Cash & Valuables in Transit

Effective practice guidelines

Introduction

This document has been created by members of the British Security Industry Association's (BSIA) Cash and Transit (CViT) section to detail effective practice guidelines used to minimise the risk of robbery and enhance the protection of staff and customers and the public during the delivery or collection of CViT services.

Targeted armed attacks have led to serious injuries to CViT staff, customers and members of the public. Some robberies are organised by criminal groups to finance further crime and stolen money can help to destabilise communities and provide further opportunities for theft. Additionally, CViT staff going about their lawful duties can be seriously injured and psychologically affected. CViT robberies are not a victimless crime.

The spread of effective practice in these guidelines will make a significant contribution in reducing CViT crime. The aim of this document is:

- To reduce the risk of injury to all persons during the provision of CViT services.
- To provide guidance for the delivery of risk management and threat mitigation.
- To minimise the threat of robbery and financial loss.
- To identify appropriate guidelines for the design and operation of CViT vehicles.
- To assist the Police in reducing crime.
- To demonstrate that the health and safety of employees of CViT companies is at the forefront of their operations.
- To drive continual improvement within the CViT Industry.
- The guidelines are pragmatic, not mandatory and will be regularly reviewed by the Industry.

Who is this document for?

This document has been written to demonstrate to all stakeholders in CViT and customers of the CViT industry that the governance and operation of all members of the BSIA's CViT section meets the standards required to ensure that the applicable legislative requirements are met. Stakeholders may also find this document informative in contributing to their own operational procedures.

Implementation of the guidelines is down to individual BSIA members. Any dispute arising from the application of these guidelines will be the responsibility of the individual companies concerned to be resolved.

Foreword

This document has been developed by members of the BSIA's CViT section with the intention of providing helpful advice to CViT companies and others to reduce the risk of CViT robbery.

The level of effort and investment made by the CViT industry in combating this crime has been (and continues to be) extensive. Investments have been made in all areas of technology, courier training, surveillance vehicles which are funded and deployed in high risk areas and a significant commitment has been made to develop and promote SaferCash / Grapevine activity.

The spread of the effective practice ideas contained within these guidelines will continue to make a significant contribution to reducing the vulnerabilities of customers to this costly, traumatic and sometimes violent crime.

Glossary

ARC	Alarm Receiving Centre
BBA	British Bankers Association
BR	Ballistic Resistance
BRC	British Retail Consortium
BSIA	British Security Industry Association
CEN	European Committee for Standardisation
CHF	Cash Holding Facility
CTU	Cash Transfer Unit
CViT	Cash & Valuables in Transit
ETA	Expected Time of Arrival
Grapevine	Single point of contact for information and intelligence for the Post Office
IBNS	Intelligent Bank Note Neutralisation System
ILO	Industry Liaison Officer
MOU	Memorandum of Understanding
NPCC	National Police Chiefs' Council
NSI	National Security Inspectorate
PAS	Publicly Available Standard
PCN	Penalty Charge Notice
PPE	Personal Protective Equipment
PS	Police Scotland
RIU	Regional Intelligence Unit
SaferCash	The single point of contact for information & intelligence for the BSIA CViT Section
VRM	Vehicle Registration Mark
VSS	Video Surveillance System
Visitor	Includes contractors
PPAD	Personnel Proximity Access Device
1PV	One person vehicle
2PV	Two person vehicle
CSR	Corporate Social Responsibility
SIA	Security Industry Authority

Legislation/standards

The following standards were referenced in the production of this guide:

- BS 7872 - Manned Security Services – Cash & Valuables in Transit services.
- BS 7858 - Screening of individuals working in a secure environment. Code of practice.
- BS EN 50518 - Monitoring and Alarm Receiving Centre
- BS 5979 - Remote centres receiving signals from fire and security systems. Code of practice
- BS 9518 – TC Processing of alarm signals by an alarm receiving centre. Code of practice
- NSI Code of Practice for the Management and Operation of Cash Centres.
- BSIA cash holding facility access protocol.
- BSIA vehicle access protocol for CViT companies.
- BSIA vehicle access protocol for non CViT companies.
- PAS 40 Bank note degradation.
- BSIA's guide to the safe working environment.
- BRC CViT guidelines.
- BBA CViT guidelines.
- PAS 68 Ram Raid Bollards.

