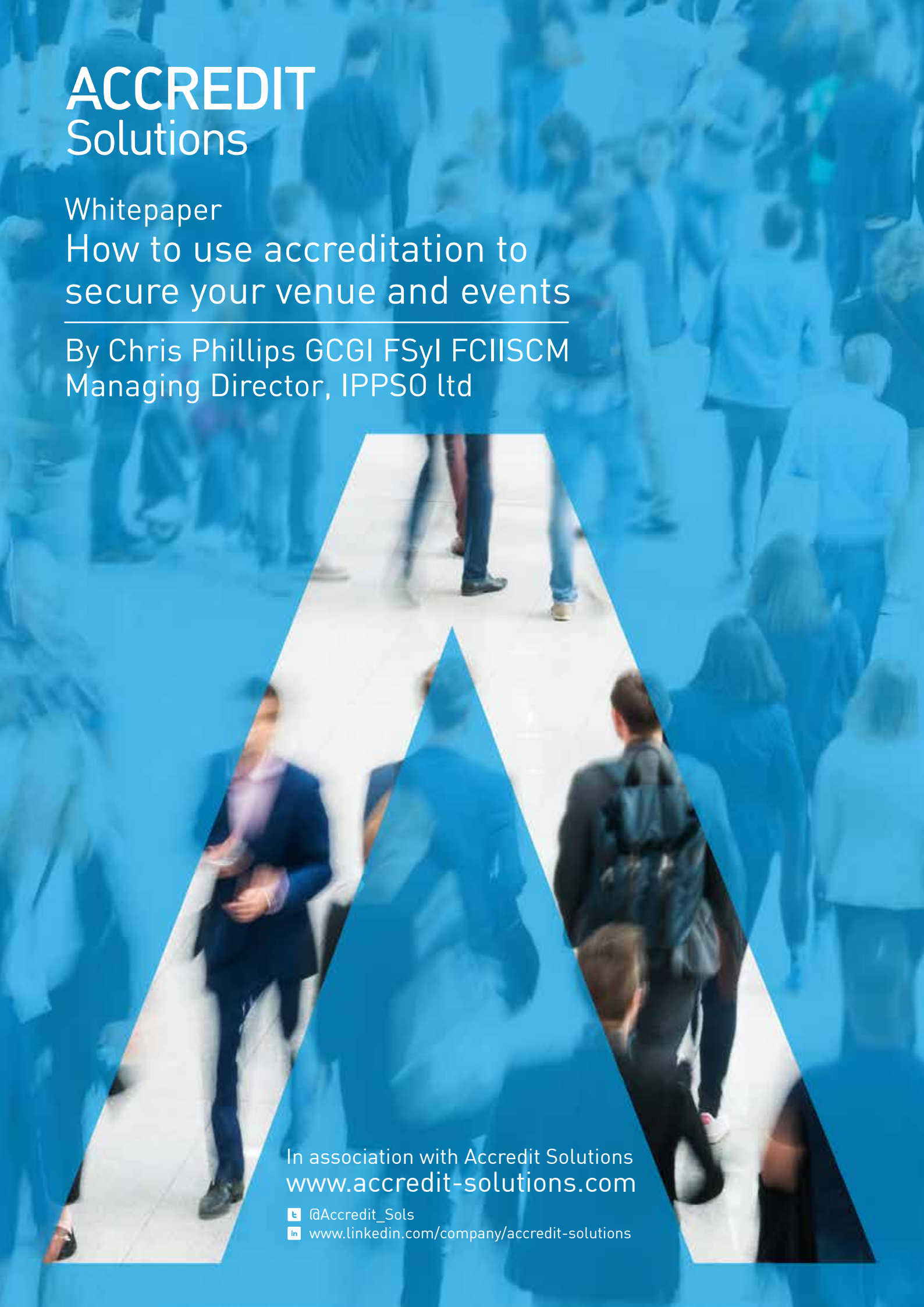
ACCREDIT
Solutions

Whitepaper

How to use accreditation to secure your venue and events

By Chris Phillips GCGI FSyI FCIISCM
Managing Director, IPPSO ltd



In association with Accredit Solutions
www.accredit-solutions.com

@Accredit_Sols
www.linkedin.com/company/accredit-solutions

About Chris Phillips

Chris is the Founder and Managing Director of the International Protect and Prepare Security Office, a company he started after thirty years as a Police officer with particular expertise in Counter Terrorism (CT) strategy, protective security, CT training, risk assessment and quality assurance.

