Site only: No Storage Replication;
- Option 2: Primary Site with Secondary Site Storage Replication.

For option 2, in the event of the primary site becoming unavailable, Sungard AS does not provide an RTO Service Level Agreement for these virtual machines at the secondary site and the recovery is carried out under reasonable endeavours.

For option 2, in the event of the primary site becoming unavailable, Sungard AS will support an RPO down to a maximum of one hour at the secondary site for Dev and Test (Alpha/ Beta) and Standard (Live) Virtual machines.

6.1.2. High Availability (Live) Virtual Machines

High Availability (Live) virtual machines on the shared platform are provisioned with storage replication enabled by default and these virtual machine resources are both uncontended and reserved at the secondary site. Sungard AS offers an RTO of four hours at the secondary site and an RPO down to a maximum of 1 hour for the recovery of High Availability (Live) virtual machines at the secondary site.

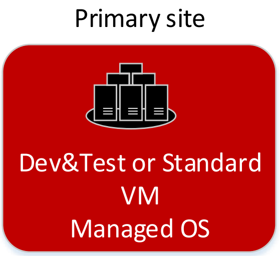
Lower RTO's and RPO's may be available upon request. To discuss this in more detail, please contact our representative shown in section 12. – Further Information.

6.2. Shared Platform Virtual Machines - Workload Design Patterns

The following designs are illustrative and are examples only. Each design includes the number of virtual machine types, OS Licences, Managed Operating system instances and other elements that are required to support the design.

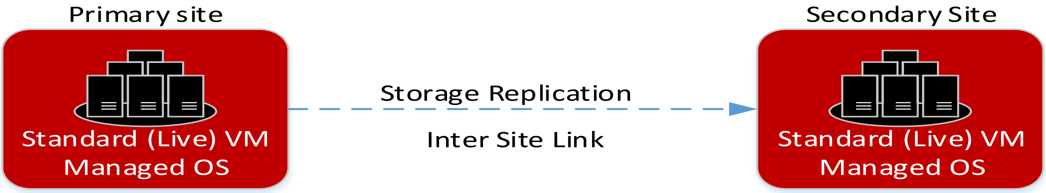
6.2.1. Dev and Test (Alpha/Beta) and Standard (Live) Virtual Machine - No Storage Replication

VM Type	Managed OS OS Licence	Replicated Storage	Example Workloads
One x Dev & Test or Standard VM	One	No	Build Server Pre-production Application server Load injection Server



6.2.2. Standard (Live) Virtual Machines – Replicated Storage

VM Type	Managed OS OS Licence	Replicated Storage	Example Workloads
Two x Standard VM	Two	Yes	Production Web Server Production Application Server.

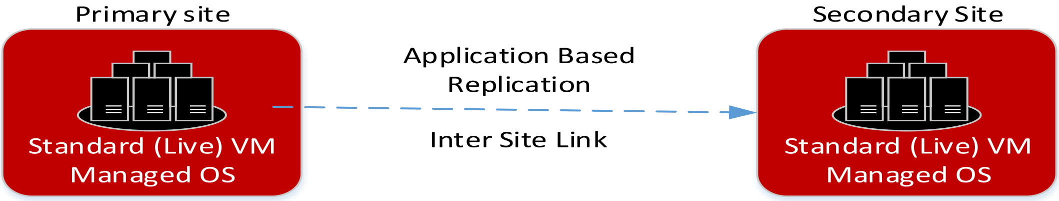


Note: Sungard AS recommends that servers and services that require this set up can operate in an Active/Passive design pattern.

6.2.3. Standard (Live) Virtual Machines – Un-replicated Storage

VM Type	Managed OS OS Licence	Replicated Storage	Inter-site Bandwidth	Example Workloads
Two x Standard VM	Two	No	Yes	Active Directory Database Server

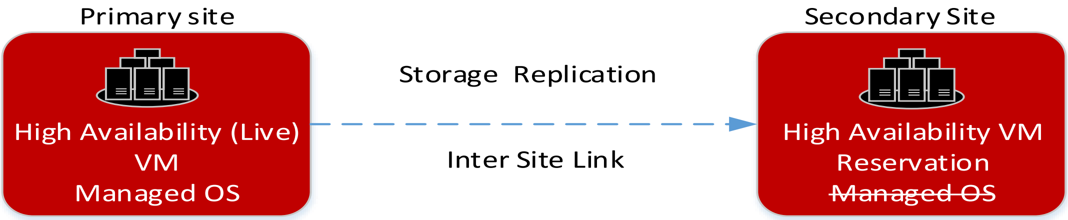
This design is appropriate for environments where downtime is highly undesirable or where application based replication is preferable.



It is the customer's responsibility to implement application level availability. Customer applications in an active-active configuration will leverage the inter-site resilient links between the data centres. Link bandwidth charges are based on reserved capacity.

6.2.4. High Availability (Live) – Replicated Storage

VM Type	Managed OS OS Licence	Replicated Storage	Example Workloads
One x High Availability VM	One	Yes (included)	Production Web Server Production Application Server



6.3. Managed Physical Hosts

Managed Physical Hosts can be deployed in the following ways.

6.2.1 Single Site Single Server

A single server or number of single servers with dual power supply connected to redundant network and storage layers at the single site. This server has no resilience or fail-over. Replicated Storage can be included as part of Single Site Server deployments

6.2.2 Single Site with N+1 Cold Standby Server

One or more active servers with one or more local cold standby servers all with dual power supply connected to redundant network and storage layers. In a local cold failover configuration the active server is shut down and its Service Profile switched to a standby server which is then booted.

6.2.3 Single Site with N+1 Warm Standby Server

One or more active servers with one or more warm local standby servers all with dual power supply connected to redundant network and storage layers. In a local warm failover configuration the active server and local warm standby server(s) have their own boot volumes (LUNs) so are independent and run concurrently. A second volume and LUN are created and presented to the primary server. The volume is replicated to the local warm standby server(s) but is inaccessible.

When failover is invoked the volume becomes accessible to the warm local standby server. When the failover server is running, the volume will appear instantly as a new drive or mount depending on the Operating System.

6.2.4 Dual Site with N+1 Cold Standby Server

One or more active servers with one or more remote cold standby servers all with dual power supply connected to redundant network and storage layers. In a dual site cold failover configuration the active server is shut down and its Service Profile switched to a standby server in the secondary site which is then booted against the replicated LUN.

