

Question 1.1 Core Services – (Schedule 1a – Section 4) – Question Weighting – 45%

Tenderers will be required to deliver a number of core maintenance services in relation to the following hardware:

- All Server types including Blade; Rack; and Tower options. Maintenance will include all internal server components, for example Processor, Memory, hard-drives and any internal cards;
- Local Area Network (LAN) Infrastructure – Maintenance services appropriate to network switch and wireless access point hardware only. (NOTE: Associated cables and adaptors are not to be included);
- Tape Drives and Tape Libraries: Maintenance services for peripheral devices attached directly to server or to the organisations network infrastructure;
- Keyboard Video Monitor Switch (KVM): Hardware Maintenance only;
- Network Attached Storage (NAS) Devices: Hardware Maintenance only. (Configuration, disk partitioning and backup facilities are not to be included);
- Storage Area Network (SAN): Maintenance services for hardware only including individual disk or shelf replacement. (Configuration, disk partitioning and backup facilities are not to be included);
- Uninterruptable Power Supplies (UPS) – Hardware maintenance only.

Tenderers should provide details of how they will deliver Server and Infrastructure Maintenance services for the core services. Details will include, as a minimum:

- Information on how the Tenderer can deliver the services, detailed above, for In Warranty; Out of Warranty; and End of Life equipment, detailing how each of these can be managed throughout the term of the framework. If relevant Tenderers should include details of how they will operate with manufactures to ensure maximum efficiency and value is achieved in the delivery of the service;
- List of partnerships and levels of accreditation with manufacturers, that are required in relation to providing maintenance on the core services;
- Processes used to verify and accept the Framework Public bodies equipment kit lists including details of any audit process and subsequent management of any kit/equipment register;
- Any relevant accreditations and certificates, where appropriate, that are required in relation to providing maintenance on the core services;
- Details of how the Tenderer will manage the process in relation to spare components including any relevant information as to the storage and confirmation that such components are of a condition (new or otherwise) to meet manufacturer warranties;
- Details of how the Tenderer will manage any changes to a Framework Public Bodies contract requirements (i.e. adding new and/or removing old kit /components) including details of the process they will operate and how changes to invoices is controlled;

- Details of inventory processes used to monitor the contractually maintained equipment, including details of information relating to manufacturer warranty.

Tenderers must also provide details of any Sub-Contractors or Consortia members in delivering the core services along with the services they will carry out.

Tenderers Response:

MCSA have 40 years' experience of delivering multi-vendor hardware maintenance services – providing our customers with support for their critical servers, storage systems, LAN infrastructure and associated peripherals, 24/7, 365 days per year.

As of April 2019, MCSA were acquired by Park Place Technologies – the Gartner-recognised global leader in Data Centre Maintenance, supporting over 15,000 customers across 140+ countries. As a global business, Park Place Technologies employ over 1,400 people (250+ within the UK), and the vast majority of the business being focused on the delivery of IT maintenance support services. Fundamental to the acquisition was the fact that both companies embrace the same customer-centric approach and share a very similar heritage in their core-business of providing exceptional service and support for our clients' data centre hardware.

Being part of this larger organisation brings many benefits to MCSA's customers, both in terms of the increased breadth of our expertise and the improved value we can offer through economies of scale. With regard to MCSA's operational delivery in Scotland, however, it is very much business as usual – with the same local Service Delivery, Account and Framework Management teams delivering the same outstanding service under exactly the same delivery model as we have for the past 30 years.

MCSA propose to utilise our existing Scottish field service team to deliver services to the Framework Public Bodies. We can also provide dedicated on-site engineer resource where required and requested by individual Public Bodies. The existing MCSA field resource will be complemented by the PPT field team along with the global Advanced Engineer Group, consisting of level 3 product experts, many of whom are recruited directly from the OEM following 10+ years in a similar level 3 role.

MCSA's policy of retaining account engagement by engineers who have previously supported specific customers will ensure a seamless continuity of service delivery quality and retain familiarity with the people, processes and culture within Public Bodies that wish to re-engage with MCSA support.

IN WARRANTY / OUT OF WARRANTY / END OF LIFE

MCSA engineers are trained and accredited to deliver warranty support on all major vendors' equipment. MCSA stock is used initially to facilitate a fix within contractual SLA and replacement parts can then be obtained from the vendors to replenish the parts used. This enables MCSA to pass this benefit on to our clients through reduced pricing for equipment which is under warranty.

MCSA's post-warranty maintenance contracts offer the same high level of service for equipment no longer being supported or maintained by the Manufacturer. As a truly vendor-independent maintenance provider, with our own comprehensive spares inventory and parts supply network, we do not differentiate or charge any premium to maintain equipment deemed "end of life" by the Manufacturer. Furthermore, our service is inclusive of all spare components, labour and travel, with no opportunistic additional charges for certain excluded parts – as is common practice among some providers.

VALUE & EFFICIENCY

MCSA have implemented a Framework pricing structure which we believe provides the Framework Public Bodies best value for all services offered. Following the acquisition of MCSA by Park Place Technologies, our pricing structures have been aligned to provide the most competitive prices to Public Sector customers. In addition, we pledge to hold our pricing at the stated rates for the duration of the Framework, without any inflation in line with RPI.

Where there is a requirement for hardware upgrades, MCSA will always leverage our position with the individual vendor (e.g. MCSA are an HPE Gold Partner) to achieve the keenest pricing possible on behalf of clients. Where possible, we will also always help organisations identify the most cost-effective means of procuring software and licencing through any pre-existing agreements they may hold (e.g. Microsoft Open Value Subscription).

We operate a flexible review process with individual customers. Many opt for a quarterly review and reporting on costs is provided as part of this process. MCSA's policy of continual market-price benchmarking, coupled with contract specific continuous-improvement initiatives, ensures an on-going best-value proposition for all our contract clients.

As MCSA's/PPT's core business is server maintenance, we are ideally placed to understand the true cost of delivering support on specific hardware types, and consequently we offer our clients a fair price for servicing which reflects the actual costs incurred by the supplier. For example, if there were no additional spares costs incurred, any cost saving would be reflected in the maintenance price for covering this equipment, to the benefit of the Framework Public Bodies.

VERIFYING KIT LISTS

MCSA have established links to vendors' manufacturing and warranty databases, allowing our administration team to verify the supplied serial numbers against these systems at the point of initial quote generation. If there are any discrepancies, missing or unidentified serial numbers, this information is passed back to the client for further verification. MCSA can identify from the manufacturer serial numbers whether a warranty discount applies and when the warranty expires.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Over the course of the contract, any changes to the kit list, such as adds, removals, location changes etc. are recorded via MCSA's contract management system, and in advance of each contract anniversary we work with the client on a true up/down exercise to ensure our asset register exactly matches the physical estate.