With an enviable reputation for delivery at both an operational and strategic level, he has widespread respect internationally within law enforcement and Government business.

As Head of the National Counter Terrorism Security Office, he was responsible for the protection of Crowded Places within the UK and to reduce the vulnerability of British nationals overseas from the terrorist threat to crowded places and soft targets. The role involved providing Counter Terrorist advice to all businesses involved in crowded places including Hotels, Stadiums, Shopping centres, Visitor attractions and licensed premises.

A keynote speaker at major conferences across the world, and a commentator on Policing, Security and Counter Terrorism matters on all the main media outlets in the UK, he is widely acknowledged as an expert in Counter Terrorism on national and world media.

Chris is a Graduate of the City and Guilds, a fellow of the Security Institute and the Chartered International Institute of Security and Crisis Management.

About Accredit Solutions

Since 2002, Accredit Solutions has helped venue security and event management teams to improve operational efficiencies and process accreditation for over six million workers and visitors at some of the best known political, sporting and live events in the world including world cups, premier league football and national rugby matches, cricket tests, and major ceremonies, festivals, and awards.

Built with 15 years of experience, the Accredit platform is the world's most sophisticated, secure and intuitive accreditation platform on the market today.

Find out more at www.accredit-solutions.com

Contents

Introduction

I have had the benefit of being one of the first group of Counter Terrorism Security Co-ordinators deployed across the UK after 9/11. This role saw me reviewing and implementing security specifically from a Counter Terrorism perspective at a variety of events and stadiums. It became apparent that there were gaps and I consistently found a major issue with people security. Even today - many years later - these gaps are still apparent across events, stadiums, and arenas that host large Crowded Place events.

Using the adage, "it's good to learn from other peoples' mistakes" I can tell you my findings over the years have been that accreditation is generally not being done well. Staff are being employed without adequate background checks and the dangers of employing a terrorist or a criminal is a major risk that needs to be addressed as a matter of some urgency.

This guide aims to help explain the terrorism and security personnel risk issues for those who have responsibility for business involved with organising events. It is especially relevant for those who are responsible for managing locations where events take place, irrespective of size and capacity, and is not specific to any particular type of event. It is aimed at those events where there may be a risk of a terrorist attack either because of the nature of the event or the number or nature of the people who host or attend it.

Terrorist attacks are a real and serious danger worldwide and there is no sign of this risk reducing any time soon. Many experts believe this is a generational issue and we will face terrorist attacks for many years to come. Terrorism can come in many forms, not just a physical attack on life and limb. It can include interference with vital information or communication systems, causing disruption and economic damage. It is a fact that attacks are easier to carry out if the terrorist is assisted by an 'insider' or by someone with specialist knowledge or access. And this is the issue we will deal with in this guide.

Chris Phillips GCGI FSyI FCIISCM
Managing Director, Ippso ltd

What can you do to ensure that you are not employing a terrorist or a criminal who may want to target your event or business?

There is an expectation from the general public that security measures will be in place. The obvious measures of access control, C.C.T.V., searches and other security measures are accepted as the norm. However all these measures are easily overcome by someone working on-site who wants to cause harm or commit crime.
People security is the most easily overlooked aspect of protecting an event. And yet employing someone who is a threat to you is one of the most dangerous risks your organisation can face.

The size and structure of your stadium, event, or business, and the level and nature of the post is likely to determine which areas of your business will have a stake in ensuring that pre-employment screening and accreditation is effective. The most active participants in the process are likely to include:

Business owners and managers – The involvement and support of business owners and managers are crucial to implementing robust pre-employment screening and accreditation. They will usually play a greater role in recruitment in smaller organisations.

Security personnel – In many organisations, the security department is responsible for pre-employment screening and accreditation. Even where this is not the case, the security department will be responsible for dealing with security concerns that emerge, as well as decisions about the levels of checks that may be required for different posts or locations.

Human Resources (HR) – In many organisations, HR departments will take the lead on the selection and recruitment of employees. They will normally be responsible for conducting or commissioning verification checks. It is vital, therefore, that HR personnel have a sound understanding of pre-employment screening.

The Legal team – The business Legal team will play a critical role in the development of pre- employment and accreditation processes. They must be involved in the production of all documents, forms and processes used for screening purposes.

Other parties – In the stadium and events business there are often governing bodies, regulatory bodies, staff unions, procurement and auditors who should be involved in setting accreditation levels.