6.2.5 Dual Site with N+1 Warm Standby Server

One or more active servers with one or more warm remote standby servers all with dual power supply connected to redundant network and storage layers. In a dual site warm failover configuration the active server and the warm standby server(s) in the secondary site have their own boot volumes (LUNs) so are independent and run concurrently. A second volume and LUN are created and presented to the primary server. The volume is replicated to the standby server(s) in the secondary site but is inaccessible.

When failover is invoked the volume becomes accessible to the warm standby server in the secondary site. Since the failover server is running, the volume will appear instantly as a new drive or mount depending on the Operating System.

Note: For customers who have multiple applications running on Managed Physical Hosts, if a single standby server is ordered either in a single site configuration or a dual site configuration to facilitate a failover, then the standby server must have the same specification as the largest Managed Physical Host in terms of the number of Processors, CPU cores/speed and RAM.

6.2.6 Active – Active Servers

One or more servers with dual power supplies connected to redundant network and storage layers at the primary or secondary site. Multiple servers can be deployed to support higher levels of application or database availability, such as Oracle RAC Clusters, Microsoft SQL Server 2014 “Always on” Availability Groups or Microsoft Exchange Database Availability Groups. The redundant network is layer 3 encrypted. The servers write to the primary SAN storage which is then replicated to the remote SAN storage.

.

Note: On any configuration of Managed Physical Host(s) application(s), if there is a reliance on other services running on shared platform virtual machines then all such virtual machines would need to be failed over as well to support a complete failover solution and RTO to maintain a consistent running state.

7. Management Services

7.1 Third Party Remote Access Laptop

Sungard AS can provide CESG accredited remote access laptop(s), as an optional chargeable service to support non-PSN secure access to the platform for third parties e.g. Independent Software Vendors, who publish applications for PSN connected customers. Remote access laptops are available for a minimum period of 12 months.

7.1.1. Limitations of Use

- All Administrators that access the device must have validated SC clearance;
- The supplied device can only be used to connect to the platform;
- Up to 3 named users per device.

7.1.2. What is Included

- Laptop and power supply;
- RSA Hard token(s) 3 maximum;
- Rucksack.

7.1.3. Provisioning and Support Process

The remote access laptops are built and supported by Sungard Availability Service' secure operations team. Each device is individual and registered to its users.

Users will need to enrol to the whole disk encryption service with their token and credentials. All registered user(s) for each device will need to produce their Systems Operations Procedures (SYOPS) and sign our (SYOPS) before they can be issued with a remote access laptop.

If the user requires support for the device, or if the device fails, you should contact the Sungard AS Managed Cloud Services for UK Government service desk. Sungard AS will arrange for the faulty device to be returned to the service desk team for replacement. On receipt of the faulty device, Sungard will dispatch a new device for next business day delivery.

In the event of loss or theft of a remote access device, the partner or customer must inform the Sungard secure operations team immediately.

Devices remain the property of Sungard AS and must be returned at the end of the contract/ life. Laptops will be replaced every 3 years.

7.2. Customer Portal

The customer portal is available to customers includes the following features:

- Service Request Catalogue;
- Raise and Track Incidents and Service Requests;
- Charts;
- Knowledge Base.

7.3. Secure Intelligent Hands

The secure intelligent hands service provides the facility for Sungard AS to assist with the provisioning of customer services on or off of the Managed Cloud Services for UK Government platform using Sungard AS personnel who have been granted Security Clearance.

When physical access or remote access is required into the secure sites where Sungard AS operate the Managed Cloud Services for UK Government platform services, Sungard AS will provide the necessary skilled Security Cleared personnel, adhering to our mandated security controls, to complete the necessary tasks.

One example task where the use of Sungard AS secure intelligent hands would be required would be for the direct import or export of customer data into or out of the platform as only Sungard AS security cleared staff may enter the restricted sites where the platform is located.

Another example would be where Sungard AS would facilitate remote access to the platform via a secure remote access laptop where the customer’s designated operator of the laptop did not have validated Security Clearance in place (a mandatory requirement for remote access) at the time, but access to the environment was required to carry out some critical work. Sungard AS secure intelligent hands can chaperone the customer whilst the work is undertaken.

Customers can order secure intelligent hands via a G-Cloud contract with the number of half days to be utilised throughout the period of the contract. The minimum secure intelligent hands order is for half a day per site either in normal business hours 8:00am to 6:00pm (UK time, Mon-Fri excluding UK Bank Holidays) or Out-of-Business Hours (All other times) . Charges apply.

Secure Intelligent Hands type	Unit
Business Hours (Monday-Friday 8am-6pm)	Half Day
Out-of-Business Hours (Monday-Friday, Weekends, UK Bank Holidays)	Half Day

All Secure Intelligent Hands requests must be made by raising a service request via email or the customer portal. Sungard AS will provide reasonable endeavours to schedule the Secure Intelligent Hands resource within 5 business days of the Secure Intelligent Hands service request being categorised, classified and assigned an owner.

7.4. Secure Direct Data Import and Export Service

The Sungard AS Secure Direct Data Import and Export Service allow customers of the Managed Cloud Services for UK Government platform to transfer their data into and out of their VDC's via a Secure Data Transfer Server at each site. Typically, this would be for larger data files, database files or potentially application installation ISO images.

The Secure Direct Data Transfer Service allows for the connection of a portable USB device to the Data Transfer server within the platform and supports the controlled, (virus and malware checking and quarantining) import and export of data to and from customer data stores.

The service is designed to enable the Customer to maintain full control over the access to their data through every stage of the process in accordance with their specific data handling procedures.

