touchstar
access | time | CCTV

Phone: +44 (0) 845 3379 155
Email: info@touchstar.co.uk
Web: touchstar-atc.com

TouchStar ATC

ACCESS CONTROL BUYERS GUIDE

CONTENTS

Introduction 3

1. The Start Point 3

2. Legislative Compliance 4
   - DATA PROTECTION ACT 4
   - GDPR 4
   - HUMAN RIGHTS ACT 4

3. Supplier Selection 5
   - ACCREDITATION / CERTIFICATION 5
   - CASE STUDIES/TESTIMONIALS 6
   - SERVICES 6
   - INSURANCE 6

4. The Survey Process 7

5. Types of Access Control System 7
   - AUDIO/VIDEO 7
   - STANDALONE SYSTEM 7
   - NETWORKED SYSTEM 8

6. Access Control Software 9

7. Access Control Devices 9
   - LOCK TYPES 9
   - READER TYPES 10
   - GATES, BARRIERS AND TURNSTILE CONTROL 11
   - KEYPADS, INTERCOMS AND EXIT BUTTONS 11
   - INTERFACES 12

8. Cost 12

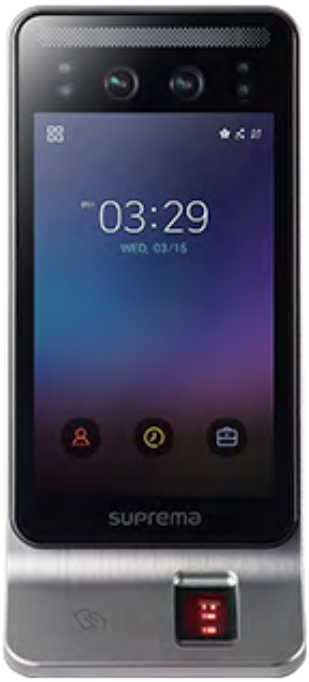
9. System Installation and Training 13

10. Commissioning & Handover 13

11. Service Support & Maintenance 14

12. Conclusion 14

INTRODUCTION



Managing employee and visitor access rights at single or multiple locations can become a complex task with many moving parts. At TouchStar ATC, we have been supplying tailored security solutions to businesses across a variety of sectors for more than 30 years.

Using our extensive experience in access control systems, we have created this buyer guide that will help support you on your way through to the purchase of a new or upgraded system.

Covering everything from starting out, defining your system requirements, supplier selection and legislation through to types of systems and system support, we take you through the steps to help you determine the best fit solution for your premises.

1. The Start Point

At it's core, access control is a method of electronically limiting entry to certain locations to improve security and better manage employee and visitor access at single or multiple sites.

The demands on any access control installation will vary from sector to sector. The first step towards designing a new system is to nail down exactly why it's needed and what it needs to achieve. Building security – essentially, being able to control who can and cannot enter premises – is often the main reason for looking to implement a new solution, but the motivations behind this need are often more complex. Different organisations will have differing objectives in mind; a school or university may be driven by a need to safeguard students and staff, while a warehouse or manufacturing company may be more interested in creating security and audit trails.

Whilst today's systems offer numerous operational and cost benefits, they are not faultless. Whatever the need, it is important that you take the time to thoroughly appraise your current organisational premises and set up at the outset. Choosing a best fit solution can really optimise security operations within any operation, ensuring they become more effective, more efficient, and more fit for purpose.

Some of the most common reasons for installing an access control system include:

- Control and track access – Real time visibility and management of onsite personnel, visitors, and contractors.
- Improve security – Fulfil all the security requirements of your building, premises and insurance whilst protecting against unwanted visitors.
- Safeguarding of people – Restrict access to potentially unsafe areas or equipment.
- Safeguarding of assets – Restrict access to commercially sensitive areas or valuable assets. Reduce instances of theft.
- Removal of physical keys – Reducing costs and security risks associated with misplaced keys.
- Integration with other systems – Such as CCTV and fire.