5

This guide also provides counter terrorism security advice to those who own, operate, manage or work in the events business. These businesses are designed to welcome customers into their business. Businesses in this sector may be licensed and will have many obligations under the assorted acts to prevent crime and disorder and improve public safety. Understanding your risks, vulnerabilities and carrying out audits to ensure that your security is fit for purpose will demonstrate that your business is committed to providing a safe and secure environment. **Therefore we have included a self Audit form at the end of the document which will allow you to review your current situation and indicate areas where you could improve. It also provides advice on managing a crisis.**

If a Terrorist attack or other crisis happens, it will happen quickly and without notice. It is imperative that you have your plans in place before any incident. This guide will help you understand the issues and point you in the direction of identifying and reducing your vulnerabilities.

Overview

1. Understand the threats. Whilst having a broad awareness of terror and other criminal threats is necessary - it is important to not only consider the threats to you, but also other premises or businesses nearby. Are you located near a landmark or iconic site which may be a target? Are your regular customers vulnerable because of their work or lifestyle choices? Are you an iconic site?
2. Carry out adequate risk assessments on the roles in your organisation. Some roles are higher risk than others. Consider each role and the potential implications of that employee going bad.
3. Set the security employment standards for each role.
4. Use pre-employment screening for all staff. Ensure that the Human Resources department understands its role in ensuring that the organisation doesn't recruit staff who are likely to cause a security concern. Reduce the likelihood of employees using their access to become a security risk
5. Training and Awareness. Ensure that all your staff are aware of the threats and risks and get some training in security awareness and Security Culture.
6. Use good practice for badging of staff. Ensure that badges are used. Include a photo, add access permissions, use counterfeiting measures and add a unique id and change designs regularly.

Understanding the threats

Make yourself aware of what is happening around the world. Think through what the terrorist intends to achieve and their capabilities - what they might do and how they might do it is crucial to assessing threat.
Consider the following. Ask yourself:

- What can be learnt from the government and media about the current security climate, or about recent terrorist activities?
- Is the location of your business, your neighbours, your customers, staff or your activities a factor that might raise the likelihood of a terrorist or criminal attack?
- Could you suffer from an attack nearby ?
- Do you keep in contact with your local Police to stay updated on local crime issues?
- Is there any aspect of your business, events, or activities that might interest terrorists?
- The very fact that you are creating a crowded place brings a legal and moral duty to consider the risk of terrorism to your event.

Risk assess roles and set the security standards

It is vital that the Head of Security - or someone in a similar position - reviews each role on not only event day but on the build and pre-event, and allocates a risk based security level for each role.
This should be documented and can be as simple as basic, medium or high risk. Each level should then have a set of security checks allocated, and all staff in each level should be checked to the allotted level. At a basic level, the staff serving tea and cakes in the VIP area might need a higher level of accreditation than those doing the same task in the non VIP areas. Those staff are not necessarily interchangeable.

- Clearly set out the different job descriptions and focus on the employees. Their job roles, their access to their organisation's critical assets, risks that the job role poses to the organisation.
- Once the risk is understood of any particular role, make decisions on the level of pre-employment screening for each role.

Pre-employment screening

Personnel security starts with the job application, where applicants should be made aware that supplying false information, or failing to disclose relevant information, could be grounds for dismissal and could amount to a criminal offence. Applicants should also be made aware that any offers of employment are subject to the satisfactory completion of pre-employment checks. If an organisation believes there is a fraudulent application involving illegal activity, the police should be informed.

Pre-employment checks may be preformed directly by an organisation, or this process may be sub-contracted to a third party. In either case the company needs to have a clear understanding of the thresholds for denying someone employment. For instance, under what circumstances would an application be rejected on the basis of their criminal record, and why?

Pre-employment screening policy - Your pre-employment screening processes will be more effective if they are an integral part of your policies, practices and procedures for the recruiting, hiring, and where necessary training of employees. If you have conducted a personnel security risk assessment then this will help you to decide on the levels of screening that are appropriate for different posts.

Identity - Of all the pre-employment checks, identity verification is the most fundamental.
Two approaches can be used:

- A paper-based approach involving the verification of key identification documents and the matching of these documents to the individual.
- An electronic approach involving searches on databases (e.g. databases of credit agreements or the electoral role) to establish the electronic footprint of the individual. The individual is then asked to answer questions about the footprint which only the actual owner of the identity could answer correctly.

