SA GROUP

G-Cloud 15

Managed Service – Secure IT Support

ISO 22301 Business Continuity Management

ISO 9001:2015 Quality Management

ISO/IEC 27001 Information Security Management

CYBER ESSENTIALS CERTIFIED PLUS

ISO / IEC 20000-1 Certificate No. SM20006

Proudly employee owned.

Crown Commercial Service Supplier

ARMED FORCES COVENANT

EMPLOYER RECOGNITION SCHEME

GOLD AWARD

Managed Service – Secure IT Support, protecting you and your client's data
When you are storing and processing data of a classified nature, it is important that your IT support provider understands the need for compliance as well as competence to manage a secure IT infrastructure and network. It is imperative your IT support provider understands your business and the needs of your users.

SA Group's Secure IT Support puts your users and the data on your systems central to our service. We know there is no compromise when it comes to the security and protection of you, your assets and the reputation you hold with your clients.

How do SA Group compare to other Managed Service Providers?

Our unique 'Secure IT Support' focuses on security and the handling of classified information and data. Our approach ensures full compliance with the UK Government Security Classification (GSC) policy and Cyber Essentials Plus, providing highly secure and resilient IT environments.

By partnering with SA Group, you will benefit from a fully managed Secure IT support service that not only ensures seamless IT operations but also prioritises security and compliance with government policies. Our expertise over 15 years of working within Government Departments, handling classified data, coupled with our adherence to GSC policy, NCSC guidance and Cyber Essentials Plus, makes us the ideal partner for a buyer that requires the highest level of security assurance.

SA Group's Secure IT Support contains several features and services that you would not typically find in a standard service (shown in the image below). Not every feature will be required, and we will tailor a support agreement around your specific requirements.

Secure Infrastructure Management
Monitoring, patching, and maintenance of IT systems to ensure security and optimal performance.

Regulatory Compliance & Auditing
Ensuring adherence to GSC policy, Cyber Essentials Plus and other critical standards.

Incident Response & Threat Mitigation
A proactive approach to identifying and mitigating security threats.

Classified Information Handling
Secure processing, storage, and transmission of classified data in compliance with GSCP.

Endpoint Security Management
Deployment and management of endpoint protection solutions.

Identity and Access Management
Implementation of strong authentication measures to enforce role-based access controls.

Our minimum standard to support any IT infrastructure is Cyber Essentials Plus, why?

Cyber Essentials is a UK Government-backed certification scheme that keep your organisation's and your customers' data safe from cyber-attacks.

The NCSC recommends Cyber Essentials as the minimum standard of cyber security for all organisations.

Cyber Essentials: A combination of self-assessment and independent audit.

Cyber Essentials Plus: The same protections, but with more rigorous, independent technical testing.

Cyber Essentials Plus includes all the requirements of Cyber Essentials but adds a crucial layer of independent verification through hands-on technical assessments. The key additional criteria that distinguish Cyber Essentials Plus from the basic Cyber Essentials certification is:

Vulnerability Assessment & Scanning – Internal & External

- NCSC approved certified assessors conduct an internal scan of end-user devices and network infrastructure to identify vulnerabilities that could be exploited by cyber threats.
- Assessors perform external vulnerability scans to test the effectiveness of firewalls, patch management, and internet-facing systems.
- Checks are made for unpatched software, insecure configurations, and compliance with security policies.
- Assess if any exposed weaknesses could be exploited remotely.

Endpoint Security Testing

- Security of workstations, laptops, and mobile devices are tested, including:
  - Malware protection effectiveness
  - Application whitelisting or blacklisting
  - Privilege escalation risks
- Assesses whether anti-virus, endpoint protection, and security policies are enforced correctly.

User & Access Controls Validation

- Tests the enforcement of multi-factor authentication (MFA) and least privilege access.
- Ensures that accounts with administrator rights are appropriately restricted.

Email & Browser Security Testing

- Assessors simulate common attack vectors, such as phishing emails or malicious downloads, to see if systems block or mitigate them.
- Ensures that web browsers and email clients follow best security practices, such as blocking untrusted scripts or links.

Secure Configuration & Patch Management Checks

- Independent auditors verify that:
  - All devices have critical security patches installed within recommended timeframes
  - Unnecessary services, ports, or software are disabled to reduce attack surfaces
  - Default passwords and insecure settings are properly managed

Simulated Cyber Attack Testing

- Conducts real-world attack simulations on internal and external systems to test resilience against threats.
- Ensures detection and response capabilities are effective.

Why Cyber Essentials Plus?

Cyber Essentials Plus provides a **high level of assurance** because it is backed **by independent technical validation**. As we are dealing with Organisations that require a **stronger cybersecurity posture**, handling sensitive or classified data, makes this a pre-requisite for our service. We maintain all secure IT infrastructure to this minimum standard 100% of the time.