RELEVANT ACCREDITATIONS

MCSA have formal partnership relationships with many of the core manufacturers and vendors associated with the Framework requirements:

- HPE – HPE Partner Ready Gold Partner
- DELL – DELL Warranty Partner
- IBM/Lenovo – Lenovo Premier Authorised Service Provider
- Oracle – Oracle Gold Partner
- Huawei – Huawei Certified Services Partner (CSP)
- Fujitsu – Fujitsu Authorised Service Provider
- Cisco – Select Certified Partner

MCSA engineers have completed accredited training for these programs, and the resulting vendor accreditations enable us to undertake warranty calls in addition to escalation for support.

For example, under our HPE Partner Ready program we are able to get the encrypted AHS (Active Health Server) log file for ProLiant G10's analysed by HPE which enables us to carry out an effective action plan. This is done via our access to HPE Priority Support which is uniquely available to Partner Ready partners against warranty entitled products.

Our engineers hold the following vendor service qualifications relating to the core manufacturers:

- HPE (ProLiant Servers (ISS) SQ, Networks SQ, Storage attached to ProLiant's SQ, EVA SQ, MSA SQ, 3PAR SQ)
- IBM (System X Servers, Bladesystems Chassis)
- Dell (Dell PowerEdge Servers, Dell Blade Servers/Chassis)
- Fujitsu (Fujitsu PRIMERY Servers Fujitsu Blade Servers/Chassis)
- Oracle (Sun Support Engineer, Sun Enterprise Servers, Sun Storage Arrays)
- Cisco (CCNP, SMB Engineer)
- Quantum (Scalar)

In addition, as part of PPT, we have accredited in-house advanced engineering resource across EMC, NetApp and Hitachi technologies available to our Scottish Public Sector clients.

SPARES MANAGEMENT

Thanks to our comprehensive local stock holding and extensive network of suppliers, MCSA have access to an immediately available supply of spare components sufficient to meet all contractual obligations. Such components are guaranteed to be either new, or of a quality and condition to satisfy the manufacturer's guaranteed levels of serviceability for refurbished or reusable parts. Replacement parts used by MCSA are in accordance with manufacturer's guidelines and will not invalidate the manufacturer's warranty.

MCSA's logistics division, together with the Service Delivery Manager and our technical personnel, determine precisely the spares that are required in order to meet all SLAs. This is monitored closely and adjusted where necessary. The MCSA team also have access to the wider Park Place global sourcing team and global support inventory across all OEM's and product ranges regardless of the age of the equipment.

- Costs are adjusted on the database as per SLA.
- Change notification form is updated and returned to customer as per SLA.

This process will take place on an on-going quarterly basis from commencement of contract and will determine the invoice value for the following quarter. The established process ensures that all parties have the opportunity of approving the charges due prior to invoice production.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

INVENTORY

Each item of equipment on cover with MCSA has its own discrete line on our Contract Management System, giving clear visibility of contract dates, SLA, physical location, system ID, serial number, MCSA service history etc. Also included, where relevant, are details of the current warranty status and warranty expiry date. The system is designed in such a way that custom reports can be generated and filtered on any of these fields – allowing a snapshot of the entire inventory or in-depth analysis at a more granular level.

In addition, MCSA can deploy tools, such as Microsoft System Centre Configuration Manager (SCCM) or our own ParkView Proactive Monitoring service, to conduct initial network assessment, ongoing asset inventory management, scheduled detailed network scans, comprehensive, warranty and end-of-life tracking.

Question 1.2 - Optional Services - (Schedule 1a – Section 4) – Question Weighting – 15%

Tenderers may be required to provide optional services to Framework Public Bodies. These may include :

- Operating System: (including Windows, Unix, Linux and Solaris) - Maintenance service relates to the operational readiness and security of the system which includes Operating System re-installation and application of Security Patches and Service Releases;
- Firmware: Maintenance services relating to installation of firmware for server components, LAN Switches and applicable peripheral devices. (SAN Firmware is not to be included);
- Equipment Moves: This will include internal moves within current location and/or external moves to another location
- PBX Equipment: This will only include an organisations telephony related legacy switching equipment (Note: Telephony equipment such as handsets or headsets are not to be included)

- Video equipment: This will only include server equipment related to Video conferencing equipment. (NOTE: video conferencing equipment like handset, screen etc. are not to be included)

Tenderers should include the following information in relation to the optional services. Details will include, as a minimum:

- Information on how the Tenderer can deliver Operating System and Firmware maintenance to In Warranty, Out of Warranty, and End of Life systems, detailing how each of these can be managed throughout the term of the framework.
- Tenderers should include details of how they will operate with manufacturers to ensure maximum efficiency and value is achieved in the delivery of the service;
- Processes used to verify and accept the Framework Public Bodies request for maintenance of Operating System and/or Firmware including details of any audit process and subsequent management of any relevant register;
- Any relevant accreditations and certificates, where appropriate, that are required in relation to providing operating system and firmware maintenance;
- Details of inventory processes used to monitor the contractually maintained equipment - including details of information relating to manufacturer warranty;
- For equipment moves Tenderers should describe the process relating to moving equipment including how the equipment is moved and all controls put in place to manage this securely.

Tenderers must also provide details of any Sub-Contractors or Consortia members in delivering the optional services along with the services they will carry out.

Tenderers Response:

OPERATING SYSTEM AND FIRMWARE MAINTENANCE

MCSA retains a privileged relationship with Microsoft and the core hardware vendors, which enables us to provision Operating System and Firmware support facilities to complement our hardware maintenance delivery. Our engineering teams are experienced in maintaining the operational readiness and security of systems, including OS reinstallation and application of Security Patches and Service Releases.

MCSA have been supporting Microsoft Operating Systems and integrated products for many years. We have been a Gold Certified partner for approaching 20 years and hold Gold Competences on most core Microsoft Enterprise products. Our teams of technical consultants and support specialists can deal with the most complex problems with a direct route of escalation to the vendor where required. MCSA are able to support Framework Public Bodies' Microsoft Operating Systems for hardware irrespective of manufacturer's hardware warranty status and will continue to deliver support on equipment deemed end of life by the manufacturer.

MCSA have extensive experience and qualification for support of Unix and Linux Operating Systems. Again, this provision is available irrespective of manufacturer's hardware warranty status.

MCSA recognises UNIX (including Sun's Solaris, HP's HP-UX and IBM's AIX) and Linux as the leading Operating Systems for stability and security, and the platforms of choice for a significant number of our customers to host their critical systems and applications.

Whether to address a short-term project or long-term skills gap, MCSA can provide a bespoke support service whereby our team of UNIX and Linux experts will provide the required level of help and assistance or resource cover. Our consultants have many years of experience of hands-on UNIX and Linux support and maintenance in customer facing roles and are an ideal extension to our clients' internal teams assisting with the management of their systems.