Right to work - In the UK the Immigration, Asylum and Nationality Act 2006 means there are requirements of employers to prevent illegal working in the UK. These include an ongoing responsibility to carry out checks on employees with time-limited immigration status. Failure to comply with the new regulations could result in a possible civil penalty or criminal conviction. Each country will have its own laws but almost all countries have a limited right to work for foreign nationals. The penalties are often extremely harsh for employers who fail to comply. **Don't forget that the right to work usually has an end date and peoples' rights to work will change. This should be checked regularly.**

Qualifications and employment history - The verification of qualifications and employment can help identify those applicants attempting to hide negative information such as a prison sentence or dismissal. Unexplained gaps should be explored.

Qualifications - When confirming details about an individual's qualifications it is always important to:

- Consider whether the post requires a qualifications check.
- Always request original certificates and take copies.
- Compare details on certificates etc. with those provided by the applicant.
- Independently confirm the existence of the establishment and contact them to confirm the details provided by the individual.

Employment checks - For legal reasons it is increasingly difficult to obtain character references, but past employers should be asked to confirm dates of employment. Where employment checks are carried out it is important to:

- Check a minimum of three but ideally five years previous employment.
- Independently confirm the employer's existence and contact details (including the line manager).
- Confirm details (dates, position, salary) with HR.
- Where possible, request an employer's reference from the line manager.

Criminal convictions - A criminal conviction - spent or unspent - is not necessarily a bar to employment (see the Rehabilitation of Offenders Act). However, there are certain posts where some forms of criminal history will be unacceptable. To obtain criminal record information, a company can request that an applicant either:

1. Completes a criminal record self-declaration form, or
2. Applies for a Basic Disclosure certificate from Disclosure Scotland.

Financial checks - For some posts it may be justifiable to carry out financial checks, for example where the employee's position requires the handling of money. Interpreting the security implications of financial history is not straightforward and will require each organisation to decide where their thresholds lie (e.g. in terms of an acceptable level of debt).

There are a number of ways in which financial checks can be carried out. General application forms can include an element of self-declaration (for example in relation to County Court Judgments (CCJs)), or the services of third party providers can be engaged to perform credit checks.

9

Contractor recruitment - Organisations employ a wide variety of contract staff, such as IT staff, cleaners, and management consultants. It is important to ensure that contractors have the same level of pre-employment screening as those permanent employees with equivalent levels of access to the company's assets, be they premises, systems, information or staff.

Contracts should outline the type of checks required for each post and requirements should be cascaded to any sub-contractors. Where a contractor or screening agency is performing the checks they should be audited.

Secure contracting - Contractors present particular personnel security challenges. For instance, the timescales for employing contractors are often relatively short, and there is greater potential for security arrangements to be confused or overlooked (e.g. due to further sub-contracting).

In managing the insider risks associated with contractors it is important to:

- Ensure that pre-employment checks are carried out to the same standard as for permanent employees. Where this is not possible, due to tight deadlines or a lack of information available for background checking, then the resulting risks must be managed effectively. Preferably the implementation of any additional security measures will be guided by a personnel security risk assessment.
- Where pre-employment checks - or any other personnel security measures - are carried out by the contracting agency rather than the employing organisation, a detailed account of the checks to be undertaken and the standards achieved must be incorporated into the contract that is drawn up between the two. Furthermore, the pre¬ employment checking process conducted by the contractor should be audited regularly. Confirm that the individual sent by the contracting agency is the person who arrives for work (e.g. using document verification or an electronic identity checking service).

Once the contractor has started work in the organisation, they will need to be managed securely. The following steps will help:

- Carry out a risk assessment to establish the threats and level of risk associated with the contractor acting maliciously in post.
- Ensure that the contract that exists, either between the organisation and the contractor, or between the organisation and the contracting agency, defines the codes of practice and standards that apply.

- Provide photo passes to contract and agency staff, and stipulate that they must be worn at all times. Ideally, the employing organisation should retain contractors' passes between visits, reissuing them each time only after the contractor's identity has been verified. The employing organisation and the contracting agency (or the contractor, if no agency is involved) should agree a procedure for providing temporary replacements when the contractor is unavailable. These arrangements should be included in the contract between the two parties, and the employing organisation will need to decide what additional personnel security measures to implement - for example, restricted or supervised access - when the replacement is on site.
- Where a contractor is in post but the necessary pre-employment checks have not been carried out - or where the results of the checks are not entirely positive but the need for the contractor's expertise is such that they are employed anyway - then additional personnel security measures must be considered (e.g. continuous supervision).