Additional benefits partnering with SA Group

SA Group is an approved Industry Personnel Security Assurance (IPSA)[1] company

IPSA is a personnel security assurance framework for companies to sponsor contractors and workers for National Security Vetting[2] (NSV) to effectively manage and provide the same degree of aftercare[3] as vetted staff are in His Majesties Government (HMG). This applies whether workers are directly employed by the company or are employed within their supply chain.

SA Group Managed Services resources hold NSV, minimum Security Check (SC) Clearance

National Security Vetting is essential for individuals who require access to sensitive UK government information, assets, or locations. The key benefits NSV clearance brings to SA Group resources:

- Enhanced Trust and Access
  - Grants individuals access to classified information and secure facilities
  - Enables work on government or defence-related projects
  - Ensures organisations can trust employees with sensitive national security matters
- Strengthened National Security
  - Ensures that only trusted personnel handle critical information
  - Reduces the risk of insider threats and espionage
  - Supports the protection of national assets and infrastructure
- Compliance with Security Standards
  - Aligns with government and industry security requirements
  - Ensures that organisations meet legal and regulatory obligations for handling classified data
  - Demonstrates due diligence in personnel security management
- Improved Organisational Reputation
  - Companies with vetted employees are more likely to secure government contracts
  - Strengthens business credibility in high-security industries

---

[1] https://assets.publishing.service.gov.uk/media/60b896bd8fa8f57ce980b579/IPSA_Policy_May_2021.pdf

[2] NSV is a protective safeguard applied by HMG as a means of assuring the suitability, integrity and reliability of workers within government service and throughout government supply chains. NSV is granted to individuals on a case-by-case basis following a series of assessments. It is required to have access to classified materials, information, individuals, facilities and systems.

[3] The ongoing monitoring activities that support individuals holding National Security Vetting over the lifetime of their clearance to assess their ability to have continued access to classified material.

- Provides assurance to stakeholders regarding security measures

- Long-Term Security Assurance
  - Ongoing monitoring helps maintain personnel integrity
  - Encourages individuals to maintain high standards of personal and professional conduct
  - Reduces the likelihood of security breaches over time

SA Group Service Management

Incident Management

All incidents are logged with the SA Group Service Desk and will go through our incident management process, described below, under the oversight of our Service Desk Coordinator:

1. Prioritisation Matrix:

Impact → / Urgency ↓	High Impact (Organisation-wide outage, major financial risk, compliance/security breach)	Medium Impact (Group level disruption, moderate risk)	Low Impact (Individual user issue, minor inconvenience)
High Urgency (No workaround, immediate attention needed)	**P1 - Critical** (System down, major data loss, security breach)	**P2 - High** (Significant disruption, partial outage)	**P3 - Medium** (Affecting workflow, but workaround available)
Medium Urgency (Limited workaround available, urgent but not critical)	**P2 - High** (Degrading performance, potential risk if unresolved)	**P3 - Medium** (Affects some users, workaround exists)	**P4 - Low** (Minor issues, cosmetic problems)
Low Urgency (Non-disruptive, workaround available, minimal business impact)	**P3 - Medium** (Intermittent issue, causing frustration but not business-critical)	**P4 - Low** (Minor inconvenience, resolution can be scheduled)	**P4 - Low** (Non-urgent request, general inquiry)

2. Heat Map Explanation

- P1 - Critical:
  - Immediate response, highest priority (e.g., major security breach, full network outage).
- P2 - High:
  - Quick action required, significant business disruption (e.g., major service degradation, security alerts).
- P3 - Medium:
  - Non-urgent but important, affecting multiple users (e.g., software bug, non-critical system issue).
- P4 - Low:
  - Minor issue, cosmetic fix, or routine request (e.g., password reset, small UI glitch).

The Service Desk Coordinator will determine the initial priority rating for the request; the assigned engineer may then discuss this further with the customer to modify this priority as investigation and resolution progress.

Service Categories and Service Level Agreements (SLAs)

Our structure to Service Categories and SLAs ensures:

- **Clarity -** Clearly defined expectations for each service category.
- **Accountability -** Stakeholders understand response and resolution targets.
- **Measurability -** Easy tracking of SLA compliance.