7.4.1. Service Responsibilities

7.4.1.1. Sungard AS

In order to utilise the service Sungard AS will undertake the following:

- Connection of the Customer supplied USB device to the Data Transfer Server within the platform at either site (the process for transporting and receipt of the USB device will be agreed with the Customer prior to commencing the data transfer process)

- Creation of a temporary Import Customer Virtual Machine if required to support data transfer to a Managed Physical Host
-

- Removal of the customer supplied USB device from the Data Transfer Server and return to the customer as per the agreed process
-

7.4.1.2. Customer

In order to utilise the service the following must be in place:

- The Customer VDC, and virtual machines and/or Managed Physical Hosts that require the files\data must have completed the operational acceptance process and formal customer acceptance.
- Customer must provide a removable USB device that meets their security requirements for the transfer of data.(The Data Transfer Server supports USB 2 and USB 3 devices)
- Transport and collection of the USB device to/from the Sungard AS Datacentres, including any associated power packs/adaptors
- Disposal and secure erasure of the USB device in accordance with the customer requirements.
- Copying of the data from the USB device to the Customer allocated storage including:
  - Management of all encryption passwords
  - Formatting the USB device to a suitable file system that can be read by the target operating system, i.e. FAT32, or EXT etc. Note FAT32 is recommended as this is compatible with Linux and Windows.
  - Making all data on the USB device Read-only (This will ensure that the Sungard AS Anti-Malware scanner does not delete/quarantine any customer data)
  - Nomination of the target VM to copy the data to/from
  - Transfer of the files to/from the customer nominated virtual machine

Customers can order the Sungard AS Secure Direct Data Import and Export Service for a minimum period of half a day per site and is available in normal business hours from 8:00am to 6:00pm (UK time, Mon-Fri excluding UK holidays) or Out-of-Business Hours (all other times). Charges apply.

Secure Intelligent Hands are included as part of the Secure Data Import and Export Service.

Secure Direct Data Import and Export Service & Secure Intelligent Hands	Unit

For Secure Direct Data Import and Export Services, the customer must raise a service request via email or the customer portal in accordance with the agreed process at service take-on. Sungard AS will use reasonable endeavours to schedule the use of the Secure Direct Data Import and Export service within 5 business days of a valid service request being received and acknowledged.

8. Accreditation & Migration Services

8.1. Accreditation Advisory Services

Our Accreditation Services are available as an optional service to assist the data owner in achieving the appropriate accreditation for connectivity and compliance for consuming and publishing services from the Sungard AS Managed Cloud Service for UK Government platform. Our consultants and advisors will formulate work packages within one or more fixed price statement of works in order to deliver the requirements.

One or more of the following activities will be included in the scope of the work package.

- **Data Gathering:** This task ensures that there is a good understanding of the service being delivered to the end-customer, in particular:
  - The scope of the service including the elements provided by Sungard AS, the elements provided by the customer/vendor and the elements provided by the vendor's customers (i.e. Sungard AS' responsibilities, customer/vendor responsibilities, the end-customer responsibilities and ownership of information assets).
  - Identification and valuation of information assets within the service.
  - Understanding how the service is provisioned, how the end-customer accesses the service, and how customer/vendor provides service management.
  - Agreeing with the end-customer the risk appetite and risk tolerance associated with the service.
- **Threat Assessment:** This would build upon the threat assessment of the Managed Cloud Services for UK Government platform, and hence would only focus on the additional threats (if any) posed by the customer service being delivered to a particular end-customer.
- **Risk Assessment:** This would build upon the Managed Cloud Service for UK Government platform risk assessment, focusing on the additional risks posed by the customer service being delivered to a specific customer. This will include:
  - Producing an Infosec Model as defined in HMG IS1 & 2.
  - Identify potential compromise methods and their associated risks.
  - Produce a prioritised list of risks based upon the capability and motivation of specific threat actors and the potential impact of a particular compromise.
- **Risk Treatment Plan:** Using the above risk assessment and building upon the Managed Cloud Services for UK Government risk treatment plan, this task will identify the degree of compliance with the security controls specified in HMG IS1 & 2. This will include identifying how assurance in those controls is achieved.
- **Residual Risk Assessment:** This task will identify any risks that are not adequately treated by the Risk Treatment Plan, and produce a remediation plan for resolving those risks.
- **RMADS Production:** This task will collate the results of all the previous tasks and produce a Risk Management and Accreditation Document Set (RMADS) in accordance with HMG IS1 & 2. This process will involve drafting, reviewing and updating activities with the end-customer accreditor. The outcome of this task will be approval from the end-customer accreditor and Senior Risk Owner that the customer service for that customer can operate at the required security level.

8.2. IT Health CHECK Service

Working with CESG approved partners, Sungard AS offers, as an optional service, an IT Health Check (penetration test) work package under the CHECK scheme to identify vulnerabilities in the IT systems that you plan to run on the Managed Cloud Services for UK Government environment.

The IT Health Check is a necessary part of the data owner's (SIRO) responsibilities to ensure the correct implementation of security functionality and to identify and mitigate vulnerabilities in the application workloads, which may otherwise compromise confidentiality, integrity or availability of information on the system or network. All systems processing data protectively marked Official, including Official-Sensitive, must be assessed under CHECK.

8.2.1. Approach of the IT Health Check Service

Each assessment performed under the terms and conditions of CHECK will be performed by a team of security cleared (SC) personnel and led by a CHECK team leader. He or she will be present throughout the test.

A CHECK assessment is an IT Security Health CHECK conducted in accordance with procedures and standards laid down by CESG.

There is no fixed technical specification for a CHECK assessment, so, in the first instance, such an assignment must be properly scoped by an accredited CHECK Team Leader. On acceptance of the scope of work, testing will be conducted by a CHECK Team, consisting of at least one qualified CHECK team leader and a number of CHECK team members.

8.2.2. IT Health Check Report

Our CESG approved IT Health Check partner will provide you with the penetration testing report in order to equip you with a full understanding of any vulnerabilities within your environment on the Managed Cloud Services for UK Government platform, as well as specific advice on how to eliminate or mitigate those vulnerabilities.

At a high level the report itself will include the following information:

- A non-technical summary of the Health Check findings.
- An objective or aim for the Health Check.
- The Scope of the Health Check as agreed with the customer.
- The vulnerability findings.
- Recommendations/ solutions.
- Basic logs.

More specifically, the following items will be included in the report:

- Individuals involved in the test are identified.
- A high-level description of the main findings in non-technical terms.
- All findings are positively identified (where possible) and described.
- Each finding is accompanied by a solution that is relevant to the customer's environment.
- Automated vulnerability scanning tools do not appear to have been heavily relied upon.
- The tests and attacks performed were as comprehensive as possible, technically sound and within the bounds of the customer agreed scope.
- The logs should contain full port scans for each live system within scope and show how each live system was identified.

8.3. Migration Services

Sungard AS also offers a chargeable full migration service. The migration service provides a low risk, benefit optimised transition plan to migrate your services onto the platform. Using proven methodology, tools and experience gained from prior migrations, the service consists of a highly collaborative process that works closely with your IT and business teams.