For additional advice on 'Secure Contracting' please refer to 'A Good Practice Guide on Pre-Employment Screening' See www.cpni.gov.uk

Overseas checks

As the level of outsourcing rises and increasing numbers of foreign nationals are employed, it is increasingly necessary to screen applicants who have lived and worked overseas. As far as possible, organisations should seek to collect the same information on overseas candidates as they would for longstanding UK residents (e.g. proof of residence, employment references, criminal record). It is important to bear in mind that other countries will have different legal and regulatory requirements covering the collection of information needed to manage personnel security and therefore this step may be difficult.

A number of options are available to organisations wishing to perform overseas checks:

1. Request documentation from the candidate.
2. Hire professional/ an external screening service.
3. Conduct your own overseas checks.

In some circumstances you may be unable to complete overseas checks satisfactorily (e.g. due to a lack of information from another country). In this case, you may decide to deny employment, or to implement other risk management controls (e.g. additional supervision) to compensate for the lack of assurance.

11

Security Culture

By far the cheapest way to improve security is to engage all staff in the security of the business. The vigilance of all staff is essential to your protective measures. They will know their own work areas very well and should be encouraged to be alert to unusual behaviour or items out of place. They must know the value of good security and understand the key part they play in keeping the staff, customers and buildings safe.

They must have the confidence to report any suspicions, knowing that reports - including false alarms - will be taken seriously and regarded as a contribution to the safe running of the institution.

It is vital to encourage a challenge culture where staff challenge anyone acting suspiciously our at the very least bring them to the attention of a senior member of staff or security.

Training is therefore particularly important. Staff should be briefed to look out for packages, bags or other items in odd places, carefully placed (rather than dropped) items in rubbish bins and unusual interest shown by strangers in less accessible places. Training in emergency response plans should also be included in staff inductions.

Security culture is about more than facilities and procedures, it is also about creating an open, trusted environment that is focused and proactive about reducing risk for everyone's benefit.

Supportive Management to demonstrate the value placed on security. If the boss is seen not wearing a pass it sends a message to others that management do not take the policy seriously.

Line managers are in best position to influence attitudes amongst colleagues and address any behaviours of concern amongst their staff. Through their regular contact it should be a part of their duties to ensure their teams are acting appropriately. It might even be added as part of each line-manager's job description.

Using Appraisals to reinforce individual security behaviours.

Employee welfare plays a key role in security culture. It's positive for staff to be able to discuss problems in confidence and find out about where and when support can be provided (e.g. cases of illegal drug use or personal debt). Discussing areas of disputed or concern can prevent staff feeling resentful towards the business.

Security hotline. In larger establishments a hotline or email account could be offered for staff to report, anonymously or otherwise, any suspicions or actual incidents of illegal, unethical or improper conduct by their colleagues, such as bullying, failure to adhere to security procedures, fraud or theft.

Responsible handling of documents. Sensitive, confidential or commercial documents should be appropriately marked with clear instructions about handling when outside of the workplace. Staff should be fully aware of their responsibilities when in possession of these documents.

Some of the material that organisations routinely throw away can be confidential.

Valuable paper documents may require shredding, incinerating or pulping. In addition, a central point for returning old IT equipment (obsolete laptops, old media disks, flash drives and so on) should be provided so that all data can be safely removed.

The importance of security within the business should be emphasised through regular communications with staff. This might be in the form of posters, leaflets and intranet, but should also include face-to-face activities such as training programmes, management forums or programme of talks and workshops.

Good housekeeping can help reduce opportunities for suspect items to be left on the premises and make it easier for them to be noticed by staff (and help reduce the number of false alarms). Staff should be asked to:

- Keep external, public and communal areas – (exits, entrances, reception areas, stairs and corridors, washrooms etc) – clear and tidy.
- Lock unoccupied offices, rooms and store cupboards.
- Minimise furniture and plants in the entrances and public areas to reduce places in which to hide devices.
- Consider removing litter bins during periods of heightened threat – use clear plastic bags as a temporary alternative.

Locking down your building (Invacuation)