Service Category	Priority Level	Response Time	Update (every)	Resolution Time	Escalation Process
Incident Management	P1 – Critical	30 mins (Call)	1 hr	8 hrs	Immediate Escalation to Senior Engineer
	P2 – High	1 hr (Call)	4 hrs	20 hrs	Escalation after 4 hours if unresolved
	P3 – Medium	4 hrs (Notification)	12 hrs	40 hrs	Escalation after 12 hours if unresolved
	P4 - Low	4 hrs (Notification)	40 hrs	96 hrs	Escalation after 32 hours if unresolved
Service Request	Standard	4 hrs (Notification)		24 hrs	As required
Change Management	Emergency	30 mins (Call)	1 hr	8 hrs	Immediate escalation
	Planned	24 hrs (Notification)		Scheduled	N/A

Points to note in relation to SLAs

- All timings are within our stipulated working hours for the service, 0900hrs to 1700hrs (UK time).
- Resolution time may be affected by availability of users, where user engagement is required to resolve any non-availability will be recorded.
- Where a resolution could be time bound i.e. happening at a specific time in a day or day in a week, this may impact the ability to meet resolution time. This will be recorded.
- Where a resolution is dependent on a third-party vendor or supplier, any delay on their part may affect our ability to meet an SLA. This will be recorded.
- Where procurement of hardware or software is required to meet an SLA, the ‘clock’ on SLAs shall stop once the Third Party Supplier has been contacted either by email or phone to place the order. It shall restart once the product has been accepted by SA Group, which includes SA Group’s defined acceptance process of receipting and then testing.

Service Request

The definition of a service request is a formal user request for information, access, or a standard IT service that does not involve an incident or failure. It will **likely follow a pre-approved workflow and has minimal impact on company operations.** Examples include, but are not limited to:

- User Access & Permissions:
  - New employee onboarding (user account creation, email setup)
  - Access request to a shared drive, system, or application
- Hardware & Device Management:
  - Request for a new end point device

- Installation or upgrade of approved software
- Software license allocation

- Communication & Collaboration Tools:
  - Email distribution list creation or modification
  - Shared mailbox or calendar setup
- Security & Compliance:
  - Multi-Factor Authentication (MFA) setup/reset
  - Request for encryption or secure file transfer

Change Management

The subtle difference of a Change Management Request (Change Request or RFC - Request for Change) is that it is a formal proposal to alter an IT service, infrastructure, or process. The change must be assessed, approved, and implemented in a controlled manner to minimise risk but also to manage potential service disruption. They are prioritised as 'Emergency' or 'Planned' and are defined below with typical examples:

Priority	Definition	Typical Examples
Emergency	High-impact, urgent changes that must be implemented immediately to resolve critical issues	• Applying a critical security patch to prevent a cyberattack • Responding to an immediate security threat, directly affecting operations • Replacing failed hardware in production
Planned	Requires detailed risk assessment, approval, and planning before implementation	• Migrating a database to a new server • Significant deployment of new or updates to existing software that may affect operations • Upgrading hardware, requiring reboots • Modifying firewall rules • Anything which would take critical service offline for a time • Standard responses to security, compliance or CE+ accreditation

Out of Hours Support

SA Group can provide an out-of-hours service, details for this additional service are available on request. Bespoke options are possible but will need to be assessed, reviewed and agreed separately to this proposal.

All fixes, outside of any pre-arranged out-of-hours service, will be charged at a standard out-of-hours rate. Any chargeable requests for out-of-hours work must be authorised and endorsed, in writing, by the Buyers authorised primary contact before work commences.

What's the process to migrate your Microsoft 365 licenses to SA Group?

It's a quick process and we won't need to reinstall software on your computers or disrupt your users. If you have already paid for 1-year licenses direct with Microsoft, we'll postpone transferring these individual licenses until they're close to renewal.

Microsoft New Commerce Experience (NCE)

Microsoft's NCE is a new way to buy Microsoft subscriptions affecting Microsoft 365, Dynamics 365, and Windows 365. The new pricing plan covers two options for licensing:

- Pay as you go: More flexible but costs 20% more. Billed on a monthly basis.
- Annual Commitment: Cheaper but you're locked in for the term. Also billed monthly, year or multi-year options are available.

Never fear, we will work with you to put together the best licensing option to give you the best price possible but retain flexibility where needed.

What happens to our Microsoft 365 licenses if we move away from SA Group?

We understand that you don't want to feel tied in. We have a simple process to move you to another partner, if required.

General Financial Terms

- Invoices are subject to 30 days terms.
- All prices quoted are exclusive of VAT.

Contract Period and Termination

The support proposal is designed to be flexible enough to meet the needs of the buyer over the course of the contract. The duration of this contract will be thirty-six months from the contract start date above.

- Secure IT Support & Enhanced Security & Protection costs are fixed for the thirty-six-month contract period.
- Direct Microsoft Software and Productivity licensing cost are subject to change, and they will be revised on an annual basis.
- A whole contract review will be conducted before the end of the thirty-six-month term.
- A review/break clause can be exercised annually at the twelve-month anniversary of the start date.