This approach enables Sungard AS to develop and execute a migration plan based on proven strategies that incorporate validation of workload compatibility, dependencies, rollback plans and testing of candidate services including an evaluation of application performance pre and post migration.

9. Service Delivery

In provision of the Sungard AS Managed Cloud Services for UK Government, Sungard AS will provide to all customers of these services four key capabilities:

- Service Desk – provided on a 24/7/365 basis, the Sungard AS Service Desk is the central point of contact for all service-related communications with Sungard AS for all subscribed services who will liaise with the customer authorised personnel to log any issues, requests or enquiries relating to these services. The Sungard AS Service Desk will ensure that calls are passed to the appropriate resolver groups for follow up and resolution.
- Service Operations – available on a 24/7 basis, the service operations teams will include an on-site presence at the appropriate data centres, providing additional support resources to the technical support teams tasked with ensuring that prescribed SLAs are maintained.
- Service Management – a team of dedicated Service Management specialists who liaise directly with Sungard AS Service Operations to ensure correct levels of governance and compliance are in place and aligned with ITIL best practice guidelines.
- Systems Support and Administration – Sungard AS will provide these technical support functions to the Sungard AS Managed Cloud Services for UK Government.

Further details can be found in the Managed Cloud Services for UK Government Operations Manual, which is owned and updated by Sungard AS Service Management. This Operations Manual describes the policies, processes, procedures and interfaces through which the Managed Cloud Services for UK Government are delivered.

9.1. Service Level Commitments

9.1.1. Service Desk and Support Windows

Managed Cloud Services for UK Government adheres to the following service desk availability and support windows.

Server Type	Service Desk	Support Window
Dev and Test (Alpha/Beta) virtual machines on shared platform.	24/7	8:00am to 6:00pm UK time, M-F excluding UK holidays + Out of Hours (OOH) for change implementation and P1/P2 support when required.
Standard (Live) and High Availability (Live) virtual machines on shared platform and Managed Physical Hosts.	24/7	24/7

9.1.2. Virtual Machine Availability Service Level Agreements

Availability is measured on a per virtual machine basis on the shared platform where the service comprises both the server and storage associated with it.

Managed Cloud Services for UK Government adheres to the following virtual machine availability targets.

Type	Virtual Machine Type	System Availability Target	Definition
SLA	High Availability (Live) shared platform VM	99.99%	Either primary or secondary server is up and OS operational.
SLA	Standard (Live) shared platform VM	99.95%	Availability on a per server basis and OS is operational.
SLA	Dev and Test (Alpha/Beta) shared platform	99.5%	Availability on a per server basis and OS is operational.

A shared platform virtual machine is deemed available when the operating system responds to ICMP (Ping) requests.

9.1.3. Managed Physical Hosts Service Level Agreements

Managed Physical Hosts in Managed Cloud Services for UK Government offers the following availability targets.

Type	Physical Host Deployment	System Availability Target	Definition
KPI	Single Server	98.5%	Physical server is up and OS operational
SLA	All other Managed Physical Host deployment types	99.5%	Either primary or standby (secondary) server is up and OS operational at either site

9.1.4. Recovery Point Objective Service Level Agreement

Managed Cloud Services for UK Government adheres to the following RPO targets

Type	Server Type	RPO Target	Definition
SLA	All Shared Platform Virtual Machines All Managed Physical Host Types	Set during on-boarding (down to every hour standard maximum) and any changes via service request in life.	Recover to last snapshot as defined by RPO target.

9.1.5. Recovery Time Objectives Service Level Agreement

9.1.5.1. Virtual Machines & Managed Physical Hosts

Managed Cloud Services for UK Government adheres to the following RTO target for High Availability (Live) virtual machines only

Type	Server Type	RTO Target	Definition
SLA	High Availability (Live) Virtual machines on shared platform.	4 hours	The HA virtual machine OS at the secondary site is recovered to the required running state.
SLA	All Dual Site Managed Physical Host Types	4 hours	The standby server OS in the secondary site is recovered to the required running state

9.1.6. Internet Access Availability SLA

Internet Access Availability is defined as the ability to route a data packet from a customer's private segment to the egress point on the public Internet. Meeting this SLA is based on an Availability Percentage of 99.99% as calculated in the following table.

Variable	Definition
Monthly Hours	Total number of hours in any month.
Scheduled Downtime	Total time in the month that the service is scheduled as unavailable either by maintenance or by customer request.
Unscheduled Downtime	Total time in the month that the service was unavailable due to an action by Sungard AS unrelated to scheduled downtime. Obtained from ICAP.
Scheduled Uptime	Monthly hours minus Scheduled Downtime.
Available Hours	Scheduled Uptime minus Unscheduled Downtime.
Availability Percent	Available Hours divided by Scheduled Uptime, rounded to the nearest 10th.

Outages caused by the following events are not included as Unscheduled Downtime:

- Hardware failures unrelated to Sungard AS negligence or Sungard AS infrastructure;
- Software failures unrelated to Sungard AS negligence or Sungard AS infrastructure;
- Breach of acceptable use policy or any breach of the agreement by the customer or customer's agent;
- Negligence or intentional acts or omissions by the customer or customer's agent;

The Commitment becomes void if any one of the following occurs:

- The customer refuses a Sungard AS maintenance change request related to the delivery of Internet Access services.

9.1.7. Incident Priority Definitions

The Managed Cloud Services for UK Government use the following criteria for prioritisation of incidents as defined in the Sungard AS – Managed Cloud Services for UK Government contract

Priority	Contact Method	Criteria (Meets One or More)	Examples (Not a Definitive List)
P1	By Phone only	Severe unusable. Severe disruption of service or business functions, possibly with revenue loss. Critical Systems Unit failed or severely impaired. No workaround(s) exist. Affects Critical business unit, users or functions.	Multiple server failures affecting key operational areas. Severe performance degradation. Financial systems affected in a close period. Security issue such as malware, virus.
P2	By Phone only	Causes major business disruption. VIP user(s) or Business Unit with significant reduction in system performance. No workaround(s) exist. Potential to cause or become a P1.	Slow response of key business application for one or more users. Security incident.
P3	email or customer portal	Impacts system availability or operation of services. Affects users within a single function. Workarounds may be in place. Business operations impacted but not severely.	Equipment failures which are covered by redundancy/ resiliency. Server or infrastructure device identified as not having current patch/pattern files within 5 days of a patch being uploaded to the distribution servers by Service Provider.
P4	email or customer portal	Minor disruption or usability issues. Affects single user or function. Workaround is available. Does not impact business operations.	Incident queries relating to Data Centre Services.