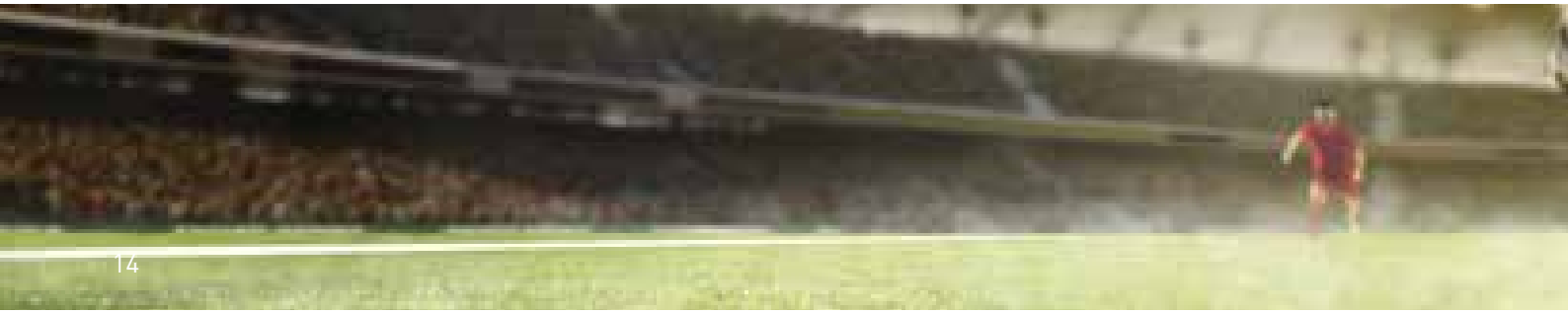
- Identify all access and egress points in both public and private areas of the site
- Practice to understand how quickly you can physically secure access/egress points
- If your building is of a substantial size, divide it into sectors it to allow specific areas to be locked down
- Ensure that staff understand their roles and responsibilities

- Stopping people leaving or entering the site is a difficult task. It needs a firm presence to direct people away from danger
- Consider building in the ability to disable lifts without returning them to the ground floor
- Plans may need to change as the incident develops, they need to be flexible enough to change to full and partial evacuation
- Consider getting specialist advice on the best location to keep people in an emergency outside your premises. The basics are that if possible it should be away from windows and in the centre of the building if possible.

Badging

We are now in an age where it is easy to forge badly designed badges. Anyone with a basic grasp of photoshop can re-produce basic badges. These simple techniques can reduce your vulnerability to this threat;

1. Include a photo
   The easiest way for your security team to check whether a person is who they say they are, is to include a photo on the badge. If the photo and the person don't match then they shouldn't be allowed to enter.
2. Add access permissions
   Consider specific colours or icons to show what a pass entitles the holder to do and where they are allowed to go. make sure access permissions are clear on the badge and that your security team know what it all means.
3. Use a unique ID
   If you hide a unique ID number for every person in a bar code, QR code or RFID chip, a quick scan at your access control points will instantly be able to tell you if that pass is valid.
4. Use anti-counterfeit measures
   Holograms, black light ink, or micro printing make it very difficult for anyone to forge a badge or ticket.
5. Change designs
   Large venues or recurring events are sure to have a high churn of temporary workers. Don't issue 'season' badges for agency staff – changing the colour of your badge for each event will make it easy for your security team to see if anyone is re-using old passes. Even better, issue a new unique ID for staff at every event and a quick scan of the badge will tell you if their pass is valid.



Top tips

- Use large format badges to make the visual ID of photos or access zones easy for your security team. No one wants to be squinting at credit card sized passes all day.
- Ensure that there is something on the back of the pass. When people share photos of their badges or tickets online, they almost always display the front. No one knows what is on the back.
- Your staff need to know they are prohibited from sharing images of their badges online.
- Print and distribute badges as close to the event as possible to reduce the opportunity of copies.
- Keep designs confidential and allocate unique IDs as late as possible.