As an additional service relating to OS maintenance, MCSA have the knowledge, experience and expertise to carry out legacy server emulation on to current-generation, virtualised infrastructure. We have assisted a number of Scottish public sector still relying on mission-critical applications running on their Legacy Dec VAX, Alpha, HP 3000 and SunSPARC systems in just this way – allowing them to retain essential, fully-working legacy applications completely unchanged while removing the dependencies and risk of old hardware at a fraction of the cost.

Through MCSA's vendor partner accreditation we can supply access to firmware updates for HPE, Dell, IBM, Fujitsu and Cisco hardware. For equipment in warranty there is no additional cost associated with this; for equipment out of warranty a separate contract is established with the vendor to run in parallel with the MCSA hardware maintenance provision. Firmware maintenance is not typically requested for end of life products but, where there is a requirement, MCSA are fully equipped to provide this service.

MCSA's contract management system operates in such a way that warranty eligibility is flagged and, where this expires part way through a maintenance contract, we can include firmware support to commence at the relevant date on a pro-rata basis. Where there is a request for firmware support, MCSA will work closely with the Framework Public Body and the vendors to minimise costs by identifying and excluding any equipment where there is no requirement, e.g. in warranty or end of life.

VERIFICATION OF REQUESTS



RELEVANT ACCREDITATIONS

MCSA have relationships with many manufacturers, vendors and partners that enable us to provide full end to end operating system and firmware support services to our customers.

The following list details our support accreditation levels:

- HPE – HP Gold ServiceOne Enterprise Partner
- DELL – DELL Warranty Partner
- IBM – Service and Warranty Partner
- SUN – Oracle Gold Partner
- Fujitsu – Fujitsu Primergy Qualified Service Partner
- Cisco – Cisco SMB Select Partner

- Microsoft – Gold Partner
- HP/Microsoft – Frontline Partner
- Toshiba – Accredited Warranty Partner
- VMware – Enterprise Partner
- Symantec – Registered Partner
- NetApp – Silver Partner
- EMC – Velocity Partner

PBX and Video

MCSA are able to offer our clients hardware support for both telephony related legacy switching equipment and server equipment related to video conferencing equipment in exactly the same way as we do for any other server, storage or networking equipment.

OTHER SERVICES

MCSA have significant experience in delivering data centre services to large Public Sector organisations, where we provide additional support based upon software solutions and service deployment, these include:

- Data Centre equipment installation
- Proactive site visits
- Deep cleaning of servers, storage and associated racking
- Asset management and CMDB
- Supply chain management
- Vendor/technology roadmap days
- Hardware component upgrades
- Disaster recovery service
- WEEE disposal and compliance
- Service Desk
- Remote Monitoring/health checks
- Pre-sales consultancy/Data Centre evaluation
- Infrastructure transition to Cloud deployment

In addition, MCSA have a long-standing partnership with CDG (Scotland) Ltd, whose expertise we utilise for aspects of Scottish Government-specific Infrastructure Consultancy and to deliver a 'hands on site' service for some of our Scottish Public Sector clients with equipment hosted at Saughton House.

BULL SUPPORT

MCSA have extensive experience in successfully delivering high quality technical services to Public Bodies operating on the Bull hardware and software platform. Where we have previously relied on a specialist partner to provide elements of this support, as part of Park Place Technology, we now have full capability in-house to provide the same level of hardware and software support for the Bull environment.

PARKVIEW PROACTIVE MONITORING

In addition to our standard hardware and OS support, as part of Park Place Technologies, MCSA are now able to offer an additional layer of proactive support with ParkView - a revolutionary, award winning, automatic fault monitoring platform that leverages Machine Learning to identify issues down to the root cause in data centre hardware. ParkView works 24/7 to proactively detect faults and significantly improves the speed and accuracy of problem resolution.

Some of ParkView's key features of are:

- **Proactive & Predictive Fault Detection** - ParkView identifies system issues – either as they happen or predictively beforehand
- **Event Management** - Once a fault or event is detected, ParkView instantly self-creates a ticket and identifies the exact nature of the issue and all relevant details to resolve it. ParkView will suppress all non-vital events including soft errors and status updates – only notifying you of issues that are pressing in nature
- **Vendor Agnostic Interface** - ParkView supports a wide range of OEMs, platforms, operating systems and generations. Real-time visibility to all events is enabled via one easy-to-use interface.

ParkView results in Faster, more accurate fixes and more uptime. We typically see incident resolution 31% faster than without ParkView and a first-time fix rate in excess of 97%.

Because ParkView detects the faults proactively, there is no need to contact us to initiate support, run diagnostics or provide log files. This results in an average of just 2 touchpoints between customer and service provider vs. an industry average of 8 – meaning more time for staff to focus on the more strategic initiatives

ParkView is extremely secure, with all outbound data SSL encrypted and security features based on individual client's requirements to ensure that non-public data is never accessed or transmitted

ParkView is provided to our customers with supported storage platforms at no charge and can be purchased for servers and switches as an addition to our standard maintenance contracts.

REMOTE SOFTWARE SUPPORT

Utilising RDP connectivity MCSA's team of consultants can access client systems to investigate any software problems or failures. The support offering covers:

- Most Microsoft products
- Unix/Linux OS
- VMware ESX Server
- BackupExec
- Anti-Virus
- Web / Email Filtering
- Networking (switch, router and firewall management)
- OpenVMS

By utilising this service Framework Public Bodies can benefit from:

- Access to expertise and experience that would be difficult to maintain in house
- Access to Microsoft escalation for the most complex of problems
- Better ROI on staff being able to focus on forward looking Business Development activities
- Peace of mind knowing that infrastructure is supported when staff are busy on other work
- Maindec provide a managed solution and take away the headache

INVENTORY

Each item of equipment on cover with MCSA has its own discrete line on our Contract Management System, giving clear visibility of contract dates, SLA, physical location, system ID, serial number, MCSA service history etc. Also included, where relevant, are details of the current warranty status and warranty expiry date. The system is designed in such a way that custom reports can be generated and filtered on any of these fields – allowing a snapshot of the entire inventory or in-depth analysis at a more granular level.

In addition, MCSA are able to deploy a variety of asset management utilities, such as Microsoft System Centre Configuration Manager (SCCM), or utilise any existing inventory tools currently in use by Public Framework Bodies, to verify pertinent OS/firmware details of the hardware estate.

EQUIPMENT MOVES

MCSA have extensive experience in coordinating equipment moves, including the relocation of Scottish Public Bodies into Scottish Government's shared service at Saughton House in Edinburgh.

MCSA retains local availability of resource and vans to accommodate urgent requests for short notice equipment relocations from Framework Public Bodies.