9.1.8. Incident Response and Resolution Targets

Incidents are responded to, resolved and reported, according to the Key Performance Indicator (KPI) specifications as listed below:

	Type	Service Level	Target	Measure
Response Time	KPI	Priority 1 (Critical)	15 min	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
	KPI	Priority 2 (High)	30 min	From the time the ticket is logged to the time it is electronically accepted by the resolving team.

	Type	Service Level	Target	Measure
	KPI	Priority 3 (Medium)	60 min	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
	KPI	Priority 4 (Low)	2 hrs.	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
Resolution Time	KPI	Priority 1 (Critical)	4 hrs.	For each Priority 1 (Critical) Incident, from the time the Ticket is logged in the Ticket Management System, to the time that the Incident is resolved.
	KPI	Priority 2 (High)	8 hrs.	For each Priority 2 (High) Incident, from the time the Ticket is logged in the Ticket Management System, to the time that the Incident is resolved.
	KPI	Priority 3 (Medium)	4 business days	For each Priority 3 (Medium) Incident, from the time the Ticket is logged in the Ticket Management System, to the time that the Incident is resolved.
	KPI	Priority 4 (Low)	10 business days	For each Priority 4 (Low) Incident, from the time the Ticket is logged in the Ticket Management System, to the time that the Incident is resolved.
Updates	KPI	Priority 1 Incident	every hour (24x7)	A Sungard AS service desk incident assignee will contact the customer named contact by phone every hour with an update on incident status.
	KPI	Priority 2 Incident	every 2 hours (24x7)	A Sungard AS service desk incident assignee will contact the customer named contact by phone every 2 hours with an update on incident status.
	KPI	Priority 3 and 4	every 24 hours Mon-Fri	A Sungard AS service desk incident assignee will email the customer named contact every 24 hours Monday to Friday with an update on incident status.
Reports	KPI	Priority 1 and 2	within 4 business days of incident resolution	The Sungard AS Service Manager will formulate an incident report and present it to the customer service owner.

9.2. Maintenance Windows

Maintenance windows are defined to ensure Sungard AS is able to perform routine and scheduled maintenance of the platform in order to maintain availability and retain certification.

Sungard AS's maintains the supporting infrastructure for this platform using the following principles:

- Maintenance windows will not be included in any formulas for calculating availability of the platform.
- Maintenance window times are excluded from the Availability service level calculation i.e. total time available will exclude the maintenance window times.
- Expected downtime during maintenance windows will not be included in any Service Credit calculation.
- Organisations that have deployed 'active-active' solutions should not experience any downtime during maintenance windows if the application has been implemented correctly in order to cater for such events; however degraded performance may be experienced.
- Sungard AS retains the right to close down all systems to perform emergency maintenance if non-performance of this maintenance could result in a security risk for the platform or any organisation using the platform.
- You will be allocated one 'scheduled' maintenance window per week, which will be defined during the service on-boarding process.
- Seven (7) days' notice will be provided for routine and scheduled maintenance.
- Twenty-four (24) hours' notice will be provided for critical and security related patching, unless deemed as an Emergency in order to stop a major outage on the platform.
- Four (4) hours' notice will be provided for emergency patches and critical changes.
- All non-emergency patches and changes will be performed on a Sungard AS Managed Test VDC prior to being deployed to your environments.

The following Maintenance Descriptions apply:

- Sungard AS maintenance windows – this will include modifications, patching or fixes to the platform or management zones, with maintenance being performed between the hours of 8pm and midnight, on the 1st and 3rd Sunday of each month at the primary site and the 2nd and 4th Sunday each month at the secondary site. Sungard AS will always strive to complete the maintenance as soon as possible within the maintenance window and will only ever use the full maintenance window when necessary. The platform and management zones run on the secondary site whilst maintenance is undertaken on the primary site and vice versa.
- Sungard AS maintenance of infrastructure in any given organisation's zone – this will include standard and routine maintenance, including the implementation of security and critical patching, fixes or hardware and software upgrades. We will agree the scheduled 'maintenance day', with maintenance being performed between the hours of 00:00 – 06:00 on the scheduled 'maintenance day'. Sungard AS will always strive to complete the maintenance as soon as possible within the maintenance window and will only ever use the full maintenance window when necessary.
- Emergency maintenance – this will include the implementation of any critical security patches or configuration changes that Sungard AS deem necessary to protect the integrity of the platform and any given Organisation's zone.

9.3. Customer Service Requests

Customer service requests can be raised by calling the service desk, via email (for CJSM users) or via the Service Request catalogue within the customer portal. The service desk will categorise and prioritise each service request received with the classifications in Table below:

Priority	Impact	Type

1	Critical	Change required to maintain total service operability
2	High	Change required to maintain a main element of the service
3	Medium	Change required to improve an element of the service
4	Low	Cosmetic change to an element of the service

Sungard AS will acknowledge customer service requests in accordance with the timescales specified in Table below

Type	Priority	Target Time to Acknowledge Service Requests	Measure
KPI	1	15 minutes	Once the service request is categorised, classified and assigned an owner
KPI	2	30 minutes	
KPI	3	1 hour	
KPI	4	12 hours	

Resolution times for customer service requests, including any requirements to perform work outside of normal business hours will be mutually agreed on a case-by-case basis. We will notify you if the customer service request will incur additional charges or require a change to any of your services. We will not proceed with the request until we have received your agreement to any additional costs or charges.

Table 9.3.3 below defines the standard service requests we offer in our Service Request catalogue and indicates which service requests are chargeable. Standard Service Request pricing can be found in our Managed Cloud Services for UK Government Pricing Guide.