2. Legislative Compliance

When starting out, there are various legislative requirements that need to be considered alongside the installation of an access control system. These can be summarised as follows:

DATA PROTECTION ACT

All organisations in the UK must comply with the Data Protection Act. This includes members of the public and staff members alike. Signage is generally the simplest way to tell people that they're in a monitored area, this must be clearly visible and readable. Guidance on using access control is provided in the Act and available from the commissioner's office at https://ico.org.uk/for-organisations/guide-to-data-protection/

GDPR

Biometric data, which may be captured as part of an access control system, is of course personal to an individual meaning that it is subject to the General Data Protection Regulation (GDPR) and its governance of the processing of personal information. Under GDPR, biometric data is known as 'special category data' whenever it is processed to identify an individual. As the Information Commissioner's Office (ICO) states, "if you use biometrics to learn something about an individual, authenticate their identity, control their access, make a decision about them, or treat them differently in any way, you need to comply with Article 9".

Article 9 includes the specific conditions for processing special category data; any organisation looking to implement biometric access control must meet at least one of these. We've also summarised some of the most relevant conditions below:

- Biometric processing is essential for reasons of public interest.
- Biometric processing is critical in protecting the vital interests of the data subjects (employees).
- Biometric processing is necessary as part of the provision of health or social care (with a basis in law).
- Biometric processing is necessary for the purposes of carrying out obligations and exercising the specific rights of the data controller (employer), or of the data subjects, in the fields of employment, social security and social protection law.
- The data subjects have given explicit consent to biometric processing.

As this list shows, many of the conditions for processing biometric data relate to the type of work an organisation carries out and whether this provides a justification for processing. Conversely, gaining employee consent negates the need for an organisation to fit certain parameters, making it perhaps the most straightforward way to implement GDPR-compliant biometric technology.

The full list can be viewed at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

HUMAN RIGHTS ACT

If you're planning to use CCTV in conjunction with an access control system, you need to be aware of your responsibilities under the Human Rights Act 1998, and more specifically, Article 8 – A right to privacy. If you're unsure if Article 8 applies to you, you can take an online self-assessment and register your CCTV solution with the ICO at https://www.gov.uk/data-protection-register-notify-ico-personal-data

3. Supplier Selection

There are many suppliers/installers that operate within the access control industry so it can be a complex task to narrow them down to the ones that will provide you with the experience, reliability, and support levels you may require.

Here are some common areas to consider when looking at potential suppliers:

ACCREDITATION / CERTIFICATION

One of the best ways to determine whether you are dealing with a competent access control installer is to check their accreditations. Some of the most common accreditations associated with a competent installer are as follows:

- **NSI**

NSI approval is a highly respected and trusted hallmark in the security and fire sectors, demonstrating technical expertise and a reassuring quality of service. NSI approved companies are all subject to a rigorous bi-annual audit programme, these take place within the company's offices and a completed installation. The vast majority of NSI approved companies choose to hold Gold approval which includes all cases ISO 9001 approval for Quality Management Systems. For companies who declare they hold NSI approval, they must demonstrate their certification alongside any NSI services they promote.

- **SSAIB**

SSAIB is a leading certification body for organisations providing security systems and services, fire detection and alarm systems, telecare systems and services, manned services, approved contractors scheme and monitoring services.

- **CONSTRUCTIONLINE**

Working to enhanced PAS 91 criteria, Constructionline have a validated portfolio of suppliers that can be "deemed to satisfy" for SSIP (Safety Schemes in Procurement). In using the Constructionline platform, buyers can expect to simplify and speed up their search, validation and purchasing decision processes considerably, improving resource and cost efficiency.

- **SAFE CONTRACTOR**

Recognised as the leading health and safety accreditation, a Safe Contractor accredited company not only demonstrates health and legislation compliance, but also provides reassurance that you are working with a safe, stable, and ethical business.

3. Supplier Selection (continued)

CASE STUDIES/TESTIMONIALS

A company that can demonstrate a portfolio of happy clients, testimonials and case studies provides a good indication you are dealing with a reputable access control installer. Companies should also be happy to provide references or a site visit if applicable.

SERVICES

It is worth investigating what services your access control supplier can provide and this can help you understand what support you are likely to expect. A supplier that has been established for many years and has their own in-house installation team provides a good level of confidence that you are likely to receive high service levels. However, it is also important to ensure that your service requirements are aligned with the capabilities of your supplier. Most suppliers can be grouped as follows:

- Supply Only.
- Supply and Install.
- End-to-End – Design, specification, install, support and maintenance.

INSURANCE

Checking the insurance details of any supplier is a must. Most suppliers that carry an accreditation will be covered, but it is always a worthwhile activity to ensure that they have the correct cover in place.