All moves will be managed safely and securely, following best practice working methods (PRINCE 2 methodology) and making use of appropriate equipment such as GPS tracked vehicles, CRB checked staff, specialist packing and comprehensive insurance.

All equipment relocation includes:

- Determining value and insurance level requirements of the equipment
- Examination of equipment passage and doorways for clearance
- Examination of loading and unloading capabilities at both the originating and destination sites
- Disconnecting and de-installation of the equipment from the network
- Packaging, loading and transportation of equipment
- Reinstallation of the equipment including securing any and all loose hardware
- Verifying, labelling and tightening of all connections

Question 1.4 - Framework Management, and Promotion - (Schedule 1a - Section 8) – Question Weighting – 5%

The Tenderers Framework Manager will be expected to work closely with the Authority and Framework Public Bodies and ensure appropriate resource for each Contract called off from the framework.

Tenderers must provide details of their Framework Manager and Framework Public Bodies Account Manager (if different). The Tenderers response should include as a minimum:

- Experience and qualification (pertinent to this framework);
- How the framework will be supported at a strategic level;
- Account Manager resource to ensure consistent level of service for all customers;
- Details of how the Framework/Account Manager would actively engage with Framework Public Bodies to define, refine and develop service requirements;
- Details of numbers of employees, numbers of field engineers, current major maintenance contracts and geographical spread of service depots should be included.

Tenderers may find it useful to provide examples of previous workshops, presentations webinars etc. that they have provided to Customers to describe how they will assist the Authority in promoting and marketing the Framework Agreement.

Tenderers Response:

MCSA have been supplying server maintenance services throughout the UK for 40 years, and our services have been widely adopted within the Scottish Public Sector since 2005. This includes our highly successful engagement on the current Server Maintenance Framework, through which we maintain servers, storage and networking equipment for a significant number of Framework Public Bodies.

We are proud to hold ISO 9001:2015 certification for the scope of 'sales, marketing, management of servicing, maintenance and technical support of computer systems, including peripherals and networks'.

bsi.



By Royal Charter

Certificate of Registration

QUALITY MANAGEMENT SYSTEM - ISO 9001:2015

This is to certify that: **MCSA Group Limited**
Maldec House
Holtspur Lane
Wooburn Green
High Wycombe
HP10 0AB
United Kingdom

Holds Certificate Number: **FS 34089**

and operates a Quality Management System which complies with the requirements of ISO 9001:2015 for the following scope:

The sales, marketing, management of servicing, maintenance and technical support of computer systems, including peripherals and networks.

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 1996-05-13
Latest Revision Date: 2018-05-11

Effective Date: 2018-05-14
Expiry Date: 2021-05-13

Page: 1 of 1



...making excellence a habit™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated [online](#).
Printed copies can be validated at www.bsi.com/Clients/Directory

Information and Contact: BSI, Blenheim Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: +44 (0)145 330 5000
BSI Assurance UK Limited, registered in England under number 2305321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

Additionally, and complimentary to this, Park Place Technologies also have

a presence within a number Scottish Public bodies for whom we have been delivering high quality services to for a number of years outside of the current framework. The alignment of the two businesses further enhances the breadth, scope and coverage for services that are accessible to Public bodies in Scotland.

The current Server Maintenance Framework accounts for large proportion of MCSA's current business in Scotland, consequently the new Server and Infrastructure Maintenance Framework and all associated contracts will be considered of equally major importance and significance within the company.

The Framework will be highly visible to both MCSA and Park Place Technologies senior management and directors, and prioritised accordingly. We propose the continuation of our well-established, dedicated local management team to coordinate all aspects of our engagement with the Authority and Framework Public Bodies.

MCSA commit to continuing the promotional activities carried out over the course of the current Server Maintenance Framework. Such as: collaborative presentations with Scottish Procurement to raise awareness of the framework with key stakeholders (e.g. NHS National Infrastructure Group, HEIDS etc.); publicising the framework through our Social-Media channels; engaging in targeted framework marketing campaigns; and regularly attending/exhibiting at national and regional events such as Procurex Scotland, P4H, Meet the Buyer and Holyrood Connect,

MCSA have appointed a dedicated Scotland Framework Manager (FM), who reports directly to the Scotland Group Manager (SGM), both of whom are based in our Glasgow office. The SGM is directly responsible for all service delivery and account management functions in Scotland. MCSA adopts a flat organisational structure, meaning the SGM has direct and immediate escalation to the board of Directors for quick and efficient high-level decision making.

The Framework Manager has over 15 years' experience of delivering critical IT contracts to the Scottish Public Sector, and a strong track record of managing similar engagements under the existing Server Maintenance and DATS Frameworks, and the ITMS Framework before that.

Following the award of the Framework Agreement, the FM and SGM will submit a detailed implementation plan to the Authority, detailing the staffing, operational and managerial processes and procedures in place to ensure effective delivery of the Specification and Service Levels outlined in the Schedule.

The FM will have a team of operational and sales administrators to manage orders, mini competitions, marketing and supporting account management duties such as creating quotations, reports and monitoring escalations.

All requested documentation will be provided to the Authority and Framework Public Bodies in a timely manner. A register will be maintained to record all activity and documentation relating to the Framework. This information will be proved to the Authority as part of the Management Information report.

The FM will act as a single point of contact for the purposes of operating the Framework Agreement, be accountable for delivering the Authority's Service Level on responding to framework orders and mini competitions and will also be empowered to make decisions relative to ensuring the Authority's satisfaction with MCSA Framework performance.

FM responsibilities will include:

- Ensuring the effective marketing, mobilisation, implementation, delivery and exit management of the Framework Agreement.

- Extensive Dialogue with the Authority's FM and production of management reporting information.
- Management of partner/subcontractor relationships.
- Coordination of regular MCSA Framework User-Group meetings.
- Active engagement within combined Authority/MCSA Framework promotional/mini-competition activities, discovery days etc.
- Engaging with Framework Public Bodies to help define, refine and further develop service requirements.
- Pricing approval
- Resource priority setting
- Framework team appointments

The Framework client account managers will report directly to the Scotland Group Manager who is proud to have delivered outstanding customer service to MCSA's Scottish clients for over 30 years. The account managers will work alongside the FM to respond to requests from Public Bodies and visit potential/existing customers to ensure that we are in the best position possible to communicate the benefits of utilising the framework in order to receive best value support from an exceptional IT service provider.

The SGM also manages the Service Delivery Manager (SDM), who coordinate all MCSA field/site-based operations. This model operates effectively throughout the UK and allows for cross-fertilisation of Ideas at regular MCSA training events.