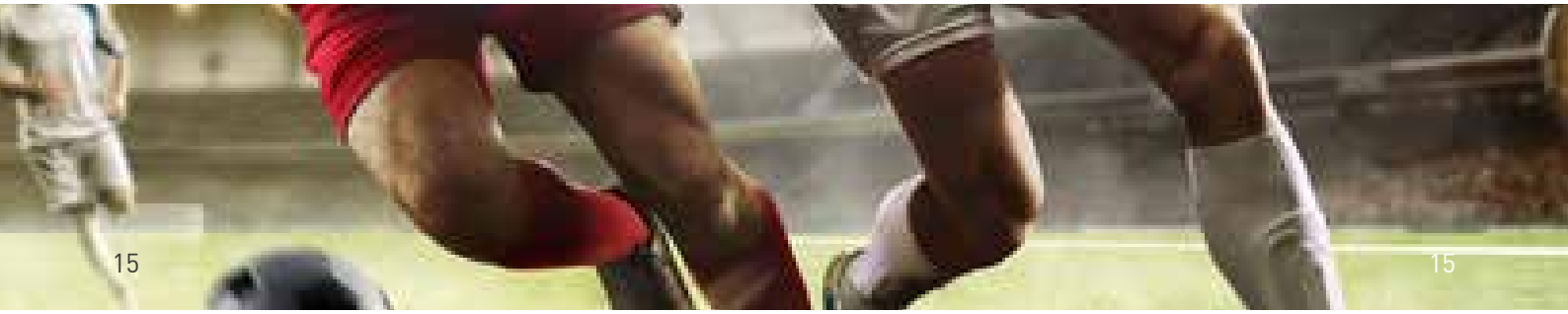
Crisis planning

It is important to develop a clear idea of protocol responses to certain situations. Doing so can save valuable time when it comes to decision-making. Talking through a variety of Terrorist scenarios and how you want staff or students to react is a good way to plan. This is not an exhaustive list and you may think of appropriate scenarios for your own educational establishment.

Types of scenario you could use;

- Terror attack nearby or within your city or town
- Suspicious package is found on site
- A direct attack on one of your buildings by terrorists with guns. (Active shooter)
- A telephone bomb threat is made to your establishment
- A suspicious vehicle is parked adjacent to the establishment
- A suspect package is delivered to the reception
- All Computer systems fail
- Losing key staff in a terrorist attack
- Losing access to the building or local transport links after an attack incident

Responses: Use the scenario prompts to list out the key actions that need to be taken in each case. These initial thoughts can be used to develop protocols and a more extensive security plan.



15

Communications in a crisis

Most events these days use a radio system of some kind. P.A. systems also form part of the security plan. Ensuring staff understand what messages mean and what to do in any given incident is vital. In any form of emergency or crisis, being able to communicate to your staff and customers is vital. Other groups that you may need to communicate with include; the emergency services, local authorities and possibly neighbouring businesses etc.

After working out how you want your staff and customers to react it is vital to be able to pass that message on. You need a communication strategy incorporating both the physical and electronic activities and supporting the delivery of safe passage, messaging and signage. The placing, interpretation and integration of signage is essential for enabling invacuation (lockdown), partial evacuation and evacuation within or outside a building or buildings.

Consider how you will communicate. You may wish to consider a variety of message systems, an App or alarm systems.

It should be remembered that immediately following a terrorist attack, mobile telephone communication may be unavailable due to excessive demand, so consideration should be given to systems that can deal with high demand.

Your message could be as simple as 'don't come to work as there is an on-going incident'. And getting that message out could save lives.

Accreditation and Crisis Management Audit

Please use this self audit checklist to help you to review your current situation and highlight areas where you could improve.