Security screening

Vetting Pre Employment

Has to be complied with, this includes information required prior to employment such as:

- Proof of identity.
- Details of education.
- Details of police cautions and Convictions.
- Details of any Bankruptcy and Court Judgments.
- Acknowledgement that misrepresentation or failure to disclose is gross misconduct.
- Authority to approach current or former employers.
- The need for a continuous record of career and history.

Verification

Written verification is required of:

- Date of leaving full time education if within the vetting period.
- Employment history.
- Periods of residence abroad.
- Incomplete employment history to be verified.
- Credit Reference.

DBS Check

A DBS check is required.

Security Screening Timescale

- A minimum of 5 years no later than 12 weeks after employment commenced.
- Longer period no later than 16 weeks after employment commenced.

Additional Application

These guidelines apply to:

- Ancillary Staff.
- Permanent Staff.
- Contractors and Sub Contractors employed in relevant work.

Individuals Employed in Screening

- Must be screened themselves.
- Signed confidentiality agreement.
- Trained to complete screening, training can be completed in-house or externally.

Outsourced screening

Recommendations in British Standards are applied.

Records

Stored securely and in line with provisions of Data Protection legislation.

Cessation of Employment

- Records retained in accordance with individual data policy.
- Documented record of return of all equipment including uniform and identity cards.

Training

Induction training

- Must start within 10 days of commencement of employment.
- Subjects to include; conditions of service, company history.

Pre Deployment Training

Specialist and industry pre deployment training must be given before being rostered for operational duties.

- This should include the SIA licence exam.
- This must have a pass or fail criteria.
- On the job training to commence within 5 working days of the pre-deployment training. To include:
    - Safe carriage of cash and valuables.
    - Prevention of loss of cash and valuables.
    - Provision of a high quality service.
    - Completion of documentation.
    - Vehicle operation.
    - Use and maintenance of equipment.
    - Operational and security procedures.
    - Health and safety training.
    - Incident management.

Refresher training

The CViT Company must have in place policies and procedures regarding the provision of refresher training. Crew refresher training should be provided every 2 years.

Refresher training should include:

- Health and safety.
- Security on the road and reducing risk.
- Personal safety.
- Crisis management.
- Transport law.
- Emergency procedures.
- Vehicles and equipment.
- Operational procedures.

CViT companies must provide CPC training for their drivers to fully comply with EU legislation.

- Training records should be kept for all training showing the date, programme of study undertaken, trainer's name and be signed by both the trainer and student.

It is recommended that Personal Protection Training is given to all CViT staff. This training should incorporate:

- Dynamic risk assessment in attack situations.
- Legal restraints on the use of force.
- Personal protection techniques.
- Post incident procedures.

- Recognition and understanding of current level of threat and risk associated with CViT.
- All SIA licence holders have to renew their SIA Licence every three years, at which point a new DBS check is completed.

Performance monitoring

- The CViT Company should set performance levels for new and existing employees.
- Performance assessors should be identified and a register kept.
- The first performance assessment should be after 3 months and thereafter at periodic intervals not exceeding 18 months.

Intelligence

SaferCash / Grapevine

Intelligence is shared between both operations by regular liaison between the ILOs at SaferCash and the intelligence officers within Grapevine; information is exchanged via daily bulletin, texts, alerts and telephone contact in line with the agreed MOU.

Use of intelligence to aid decision-making and allocate resources

SaferCash produce a number of intelligence and information products including the Annual Strategic Assessment, Monthly Tactical Assessment, Quarterly Reports to support BSIA CViT Section meetings, regional Police and Industry meetings and to support particular National meetings such as the National CViT and Home Office working groups.