MCSA currently has 148 Employees comprising of:

- 111 Technical Personnel (Field Engineers 88, Technical Support 23)
- 37 Management, Personnel and Sales

MCSA's HQ and Central Logistical Support Centre is situated in Wooburn Green, Buckinghamshire where overall logistics, technical support and workshops are located. A nation-wide network of regional service centres in the following areas supports MCSA service delivery to our clients across the entire country:

- Scotland – Glasgow, Edinburgh
- Northern Region – Bradford, Redditch
- Southern Region – Huntingdon, Wooburn Green, Harpenden, Bristol, London

In addition to the above, MCSA engineers and retained contractor engineers are strategically located throughout all regions to give comprehensive, UK-wide coverage.

To provide some context to the total number of UK employees including the wider Park Place Technologies business, we now have in excess of 250 full time employees. All members of the MCSA team have access into all global functions of PPT to provide additional support resources as part of the wider business continuity process for regional protection.



Question 1.5 - Service Desk, Complaints, & Escalation Procedures - (Schedule 1a – Section 17, 23, 24) – Question Weighting – 10%

A Service Desk service is required to receive, log, prioritise and action the maintenance support requests from the Framework Public Bodies

Tenderers must provide details of how their Service Desk will operate and information on the different levels of Service Desk support which can be provided, including the staff providing the support and the mechanism used when raising requests (e.g. phone, e-mail, web portal with live incident tracking).

Responses should include as a minimum:

- How support tickets are managed and the audit trail involved;
- Tuition on the services available (e.g. Web Portal instructions) and any support available on the use of the Service Desk functionality;
- Details of the times that Service Desk is available (e.g. 24/7, Working day, weekends, Scottish bank holidays etc.);
- Information on the different levels of Service Desk support which can be provided, including the staff providing the support (e.g. number of staff, levels of experience) and the mechanism used when raising requests (e.g. phone, e-mail, web portal with live incident tracking);
- Mechanism for managing complaints and their escalations;
- Details of proposed approach to communication with the Authority and/or the Framework Public Bodies on the status of any complaint;
- Details on how issues will be managed and escalated to ensure resolution.

Tenderers Response:

MCSA operate an ITIL compliant, UK-based Service Desk / Call Management System which will receive, log, prioritise and action the maintenance support requests from the Framework Public Bodies.

- All processes based on ITIL V3 Best Practice Guidelines
- 99% of telephone calls answered within 15 seconds by a UK based dispatch team

MCSA's service desk has considerable experience in managing call handling and service requests from the Scottish Government IT support team (ITECS) and other collaborative Public Bodies.

The MCSA call management system has the capability of 'transparently' electronically, integrating with call systems (such as Scottish Government's Assyst platform) and many other types of service management system.

The call system is available 24/7, 365 days per annum (including Bank Holidays) to receive all maintenance requests from the Framework Public Bodies.

The service desk will be a single point of contact, contactable on either a UK local or Freephone number and staffed by employees familiar with both Scottish Government Frameworks and the Framework Public Bodies.

Our call management system accommodates Framework Public Bodies requests for more than one SLA within the same call-off contract as each line item can have its own specific SLA (e.g. 2 Servers on 24/7 SLA; 6 servers on Standard Business Hours)

Call requests can be processed by the service desk via telephone, email and web portal. Additional facilities available from the portal include flexible call management report generation and asset inventory visibility.

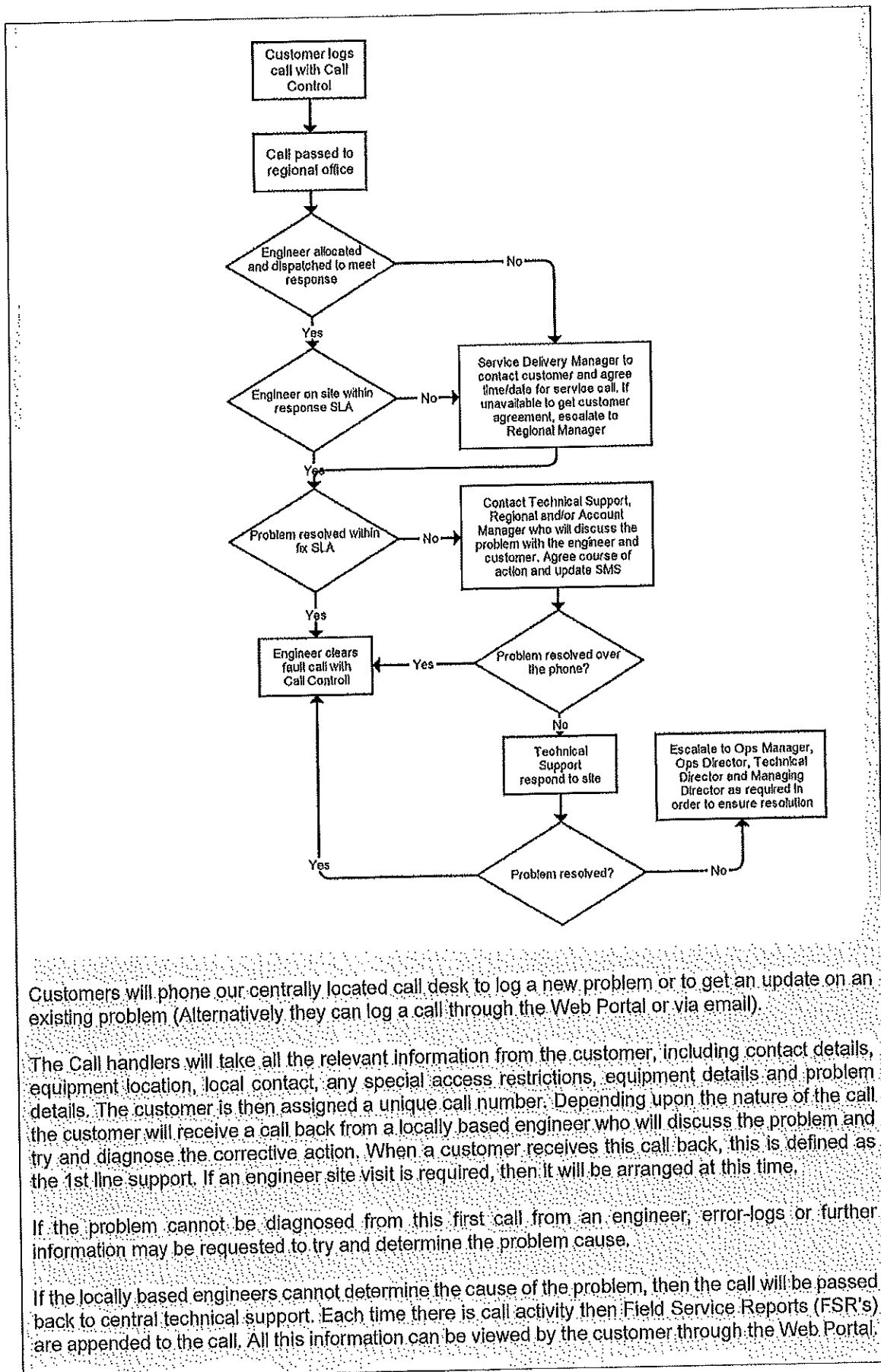
MCSA's on-line portal is extremely intuitive and user-friendly. Full familiarity is quickly achieved via either an MCSA-delivered or on-line tutorial.