It is important to check for the following:

- Employers' liability to cover their own staff in the event of an accident.
- Public liability to cover damage or injury to clients and their property.

4. The Survey Process

It is important that when considering an access control installation of any kind that you should look for a supplier that will help you undertake a FREE no obligation appraisal of your requirements and objectives.

Requirements can vary from sector to sector, the size and complexity of the building and the type of business trading from the property can all have an impact on the final recommendations or the installation phase of your project.

Following your site survey, you should expect a provider to address the following aspects:

- IT network requirements.
- Risk assessment.
- Insurance requirements.

Any recommendations should consider the scalability and futureproofing of your proposed installation.

5. Types of Access Control System

Once you have specified what your new access control system needs to be capable of, it's time to decide on the technology that will best do the job. There are many forms of access control hardware, software, and peripherals, so it's all about finding a customised combination that works for your business.

As a start point, there are several different types of systems on the market which can be defined as follows:

AUDIO/VIDEO

This is an entry level system that is both simple in design and to install. These systems are more commonly used for small scale installations whereby there is only a need for one or two doors to be controlled.

These systems comprise of an outside panel with either a simple press button/audio device or camera device. The device will contact the operator who will then authorise access to the premises by releasing the door lock.

Keypad/reader entry systems can also be integrated as an alternative option to audio/video system. This type of access control would require the visitor to present their credentials, whether it is a code or proximity card/tag which when approved, would in turn facilitate authorised access to the premises.

STANDALONE SYSTEM

This type of system is useful for premises whereby access control is only required to secure a few doors within the building. All the equipment is positioned near to the door on the secure side. This type of standalone system will have either a keypad or proximity reader adjacent to the door it controls. Access can be granted by entering a code or presenting a proximity card or tag to the reader.

5. Types of Access Control System (continued)

NETWORKED SYSTEM

These types of systems are an effective means of managing the secure movement of people within all types of premises. Usually recommended for installations of 3 or more doors, they provide a scalable and operationally efficient means of controlling access for companies of all sizes.

A networked system will consist of a controller above each door and a central interface to the ethernet LAN. These types of systems capture, monitor and control employees, visitors or contractors access rights and therefore is an integral part of managing both site security and health and safety. These systems can control different doors at different times and limit certain people to certain areas.

A combination of keypad, proximity or biometric options can be integrated to provide a best fit solution, not only that, but networked systems can also be easily integrated with other systems such as CCTV or Fire. Combined with CCTV, specific details of those who have entered and exited the site can be displayed in real time to identify any potential security threats or health and safety issues.

Furthermore, there are many other health and safety related reasons why a business may benefit from an integrated system. The most critical being in the instance of an emergency. In this scenario, when a fire alarm is triggered, the access control software can automatically move to an open profile, so that all persons on site can move quickly to a safe place or muster point within the site perimeter.

Networked systems can be accessed from any connected PC, smart phone, or tablet device, this can be particularly useful for multi-site systems whereby the system can be controlled and administered efficiently from one central location. Whether you are looking to designate complex staff access rights that match working patterns, or simply provide temporary access to visitors requiring the use of the car park, all this can be achieved with minimum time, cost, and effort.

6. Access Control Software

Access control software operates at the heart of any networked system installation, capturing, monitoring, and controlling access rights.

When looking at access control software, you should expect to see the following system features which may be specified as part of your solution:

- Badge production.
- Badge design and print.
- Visitor management.
- User management.
- Facilities management.
- Personnel management.
- Image capture and authentication.
- Real time monitoring.

From controlling one door to managing multi-site operations, access control software can integrate with a wide range of access control devices including door systems, car park barriers, gates and turnstiles.

Via the use of interfacing tools, it also has the capability to link with almost any other system, from HR and Payroll, Fire and Intruder through to cashless vending. This works by automating the transfer of access control related data to streamline operational processes, reducing associated costs and errors.

7. Access Control Devices

Networked systems often require the integration of additional hardware products. Once you have engaged with an installer, it is good to be aware of what options are available. What is most important is that each device is correctly specified against the business requirements to reduce the risk of a system failure or potential security breach. The survey process will make recommendations for a best fit solution.

An overview of the various access control device types can be summarised as follows:

LOCK TYPES

- **ELECTRIC STRIKE LOCK**

The electric strike lock is basically a metal plate that is installed on the door frame to catch a latch which will in turn lock the door. An electric strike always remains locked from the outside and is very similar to a normal latch type, the exception being that it is connected to a power supply. Once activated, the latch is released therefore unlocking the door for safe entry/exit, the door will automatically return to a locked position once closed.