Table 9.3.3

Customer Service Request Type	Chargeable	Additional Monthly Charges
Change Firewall Rule Set (Max 5 Rules per request)	Yes	No
Change Load Balancing Rule Set (Max 5 Rules per request)	Yes	No
Change Virtual Machine Resources (CPU, RAM, Storage)	No	Yes (Storage and/or compute)
Change Storage Snapshot/Replication Frequency/Retention	Yes	No
Clone Machine/Data store/VDC	Yes	Yes (Storage and/or compute)
Delete a Virtual Machine(s)	No	No
File/data upload to existing Virtual Machine/Host	No	No

Customer Service Request Type	Chargeable	Additional Monthly Charges
Order a new Virtual Machine/Host	No	Yes (Storage and compute)
Power off a Virtual Machine/Host	No	No
Power on a Virtual Machine/Host	No	No
Rebuild Virtual Machine/Host as Initial Build	Yes	No
Restart a Virtual Machine/Host	No	No
Restore Data to a Machine from a Snapshot	Yes	No
Restore Machine from a Snapshot	Yes	No
Shutdown a VM/Host	No	No

9.4. Service Credits

9.4.1. Virtual Machine and Managed Physical Host with Standby Server Availability SLA

Unavailability applies where the virtual machine(s) or Managed Physical Host become unresponsive due to a fault recognised at the:

- virtual machine level (hypervisor);
- enterprise supported operating system level (see section 3.6);
- supported Microsoft applications (see section 3.8);
- host layer;
- storage layer;
- network layer.

And not where the fault is with:

- the customers control (application, user network);
- external connectivity providers;
- community supported operating system level;
- Incompatibility between customers provided software and the operating system or patch applied to the operating system.

If Sungard AS fails to meet the Virtual Machine Availability SLA for virtual machines on the shared platform or Managed Physical Hosts then the customer is entitled to a service credit equal to the percentage identified in tables 9.4.1.1, 9.4.1.2, 9.4.1.3 and 9.4.1.4 for each month in which the failure occurred.

9.4.1.1. Dev & Test (Alpha/Beta) Virtual Machine Service Credits

Availability (%)	Measure	Service Credit (% of pro-rata portion of Monthly Fee based on affected virtual machine(s))

≥99.3% and <99.5%	VM started on alternate node and the supported Enterprise Operating System and Microsoft Application (where applicable) is operational	10%
≥99.1% and <99.3%		20%
<99.1%		30%

9.4.1.2. Standard (Live) Virtual Machine Service Credits

Availability (%)	Measure	Service Credit (% of pro-rata portion of Monthly Fee based on affected virtual machine(s))
≥99.9% and <99.95%	VM started on alternate node and the supported Enterprise Operating System and Microsoft Application (where applicable) is operational.	10%
≥99.5% and <99.9%		20%
<99.5		30%

9.4.1.3. High Availability (Live) Virtual Machine Service Credits

Availability (%)	Measure	Service Credit (% of pro-rata portion of Monthly Fee based on affected machine(s))
≥99.97% and <99.99%	VM started on alternate node at Primary Site or VM started on alternate node at Secondary Site and the supported Enterprise Operating System and Microsoft Application (where applicable) is operational.	10%
≥99.95% and <99.97%		20%
<99.95%		30%

9.4.1.4. Managed Physical Hosts with Standby Server(s)

Availability (%)	Measure	Service Credit (% of pro-rata portion of Monthly Fee based on affected machine(s))
≥99.93% and <99.95%	Standby Server running at Primary or Secondary Site And the supported Enterprise Operating System and Microsoft Application (where applicable) is Operational.	10%
≥99.91% and <99.93%		20%
<99.9%		30%

9.4.2. Recovery Point Objective SLA

The RPO SLA is aligned to the RPO for each shared platform virtual machine or Managed Physical Host (all types) based on the storage snapshot frequency that the customer defines for each virtual machine. Sungard AS will facilitate the recovery of a virtual machine(s) or Managed Physical Host (all types) to the required point in time, as long as the frequency and retention period set by Sungard AS, but by order of the customer, can facilitate the RPO, down to a 1 hour RPO.

If Sungard AS fails to meet the customer RPO SLA, then the customer is entitled to a service credit equal to the percentage identified in table 9.4.2.1 for the month in which the failure occurred.

9.4.2.1. RPO Service Credits

RPO missed by _ %	Service Credit % of pro-rata portion of Monthly Fee based on affected virtual machine(s) and/or Managed Physical Hosts
1%-49%	30% of the affected virtual machine(s) and/or hosts monthly subscription charges
50%-99%	40% of the affected virtual machine(s) and/or hosts monthly subscription charges
100% - 199%	60% of the affected virtual machine(s) and/or hosts monthly subscription charges
200% or more	100% of the affected virtual machine(s) and/or hosts monthly subscription charges

9.4.3. Recovery Time Objective SLA

Recovery Time Objectives apply to High Availability (Live) Virtual Machines and Dual Site Managed Physical Hosts with cold or warm standby servers, The RTO target time is 4 hours. Sungard AS will endeavour to meet the RTO when and if it becomes necessary to fail over to the secondary Sungard AS site. This is measured from the time of Sungard AS's acknowledgement that a site failover is required, until the virtual machine(s) and/or Managed Physical Standby Host(s) have started at the secondary site with the Operating System operational to the required running state.

Note: the RTO to fully recover the application to a consistent state may take longer and is dependent on the application. The responsibility for application recovery resides with the customer or their chosen 3rd party application management provider,

If Sungard AS fails to meet the RTO SLA for the aforementioned server types at the secondary site, then the customer is entitled to a service credit equal to the percentage identified in the table 9.4.3.1 for each month in which the failure occurred.

9.4.3.1. RTO Service Credits

RTO missed by _ %:	Service Credit % of pro-rata portion of Monthly Fee based on affected HA virtual machine(s) and Dual Site Managed Physical Host(s) with cold or warm standby
1% – 49%	30% of the affected virtual machine(s) and/or hosts monthly subscription charges

50% -99%	40% of the affected virtual machine(s) and/or hosts monthly subscription charges
100% - 199%	60% of the affected virtual machine(s) and/or hosts monthly subscription charges
200% or more	100% of the affected virtual machine(s) and/or hosts monthly subscription charges.

NOTE: The RTO service credit agreement applies for all services for which the customer has conducted a failover services test within the previous 6 months.

9.4.4. Service Credit Terms

Sungard AS will pay service credits against failure to meet Server Availability SLA's or Recovery Time and/or Recovery Point Objectives but not both Server Availability SLA failures and RTO/RPO SLA failures in the same month.

Where both server availability and RTO/RPO SLA failures occur in the same month Sungard AS will pay service credits against whichever SLA failure gives the higher monetary value in service credits.

Claims for service credits must be made within 60 days of the service restoration.