The service desk can provision immediate support (in-house help-desk personnel) for Level 1, 2 and 3 technical advice and guidance. The desk can also engage with our vendor partners via dedicated (authorised service partner) support links in order to obtain immediate escalation to the original equipment manufacturers (though rarely necessary).

Each support call logged is assigned a unique call number (ticket). The call number can be used by the client at any time to access the web portal in order to obtain real-time status on call tracking and progress monitoring.

Each support call logged is assigned a unique call number (ticket). The call number can be used by the client at any time to access the web portal in order to obtain real-time status on call tracking and progress monitoring.

CALL FLOW PROCESS



Customers will phone our centrally located call desk to log a new problem or to get an update on an existing problem (Alternatively they can log a call through the Web Portal or via email).

The Call handlers will take all the relevant information from the customer, including contact details, equipment location, local contact, any special access restrictions, equipment details and problem details. The customer is then assigned a unique call number. Depending upon the nature of the call the customer will receive a call back from a locally based engineer who will discuss the problem and try and diagnose the corrective action. When a customer receives this call back, this is defined as the 1st line support. If an engineer site visit is required, then it will be arranged at this time.

If the problem cannot be diagnosed from this first call from an engineer, error-logs or further information may be requested to try and determine the problem cause.

If the locally based engineers cannot determine the cause of the problem, then the call will be passed back to central technical support. Each time there is call activity then Field Service Reports (FSR's) are appended to the call. All this information can be viewed by the customer through the Web Portal.

The status of the call is displayed at all times via call monitor screens at MCSA Head Office as well in each local office. The call changes colour if it gets within two hours of a response being missed or a fix time not being achieved. The colours change again if the call goes outside of the SLA.

The key people involved in call escalation are the Service Delivery Manager (SDM), Regional/Account Manager (RM) and Operations Director (OD).

Additional visibility of an escalation event will be provided to MCSA's Technical Director (TD) and Managing Director (MD).

MCSA will be working continually with customer to resolve an issue, sometimes this will mean that a normal call flow will follow a different path due to customer requirements and agreement e.g. problem is only partially fixed but still allows key customer operation to continue so call deferred to later time.

The service level determines the escalation points.

For example, if the Service level is a 6 hour fix, the escalation points are:

Level 1 is 3 hours after the call has been logged.

Level 2 is 4 hours after the call has been logged.

Actions undertaken at Level 1:

1. The Service Delivery Manager and Regional Manager will discuss action plan with customer.
2. Additional logistics support and technical support are allocated by MCSA.
3. Milestones and notification processes are agreed.

Actions undertaken at Level 2:

1. The Operations director is informed.
2. The Service Delivery Manager, customer and Operations Director discuss situation and agree how to proceed.
3. Additional logistics support and/or technical support is assigned.
4. Further milestones and notification processes are agreed and adhered to until problem is resolved.

When customer agrees problem is resolved De-Escalation process is started.

De-Escalation process

A post-mortem takes place where the Service delivery Manager and Operations Director review the whole process, and discuss the problems that were encountered

COMPLAINTS, ESCALATIONS AND COMMUNICATION

MCSA considers customer focus to be a key principle of Quality Management and customer feedback is a vital tool for organisations to assess satisfaction with its services. Effective customer feedback management can improve the reputation, credibility and image and improve customer confidence and satisfaction. Our quality systems incorporate procedures on corrective and prevention action which are integral to managing and learning from complaints and customer feedback. Our quality management system is certified and complies with the ISO 9001 standard.

A complaint is an expression of dissatisfaction, whether justified or not, however made, about the standard or delivery of service, the actions or lack of action by MCSA which affects an individual service user or groups of users, or a policy we adhere to.

Complaints can be made by telephone, in person, in writing or by email to any member of the MCSA framework team. This will be forwarded to the Service Delivery Manager (SDM) and/or the Framework Manager (FM) as applicable, who will acknowledge the complaint along with a full action plan and expected timescale for resolution within 2 working days, and advise the Authority within 5 days of receipt.

All complaints are logged on our customer feedback register, identifying complainant, issue, date and manner received, acknowledgement date, response date, status and resolution. If a response cannot be made within the timescale, the complainant is kept informed and given a revised timescale for the response. Additionally, advice will be given regarding the next stage of the complaint procedure and points of escalation. The SDM/FM will engage all appropriate resource as necessary to provide the response, which may include involvement of the customers equivalent peer level or line management of complainant.

The SDM/FM will then check with the complainant if they are satisfied with the outcome and the matter resolved. If so, the register is updated, and the issue closed. If not, the issue remains open and is escalated to the Scotland Group Manager to draft a response, and the SDM/FM updates the register as appropriate. The SDM/FM will then follow up with the complainant, and if the matter is still unresolved to the satisfaction of the complainant, the issue remains open and is escalated to the Managing Director or another Board member for review and response. The SDM/FM will continue to update the register.

Monthly audits are undertaken to ensure adherence to our customer feedback procedure. In addition, our quality management team performs a biannual review of all feedback, where all complaints are analysed to determine the root cause of each issue. The review's findings are examined at our management review meeting to establish if our processes can be amended to improve customer satisfaction.

All customer complaints are logged in our register and are not closed until confirmation that the issue has been resolved is received from the complainant. Again, this confirmation can be received by telephone, in person, in writing or by email.

In addition, non-conformance issues discovered by our monthly audit procedure are also logged in our register and investigated by the same method as a customer complaint. Compliments and praise are another rich source of customer feedback and are therefore also logged in our register and acknowledged. All feedback records are reviewed every 6 months and the results examined at our management review meetings.

ESCALATION AND MANAGEMENT OF ISSUES

MCSA's Regional Service Delivery Manager monitors all metrics relating to service levels and engineering activity on a daily basis using a dashboard view and, where necessary, will invoke a formalised and effective escalation process which is capable of handling all operational matters.

- 1st Level – Dedicated Framework Manager
- 2nd Level – Scottish Regional Manager
- 3rd Level – Managing Director

The Scottish Regional Manager is directly responsible for service delivery and account management functions in Scotland. He has direct and immediate escalation to the board of Directors for prompt and efficient high-level decision making.

Any issues regarding non-operational aspects will be handled by the dedicated Service Delivery Manager (SDM) who will organise the required management team to provide a resolution.

This in-depth approach avoids the single point of failure and draws upon a wider knowledge base which includes technical, commercial and managerial engagement.