These units can be set up as:

- Power safe: Open in the event of a power failure.
- Power secure: Lock in the event of a power failure.

Because the unit is a mechanical design it can wear out frequently when used on a door with a lot of traffic.

7. Access Control Devices (continued)

- **MAGLOCK**

The electromagnetic lock or “Maglock” for short consists of a metal plate fitted to the door and an electromagnetic armature. The magnetic lock is by far the most common lock type in use for access control due its strength and low cost. Most used within premises with a high throughput, they offer a more reliable option to the electric strike due to there being less moving mechanical parts.

Like the electric strike, these locks can also be set up on a power safe or power secure, however unlike the electric strike, the maglock is constantly drawing power to remain secure. When specifying this type of lock, your installer should be recommending a good back up battery to ensure security is maintained in the event of a power failure.

- **EXTERNAL DOOR LOCKS**

Whilst an access control system is an effective means of controlling safe and permitted entry to a building or premises, these should still be complemented by the use of traditional external door locks. A traditional lock provides a sensible back up that helps close any potential gaps in security should there be a system failure or an electrical power cut. The best locks on the market allow for a mechanical override in cases of system issues and to comply with British and European standards. A mechanical exit should be specified for a certain class of door use, (BSEN179 and BSEN1125 are the most common).

READER TYPES

- **PROXIMITY READERS**

Proximity readers are a popular entry level option for physical access control. These reader types are fitted adjacent to the controlled door. Presentation of credentials by card or tag are the most common methods of authorisation. When presented at a reader, the card or tag releases the door for a pre-determined time before locking again.

These readers are suitable for internal and external environments with the availability of heavy-duty vandal and water-resistant outdoor units.

Whilst these readers are an effective means of authorising access, they are not faultless. Buddying or unauthorised use of stolen cards/tags can mean that access could be allowed to those who are not permitted to enter the premises. In these scenarios, your access control installer would be able to recommend additional security enhancements based upon your system objectives and requirements.

- **BIOMETRIC READERS**

Our physical attributes are the most impervious form of identity verification there is. Virtually impossible to replicate and completely unique, physical features such as eyes, faces and fingerprints make ideal ID credentials. Biometric access control readers are built around this exact principle. These readers scan and read an eye, a face, or a fingerprint in seconds, to admit access for those registered in the solution’s database. Due to the uniqueness of these credential’s, biometrics is one of the most secure types of credentials available.

Biometric data, which may be captured as part of an access control system is of course, personal to an individual, which means it is subject to the General Data Protection Regulation (see GDPR) and its governance of the processing of personal information.

7. Access Control Devices (continued)

GATES, BARRIERS AND TURNSTILE CONTROL

Gate and barrier systems provide effective & safe means for vehicle and pedestrian flow control at entrances ranging from manufacturing facilities, commercial buildings, schools & educational campuses through to leisure stadiums, amusement parks and retail shopping outlets etc. Gates and barriers can often be integrated into access control systems and offer a cost-effective alternative to on-site manned gatehouses.

KEYPADS, INTERCOMS AND EXIT BUTTONS

- **KEYPAD**

For use on both standalone and networked systems, keypads can be situated adjacent to secure doors. For standalone systems, a standard pin is issued to all users whereas networked systems allow for the generation of a number of codes that can be allocated to a number of users.

- **DOOR ENTRY PANEL (AUDIO/VIDEO)**

Door entry panels are situated at the entrance to a building where visitors need to gain access. They provide instant audio and/or video communication with a member of staff alongside access control. These panels can integrate anything from a simple press button, through to a keypad or proximity reader as a part of a standalone or networked system.

A door entry handset is used in conjunction with an external door entry panel. The handset is used to have an audio or video conversation with the visitor outside and can release the door if required.

- **EXIT BUTTONS – PUSH TO EXIT (PTE) / RELEASE TO EXIT (RTE) / CONTACTLESS**

Exit buttons can be used on any power safe or power secure door system, they are usually positioned on the secure side of a controlled door. When an PTE button is pushed, it provides a momentary break in the circuit to allow an electric strike or maglock to de-energise and allow for the door to open. These types of exit buttons are more commonly used in basic access control systems where there is no requirement to log people out of the building.