9.5. Managed Operating System Services

9.5.1. Managed Operating System - Monitoring and Management

Managed Operating System - Monitoring and Management	
Service Description	The service provides customers with day-to-day monitoring and management of supported operating systems hosted by Sungard AS. Aspects managed include OS availability and performance, software agents and connectivity. The service provides application of fixes where necessary and regular reporting.
Support Hours	Levels 1, 2
Service Dependencies	Service will only be provided to supported Operating Systems, see section 3.6
Monitoring Scope	Including CPU utilisation, memory utilisation, swap space utilisation, file system utilisation, log file monitoring, process monitoring, resource threshold alarms.
Agent Software Included	Monitoring, Management, Anti-Virus
Administrator Access Required	Yes.
Service Scope	This service provides the following: ▶ 24/7 monitoring of the OS for availability using appropriate tools.

Managed Operating System - Monitoring and Management	
	▶ Monitoring and maintenance of backup/restore tasks and resource utilisation. ▶ Assistance with troubleshooting of agents and connectivity issues. ▶ Alert categorisation and incident escalation. ▶ Monitoring of event logs, error reports, scheduled activities, and services, raising and tracking incident tickets as required. ▶ Application of hot fixes and service packs as per maintenance schedules. ▶ Management of server memory; optimisation and configuration of page files. ▶ OS hardening. ▶ Troubleshooting of OS performance issues. ▶ Performance reports (defined at service take-on).
Service Exclusions & Constraints	This service specifically excludes the following: ▶ Management of DNS, Active Directory and LDAP. ▶ Application monitoring. ▶ Other additional Server Services: for example IIS, DHCP, Certificate Services.

9.5.2. Managed Operating System - Anti-Virus

Managed Operating System - Anti-Virus	
Service Description	The service provides system security protection against viruses through monitoring and management tasks.
Support Hours	Levels 1, 2.
Service Dependencies	Managed Operating System - Monitoring and Management.
Monitoring Scope	Anti-virus service is provided only on supported operated systems.
Agent Software Required	Monitoring, Management, Anti-Virus.
Administrator Access Required	Yes.
Service Scope	This services provides the following: ▶ Initial installation and configuration of AV software on all managed Windows OS servers. ▶ Testing and verification of AV and system performance. ▶ Periodic assessment of maintenance and security updates. ▶ Maintenance and management of AV servers and updates of client servers. ▶ Monitoring and reporting on virus alarms; performance of file clean-ups. ▶ Monitoring of product updates and patches, and performance of regular analysis of critical security patches. ▶ Monitoring of CPU, memory, and hard disk drive (HDD) usage on the AV server as well as the AV console and clients. Performance of fixes on client systems. ▶ Root cause analysis and management of incidents for all virus-related calls, raising incidents where necessary. ▶ Regular AV console reports. ▶ Latest virus definitions for all systems.
Service Exclusions & Constraints	Service will only be provided to supported Microsoft Operating Systems only see section 3.6

9.5.3. Managed Operating System - Patch Management

Managed Operating System - Patch Management	
Service Description	The service provides patch management within an environment covered by the Managed Operating System Service.
Support Hours	Levels 1, 2.
Monitoring Scope	Status of managing agent and patch level.
Agent Software Included	Monitoring, Management, Anti-Virus.
Administrator Access Required	Yes.

Managed Operating System - Patch Management	
Service Scope	This service provides the following: ▶ Management of OS files; quarterly assessment of software patches and service packs. ▶ Monitoring of product updates and priority patch alerts. ▶ Deployment of OS patches/updates. ▶ Risk assessment, testing, qualification, application and verification of patches for server software and standard builds. ▶ Management of the patching environment and tools. ▶ Production of regular patch reports.
Service Exclusions & Constraints	Service will only be provided to supported Operating Systems see section 3.6

9.6. Managed Microsoft Application Services

9.6.1. Managed IIS - Monitoring and Management

Managed IIS	
Service Description	The service provides customers with day-to-day monitoring and management of supported Microsoft Internet Information Server instances. Aspects managed include web server availability and performance, software agents and connectivity. The service provides application of fixes where necessary and regular reporting.
Support Hours	Levels 1, 2
Service Dependencies	Service will only be provided on top of supported MS Windows Operating Systems, see section 3.6
Monitoring Scope	Including CPU utilisation, memory utilisation, swap space utilisation, file system utilisation, log file monitoring, process monitoring, resource threshold alarms.
Agent Software Included	Monitoring, Management
Administrator Access Required	Yes.
Service Scope	This service provides the following: ▶ 24/7 monitoring of IIS for availability using appropriate tools. ▶ Monitoring and maintenance of backup/restore tasks and resource utilisation. ▶ Assistance with troubleshooting of agents and connectivity issues. ▶ Alert categorisation and incident escalation.

Managed IIS	
	▶ Monitoring of event logs, error reports, scheduled activities, and services, raising and tracking incident tickets as required. ▶ Application of hot fixes and service packs as per maintenance schedules. ▶ Troubleshooting of IIS performance issues. ▶ Performance reports (defined at service take-on).
Service Exclusions & Constraints	This service specifically excludes the following: ▶ Application monitoring.

9.6.2. Managed Active Directory Servers - Monitoring and Management

Managed Active Directory Servers	
Service Description	The service provides customers with day-to-day monitoring and management of supported Microsoft Active Directory Server instances by. Aspects managed include Domain Controller and Directory Service server availability and performance, software agents and connectivity. The service provides application of fixes where necessary and regular reporting.
Support Hours	Levels 1, 2
Service Dependencies	Service will only be provided on top of supported MS Windows Operating Systems, see section 3.6
Monitoring Scope	▶ Management and monitoring of trust relationships and AD security. ▶ Monitor and manage replication of the AD. ▶ Monitoring of event logs, error reports, scheduled activities, and services.
Agent Software Included	Monitoring, Management
Administrator Access Required	Yes.
Service Scope	This service provides the following: ▶ 24/7 monitoring of MS Active Directory Server(s) for availability using appropriate tools. ▶ Monitoring and maintenance of backup/restore tasks and resource utilisation. ▶ Assistance with troubleshooting of agents and connectivity issues. ▶ Alert categorisation and incident escalation. ▶ Monitoring of event logs, error reports, scheduled activities, and services, raising and tracking incident tickets as required. ▶ Application of hot fixes and service packs as per maintenance schedules. ▶ Troubleshooting of AD performance issues