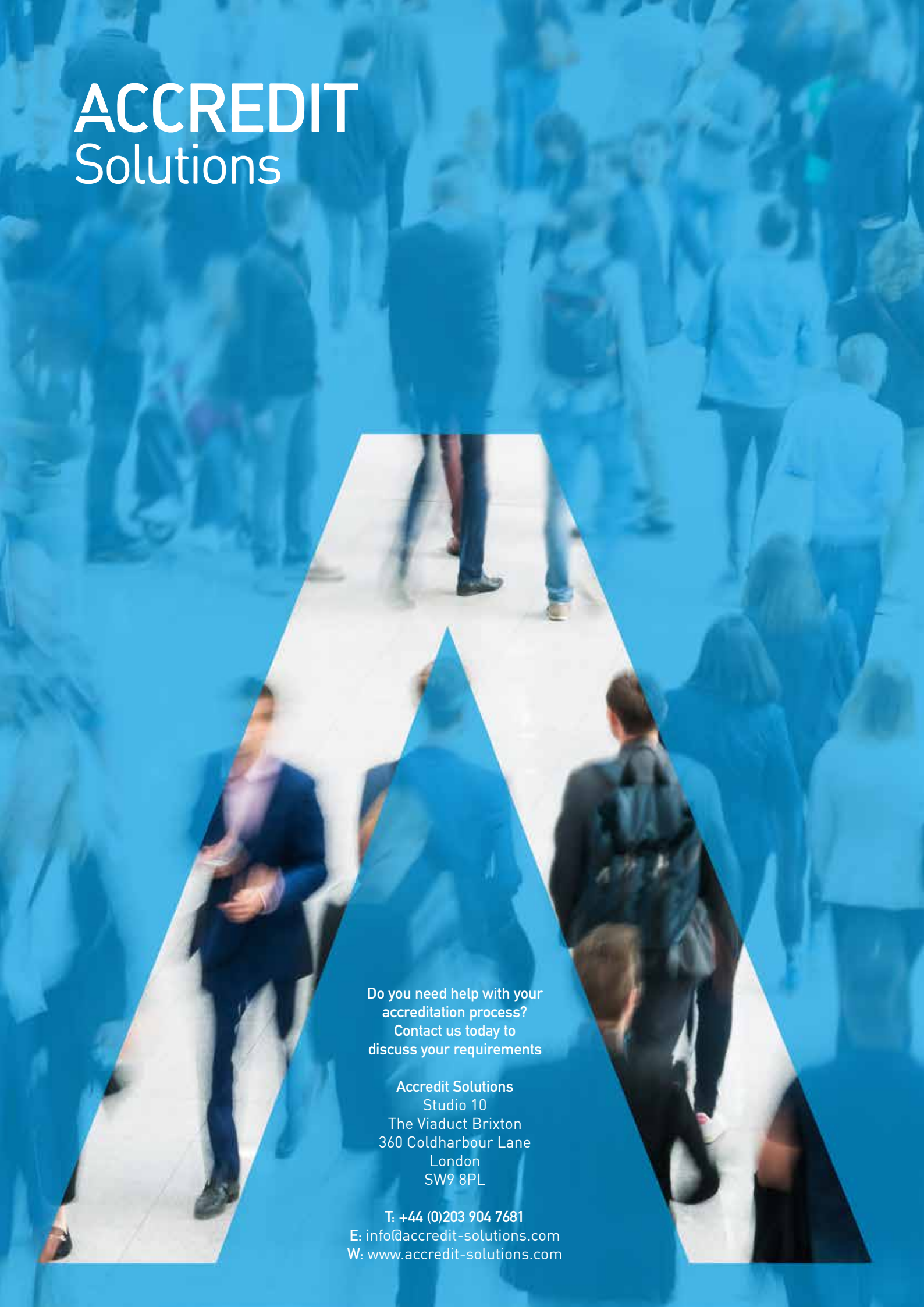
Personnel Security - identity assurance	**Yes**	**No**	**Unsure**
Have you risk assessed all staff roles across the business?			
Have you allocated a risk level for all roles and set standards of security background checking for each role? Do you do proof of identity, right to work and require check references?			
When staff leave do you have procedures for returning company property such as uniform/passes/computers/phones?			
Personnel Security - identity assurance	**Yes**	**No**	**Unsure**
Do you ensure they ate taken off computer systems and have intranet access closed etc?			
Do you regularly check that this is being complied with?			
Training and Security Awareness	**Yes**	**No**	**Unsure**
Is Security/Terrorism Awareness part of the ongoing training regime for all staff?			
Do have a culture of security in your business? Is there a challenge culture?			

17

Communication	Yes	No	Unsure
Are security issues discussed/decided at senior management level and form a part of your organisation's culture?			
Do you have a security policy or other documentation showing how security procedures should operate within your institution?			
Is this documentation regularly reviewed and if necessary updated?			
Do you regularly meet with staff and discuss security issues?			
Do you encourage staff to raise their concerns about security?			
Badging	**Yes**	**No**	**Unsure**
Do you use badges?			
Do you include an up-to-date photo on badges?			
Do you include access permissions on badges?			
Do you use a unique ID on the badge?			
Do you use anti-counterfeit measures?			
Do you frequently change designs on your badges?			
Do you use large format badges			
Do you include a design on the back of the pass?			

	Yes	No	Unsure
Do you ensure your staff are instructed that they are prohibited from sharing images of their badges online?			
Do you print and distribute badges as close to the event as possible?			
Do you keep designs confidential and allocate unique IDs as late as possible?			
Do you have a emergency response plan and a business continuity plan?			
Do you review and update your plans at least every 6 months? Have you thought through your actions if there is; Firearm and weapon attacks? Terrorist attack nearby? Lockdown/Invacuation? Partial evacuation of the site? Are your staff trained in activating and operating your plan?			
Have you prepared an emergency 'Grab Bag'?			
Do you have access to an alternative workspace to use in an emergency?			
Are your critical documents adequately protected?			
Can you access critical records at a separate location?			
Do you have contingency plans in place to cater for the loss/ failure of key equipment?			
Do you have sufficient insurance to pay for disruption to business, cost of repairs, hiring temporary employees, leasing temporary accommodation and equipment?			

ACCREDIT
Solutions



Do you need help with your accreditation process? Contact us today to discuss your requirements

Accredit Solutions
Studio 10
The Viaduct Brixton
360 Coldharbour Lane
London
SW9 8PL

T: +44 (0)203 904 7681
E: info@accredit-solutions.com
W: www.accredit-solutions.com