MCSA place a high degree of emphasis on managing and resolving problems and include Problem Management as a matter of course in all our Managed Services and Support Contracts as a mechanism to drive continuous improvement through day to day service delivery, as well as more formally as part of monthly/quarterly Service Reviews with customers.

Customer Service Improvement Planning is an agenda item for these reviews and actions are discussed and minuted. It is often the case that actions are shared between customer and supplier which is reflective of the partnership approach that MCSA fosters.

Question 2.2 – Malicious Software – (Schedule 1a Section 21) – Question Weighting – 28%

Any components used or supplied by the Tenderer shall be checked and certified and certified malicious software free by the tenderer. It shall be the Tenderer's responsibility to put right, at no cost to the Framework Public Body, and with no resulting delays in attending to other repairs, any damage caused by any breach of this requirement.

Tenders are asked to describe their internal processes and operating rules

Tenderer Response:

MCSA implement and maintain an Information Security Management System (ISMS) certified as meeting the ISO/IEC ISO27001:2013 international standard.

bsi.



By Royal Charter

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that: **MCSA Group Limited**
Maindec House
Holtspur Lane
Wooburn Green
High Wycombe
HP10 0AB
United Kingdom

Holds Certificate Number: **IS 657140**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The processing of customer information in the provision of managed IT services and the support work carried out by their support staff located on-site, at the MCSA Maindec House, Headquarters premises in High Wycombe, in accordance with the Statement of Applicability Version 2 dated 09/01/2017.

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2017-02-09
Latest Revision Date: 2018-10-11

Effective Date: 2017-02-09
Expiry Date: 2020-02-08

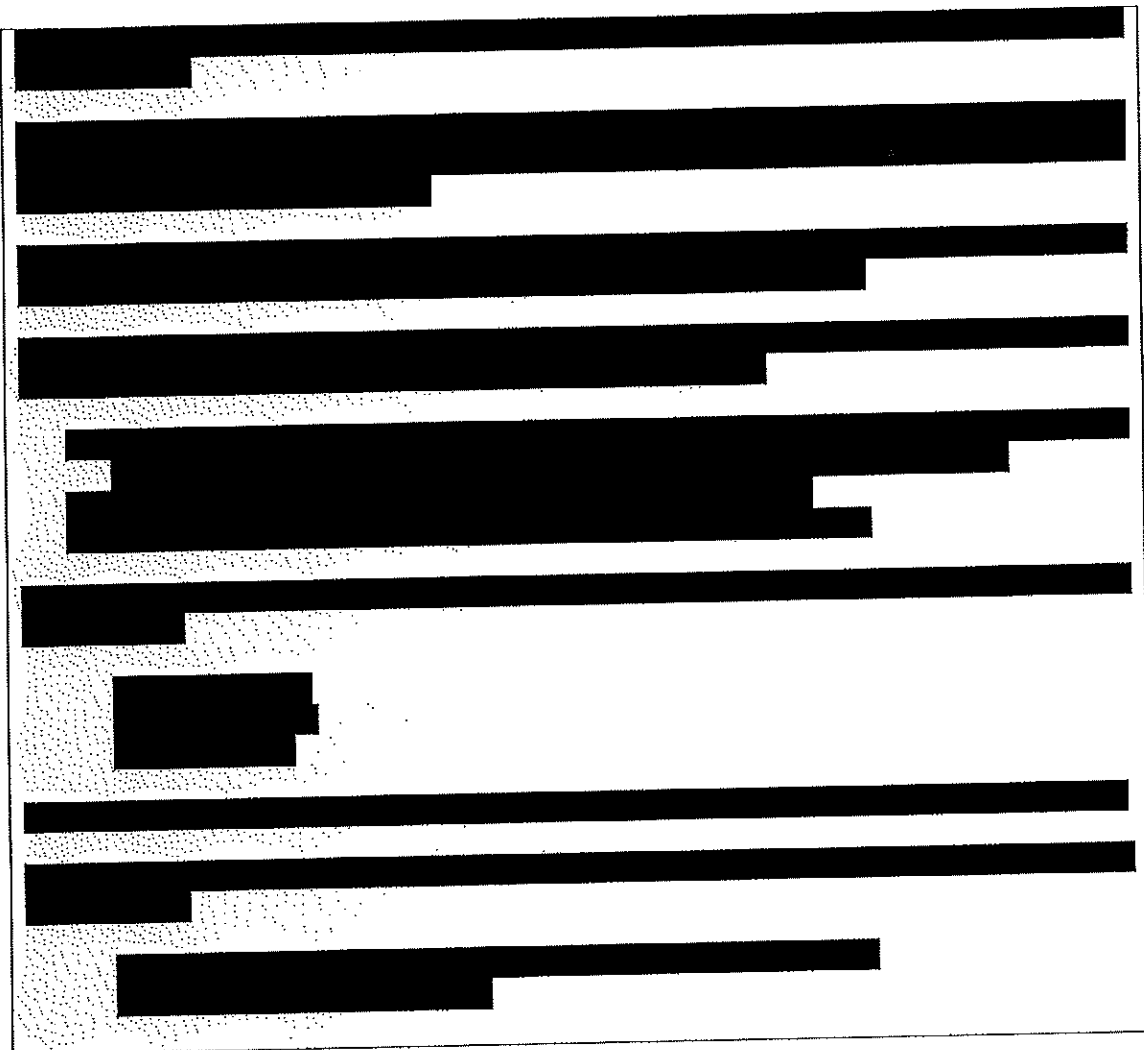
Page: 1 of 1



...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract. An electronic certificate can be authenticated online. Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Paternoster Court, Deodar Avenue, Knowlton, Hillen, Raynes HR5 9PP. Tel: +44 344 830 0000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.



Question 2.3 - Risk Management – 28% (Schedule 1 – Section 32) – Question Weighting – 28%

Tenderers will be required to have a suitable Risk Management Strategy, including a detailed plan, in place in relation to the Server and Infrastructure Maintenance framework.

Tenderers should provide details of their own Risk Management Strategy which should include, as a minimum:

- An overview of the Risk Management Strategy;
- A copy or details of the Risk Management plan in relation to the delivery of the services to Scottish public sector;
- Information on how the Tenderer plans for any potential future risks and what process they have in place to identify these.

Tenderer Response:**RISK MANAGEMENT STRATEGY**

MCSA's Risk Management Strategy includes: the identification of risks, the assessment of risks, risk reduction and planning, risk monitoring and reporting, and feedback on lessons learnt. Risk management is a continuous process throughout the framework lifecycle.

Risk Identification

MCSA believes the key to good risk management is identifying all potential risks that can cause problems. We understand that it does not matter how good the risk assessment or action plans are, if the key risks that are going to affect the framework are not identified then risk management is worthless.