Managed Active Directory Servers	
	▶ Addition/deletion/modifications of domain controllers as required; modify configuration of AD to reflect changes within the organization (for example new office). ▶ Management and administration of containers within the AD. ▶ Perform import/export of AD information in line with ad-hoc requirements, for example exports of the Global Address List (GAL). ▶ Performance reports (defined at service take-on).
Service Exclusions & Constraints	This service specifically excludes the following: ▶ User, Group and other Directory Administration

9.6.3. Managed Microsoft SQL Database - Monitoring and Management

Managed Microsoft SQL Database instances	
Service Description	The service provides customers with day-to-day monitoring and management of supported Microsoft SQL Server Database instances. Aspects include assuring the availability, performance and connectivity of the database instances. The service provides application of fixes where necessary and regular reporting.
Support Hours	Levels 1, 2
Service Dependencies	Service will only be provided on top of supported MS Windows Operating Systems, see section 3.6
Monitoring Scope	▶ 24/7 monitoring of database instances ▶ Monitoring and maintenance of backup/restore tasks and resource utilisation.
Agent Software Included	Monitoring, Management, Backup
Administrator Access Required	Yes.
Service Scope	This service provides the following: ▶ Validation of database backups ▶ Database user/role password management ▶ Add/remove/modify users to DB Security Configuration ▶ Addition, resizing and configuration of database files and objects ▶ Configuration of Database logical backups ▶ Configuration of Database initialization and tuning parameters ▶ Provision of DB copies (cloning) where required ▶ Configuration of Database Exports ▶ Configuration of monitoring tools for Database Resource thresholds

Managed Microsoft SQL Database instances	
	- Modification of Security Privileges - Database & Table Management - Memory Management - Process Management - Storage Management - Session and Transaction Management using proactive monitoring toolset - Creation and management of Database Management Tasks - Backup/Restoration - Performance Tuning - Log Shipping - Replication - Application of hot fixes and service packs as per maintenance schedules

9.6.4. Managed Microsoft Exchange - Monitoring and Management

Managed Microsoft Exchange	
Service Description	The service provides customers with day-to-day monitoring and management of supported Microsoft Exchange Server instances. Aspects include assuring the availability, performance and connectivity of the Exchange Server instances. The service provides application of fixes where necessary and regular reporting.
Support Hours	Levels 1, 2
Service Dependencies	Service will only be provided on top of supported MS Windows Operating Systems, see section 3.6
Monitoring Scope	- 24/7 monitoring of Exchange Server instances - Monitoring and maintenance of backup/restore tasks and resource utilisation.
Agent Software Included	Monitoring, Management, Backup
Administrator Access Required	Yes.
Service Scope	This service provides the following: - Perform continuous assessments of priority security patch updates - Coordinate and participate in testing of Security Patches prior to production release - Validation of Exchange Server backups - Configuration of Exchange Server logical backups - Configuration of Exchange Server initialization and tuning parameters - Configuration of monitoring tools for Exchange Resource thresholds - Modification of Security Privileges

Managed Microsoft Exchange	
	▶ Memory Management ▶ Process Management ▶ Storage Management ▶ Session Management using proactive monitoring toolset ▶ Creation and management of Exchange Server Management Tasks ▶ Backup / Restoration ▶ Performance Tuning ▶ Replication ▶ Additions, deletions, and modifications to public folders and access rights to folders only as 3rd line of support with customer responsible for end user management activities. Management of public folders replication. ▶ Monitoring and management of Exchange log files, resolution of any issues caused by log files. ▶ Monitoring of backup jobs to ensure that jobs have been completed, and that log files have been cleared down. ▶ Management and support for the Messaging configuration – installation and configuration files, log files, messaging databases and storage groups. ▶ Regular maintenance and defrag of messaging databases, repair and recovery of databases to maximise system availability. ▶ Troubleshooting email delivery issues, NDRs (non-delivery receipts) from source to recipient. ▶ Management of Global Address List entries - custom recipients, mail forwarding, address book views, primary email address changes only as 3rd line of support with customer responsible for end user management activities. ▶ Managing mailboxes – implementation of mailbox policies and limits, moving of mailboxes between storage groups and/or servers. ▶ Producing regular and ad-hoc reports from the messaging infrastructure, using native reporting tools. ▶ Adding, configuring, modifying, and deleting mail domains within anti-spam & content filtering software. ▶ Blocking domains or addresses reported as known spammers. ▶ Management of quarantine and tag levels. ▶ Tool based Reporting on mail traffic volumes, spam volumes, etc. on a regular basis.

Managed Microsoft Exchange	

9.7. Ordering and Invoicing

Please use the contact details at the end of this Service Description for initial enquiries and ordering. Thereafter our Service Management team will provide a single point of contact for subsequent orders.

Billing for the service will be monthly in arrears; this will represent total usage for a month. Payment can be via the following methods:

- Purchase Order
- Direct Debit

9.8. Service Termination

At the point of termination, all your data, accounts and access will be securely deleted; there will be no mechanism to subsequently recover data after this point.

Termination fees may apply for customers who wish to cancel their Managed Physical Host(s) after the 12-month minimum term and before the 24-month contract period ends.

10. Responsibilities

10.1. Customer

You will be required to agree and sign the PSN Code of Connection (CoCo) and will require PSN network connectivity in order to access the platform.

You are also responsible for ensuring only appropriate data is stored and processed by applications within the environment and that they comply with the Sungard AS Acceptable usage policy and PSN information assurance requirements.

10.2. Sungard AS

Sungard AS supports mission-critical operations of financial institutions, businesses, local governments, public safety and justice agencies, and educational institutions around the world. It is through our commitment to doing things the right way and doing them well that we have earned the trust of our Customers to help them with their most critical missions.

Our good name and reputation are based on setting and achieving high standards for how we conduct ourselves. We also believe that as one of the world's leading software and technology services companies we have an obligation to use our size and influence to raise ethical, social and environmental standards wherever we do business. We focus our Corporate Responsibility efforts in three main areas:

- Environmental;
- Social;
- Governance.

Further details are available on request.

11. Contract

Please note that only the appropriate Sungard AS terms and conditions and schedules will apply to the services procured on the Digital Marketplace.

12. Further information

There are a number of documents available on Digital Marketplace covering Sungard AS services.

In order to progress, please contact:

infoavail@sungardas.com

0800 143 413(Monday-Friday, Business Hours Only)