- **EMERGENCY BREAK GLASS UNIT**

The emergency break glass unit allows for emergency exit through secured doors. Surface mounted and easily visible, they are fitted to the secure side of the door. In the case of an emergency, by breaking the glass, power is automatically disconnected, enabling the door to be released and allowing for the free movement of personnel to a place of safety. It is worth noting that modern equivalents of these units no longer use glass but a resettable plastic plaque which is more eco-friendly, however, despite this, the common name of “Break Glass”, remains.

- **EXIT PIR**

A request to exit PIR motion detector is most often used in applications such as retail or an office. Used in scenarios whereby there is no need to log people exiting the secure area or premises, they detect people approaching and will release the door without any other intervention. Doors for this type of exit are typically automated for user ease.

7. Access Control Devices (continued)

INTERFACES

- **INTEGRATION PLATFORMS**

For companies that are looking for a more integrated solution, middleware platforms offer a means of integrating any third-party application into your access control system when a direct link is not possible. This could include anything from HR and Payroll through to CCTV or Fire systems.

Enabling the automatic transfer of data from a separate system into access control, is an efficient and accurate method of populating multiple systems by removing the manual re-keying of data.

- **FIRE ALARM INTERFACE**

It is important to remember than any building that operates a fire alarm system should be integrated with the access control system so that in the event of a fire alarm activation all doors are released enabling free movement to a place of safety.

Commercially sensitive areas or high security risk areas can be exempt from these restrictions, your access control installer will be able to make the appropriate recommendations for these scenarios when specifying your installation.

8. Cost

When looking at quotes comparatively, it is very common for costs to vary. Whilst reviewing an access control quote, it is often good to review them with the following cost checks in mind:

- **Types of devices** – The costs will vary dependent upon quality and features such as the lock types, reader types and so on.
- **Service charges** – Some providers may or may not include costs such as maintenance and repairs. As a minimum, ensure that servicing costs are included – any access control system is a business asset and should be maintained as such.
- **Licence costs** – For either the software or number of doors on the system.

9. System Installation and Training

Once you have approved a quote you should expect a project delivery manager to be assigned to your installation. The purpose of the project delivery manager will be to verify the initial recommendations, undertake the appropriate level of testing to support the process, carry out the relevant risk assessments, issue a method statement and plan the installation.

A good project delivery manager will work hand in hand with the relevant contacts on your site to develop the infrastructure for an effective deployment. Identifying the work areas and schedules, a successful installation will ensure there is little or no disruption to your day-to-day operations.

10. Commissioning and Handover

Once it's in place, it's time to test the system. Your installer should run through a thorough set of tests to ensure the solution is as required/quoted to confirm an "as fitted" specification.

Your installer should provide advice on testing and provide a logbook for the system. If you are working with an NSI Gold accredited company, they should provide detailed documentation including the installation and commissioning certificates alongside an NSI "Certificate of Conformity". An approved NSI quote for instance, should clearly outline the expected system to then be compared to the actual installation. The quote and installation should match which protect both the customer and the installer.

TRAINING

Once your new access control system is in place, the best way to ensure a smooth transition to full adoption is to provide employee training. Your installer should be able to provide short onsite sessions, run in small groups, covering everything from basic daily operation to specific access control scenarios they are likely to face. A train the trainer approach works best as you then have onsite ownership that champions the solution.

By getting hands-on under the guidance of a system professional, your employees can quickly gain the knowledge and confidence they need to use your new access control solution to its full potential. Once new working practices are rolled out, it's also a good idea to add access, security and any other updated processes to staff handbooks and policy documents.

11. Service Support and Maintenance

When looking for a supplier, it is worth looking for a well-established supplier that has a good network of local engineers to provide the best and most reliable support for your installation.

Access control systems are an asset and do require regular maintenance. This could be an annual service or more frequent preventative maintenance visits depending on the size and complexity of the system. It is important to be aware of what support your supplier can offer and whether these align with your needs, e.g. are their response times and whether they offer out of hours etc.

12. Conclusion

We hope you have found this guide useful. If you need any further information or guidance, talk to our team of experts who will be able to advise you on any element of an access control installation.

Get in touch:

Phone: +44 (0) 845 3379 155
Email: info@touchstar.co.uk
Web: touchstar-atc.com

TouchStar ATC Limited 7 Commerce Way, Trafford Park, Manchester, M17 1HW