As a starting point for identifying risks we first define and agree the success criteria. The top-level risks are those where the success criteria are not met. Identifying the success criteria also ensures that all framework team members are working towards the same success goals.

MCSA's risk identification process involves thorough and systematic research of the framework requirements, plans, proposed technologies and techniques, requirement specifications, contract conditions and potential sub-contractors and suppliers.

Where appropriate we routinely carry out a series of informal or formal interviews with internal and external stakeholders

MCSA understands that the effective identification of risks requires experience, lateral thinking and common sense, it is therefore essential to conduct a peer group review involving different functions to draw out and organise information.

In addition, looking at the risks from another point of view, such as the customer or a subcontractor, helps highlight previously unidentified risks.

In summary, risk identification is a group activity involving all functions, and is not left to one person to identify the risks. MCSA's key techniques for risk identification are:

- Define framework success criteria
- Undertake systematic research of the framework, requirements and plans
- Carry out expert interviews
- Conduct peer group review involving different functions across the whole framework

The Framework Manager will review the risks identified each month in order to monitor the changes in risk and the effect on the framework delivery.

Risk Assessment

Risk assessment is the method used to prioritise the relative importance of the risks that have been identified and assigning contingency. Each risk is qualitatively assessed in terms of its probability of occurring and its impact on the framework if it did occur. Each risk is also quantitatively assessed to determine its cost to the framework if it occurred. This is done during the brainstorming session when identifying the risks. Many risks can only be assessed on the basis of experience, judgement, intuition or history.

Probability of Risk Occurring

The probability of the risk occurring is assessed in terms of high (>50%), medium (20%-50%), or low (<20%).

Impact on Framework

The impact of the risk on the framework is broken down into

- Timescale; how much overrun/delay on delivery will there be?
- Cost; how much cost overrun will there be?
- Performance; how many requirements will not be met, including reliability and maintainability?

The impact on other areas may also be relevant, such as contractual obligations, and these are also included in the assessment.

Risk Mitigation and Fall-back

All risks that have a significant impact have an action plan for mitigation and fall-back. Where required immediate action is taken to eliminate or reduce some key risks. Once the immediate short-term risk reduction actions have been done then the longer-term actions are tackled.

Risk mitigation can be by:

- Risk Prevention - take action now to prevent the risk from occurring.
- Risk Protection - take action which will reduce the impact, e.g. by considering an alternative option
- Risk Transfer - reduce or remove the risk by transferring it in time or ownership

Risk Mitigation Plan

The risk mitigation plan forms an integrated part of the overall Framework Management Plan and contains the following information:

- Description of the action plan, indicating the approach to be adopted in reducing and controlling the risk throughout the lifecycle of the framework
- Identification of the owner of the risk who will be responsible for ensuring that the actions are carried out efficiently and effectively
- A completion date that everyone is committed to
- The estimated costs of carrying out the action plan
- Comments on the status of the action plan and the risk trends including successes or problems in the effectiveness of the action plan

Every risk action plan has an estimated cost associated with it in order to establish if it is achievable. The objective of any risk action plan is to get all risks to a tolerable level as cost effectively as possible. It is not to remove all risks totally since this is too costly and is generally not possible.

Fall-back Plan

The risk action plan does not only include the long-term and short-term plans, but also fall-back plans in case the action plan does not work, and the risk becomes a problem. The fall-back plan includes well-defined triggers, at which point the fall-back plan is put into place. The triggers result from early symptoms of the issue going wrong, leaving time for the contingency plan to work.

Secondary/Future Risks

The risk action plan in itself often creates further secondary risks that are identified, analysed and reduced. For example, where the action plan is to use a different subcontractor, this will also have its own risks associated with it. These are identified and an associated risk action plan produced.

Any changes made to the framework, such as requirement changes, will alter the risks and will create new risks. It is for this reason that MCSA plan to review all the risks identified, with their associated action plan, secondary risks and fall-back plans, at regular intervals, especially when any changes are made.

Risk Monitoring and Re-Assessment

It is acknowledged that, throughout the lifecycle of the framework, the risks will change. MCSA will, therefore, monitor and update the risk assessment and risk action plan on a continuous basis. The risk register will be re-assessed regularly across the different functions of the framework team.

Monitoring involves:

- Identifying new risks as they appear
- Identifying old risks that rise to a risk factor of 9 or above
- Identifying old risks that have successfully been managed below a risk factor of 9
- Identifying action plans that are not working
- Updating the action plans to reflect the changing situation

Monitoring risk management requires continual monitoring of the framework progress against the success criteria and the risks identified. MCSA will utilise monitoring techniques, such as graphically recording key aspects, such as required intervention rate or service calls raised per week. Any anomalous points or adverse trends of the graph will be investigated as they may indicate a problem occurring.

Risk Register & Reporting

All identified risks throughout the life of the framework will reside in and be tracked through a Risk Register. The Risk Register is thus a central library that contains all identified risks and any amendments or updates made to those risks. The Risk Register will contain a history of updates in addition to the original risk report raised. Even when a risk has been deleted or resolved it will remain in the register. Thus, at the completion of the framework the Risk Register will contain a complete history of identified risks and any action taken to avoid the risk occurring or any corrective action taken.

The risk register will be reported to both MCSA Senior Management and the Authority with the quarterly Framework Management Information Report.

SERVER MAINTENANCE FRAMEWORK KEY RISKS

MCSA identify the key risks involved in the delivery of the Server Maintenance framework as spares availability, engineer availability, business continuity and training and knowledge. MCSA mitigates all of these risks as follows:

[REDACTED]

[REDACTED]

[REDACTED]

Engineering Resource

MCSA currently provides, and can continue to provide if requested, a resident engineer onsite at the Scottish Government's Saughton House location. The resident engineer forms part of a Primary Support Team aligned to Scottish Government. The team operates on a buddy system basis ensuring there are always engineers immediately available in the event the resident engineer is unavailable e.g. during any period of holiday or sickness. MCSA will have in place at the commencement of the framework a team of pre-security cleared engineers, both from our local and adjacent regional centres. Further back up is available from our HQ Technical Support team.

Business Continuity

MCSA have a full Business Continuity plan which includes service desk and engineering. A copy of the full plan is available if required.

MCSA now also have access into the wider PPT global functions to further enhance the risk mitigation plans associated to the delivery of these services. Spares and engineering resources could easily and efficiently be provisioned in the event of any regional losses of either facilities and or personnel. Following the acquisition of MCSA and the ongoing integration process, PPT also have all contract information including asset registers/schedules to further bolster the above policy.

Training & Knowledge

Technology refreshes are commonplace and MCSA have 40 years' of experience in dealing with keeping up to date with the latest technology offerings. All MCSA engineers are provided with comprehensive training both in-house and from vendors to ensure they are up to date with the latest technology offerings. MCSA engineers consequently hold a very large number of vendor technical accreditations.