These reports include Industry and sanitised Police held intelligence to provide an accurate update of the current position in relation to CViT crime including significant offences, arrests and prosecutions. They also detail emerging trends including changing methods of attack and identification of displacement of offenders. This intelligence is discussed within the meetings between Police and Industry at local, regional and national levels and is used to allocate enforcement and prevention resources within both appropriately.

SaferCash Industry Liaison Officers are located within key strategic areas of the UK. They work with industry security staff and local Police on a daily basis to arrange for Police cover in identified vulnerable areas. They also disseminate live time information and intelligence around suspicious incidents and attacks and feedback directly to crews.

Actively Share Intelligence

SaferCash Police Analysts are located within the South East, West Midlands and North West Regional Intelligence Units with networks established with local Forces across the UK. They have access to intelligence and information held by Law Enforcement and private databases such as SaferCash, UK Finance and Bank of England. This enables effective intelligence analysis and sharing which results in the formulation of bespoke National Intelligence Model products as such Comparative Case Analysis and Crime Pattern Analysis to address specific issues identified at national or regional level. These products can then feed into the Police Regional Tasking Group for adoption as a regional enforcement target or back to industry in accordance with the Information Sharing Agreement with identified prevention options.

SaferCash Governance Group

SaferCash is monitored by a Governance Committee. The Committee is chaired by a Director of the BSIA and is made up of representatives from the CViT industry; the banking sector and Law Enforcement Agencies.

The committee meets bi-annually and review operational activities to ensure effective use of analytical resources; provide financial oversight of the SaferCash income streams and provides strategic advice and guidance to the Head of SaferCash.

Partnership Working

The welfare and safety of all staff working within the CViT Industry is of paramount importance and so it is for the BSIA, along with every member of the CViT Industry, to commit to working in partnership with a variety of different stakeholders to help reduce the threat of harm to such staff.

The CViT Industry has already assisted in the production of CViT Best Practice Guidelines. In recent years, the increase in Industry collaboration with external stakeholders such as Police, central and local Government together with customers has helped reduce the number of attacks committed on CViT staff and has assisted the Police increasing the number of CViT offenders that have been detected.

With the demands on the time and resources available to the UK's Police Forces, it is vital that every avenue of support is explored in order to combat CViT crime. By drawing on the resources and intelligence available from the BSIA and its members, Police Forces around the UK could increase further their success rates in identifying and removing the individuals involved in criminal activity from their community.

Regular dialogue between the BSIA, CViT companies, Law Enforcement Agencies and other Industry Associations will ensure that processes, procedures and mitigating actions are discussed and agreed to reduce risk where appropriate. This contact should be between an appropriate individual responsible for security at a local level and the appropriate security manager within the CViT company. This is to ensure a more coordinated approach to the delivery and collection of cash, seeking to problem solve issues and reduce vulnerability.

Site Surveys

Standard

Risk assessments of service types and premises will be produced through BSIA site survey.

- There will be a procedure in place for the risk assessment of all new and current customer locations.

Effective Practice Specification

- Reviewed as and when required or following an attack.
- Change of circumstances review.
- Communicate findings.
- All risk assessments will be conducted in accordance with current Health & Safety legislation.
- Each risk assessment will consider known and expected attack profiles.
- Systems will be in place to respond to and correct deficiencies as found within such surveys.
- System in place to escalate any issue.

Pavement Protection

Intelligent Banknote Neutralisation Systems (IBNS)

The IBNS is a secure carrying case used to transport valuables, when appropriate, between the vehicle and the customer premises in order to deter criminal attack. In the event of an attack, the case may include a number of features which will aid detection and possibly the recovery of the valuables.

A formal documented risk assessment should be completed prior to the procurement and use of any new IBNS equipment and the assessment should consider the legislation and regulations with respect to the use of IBNS, Health and Safety, Operating conditions and environment and user training.

Any attempt to breach the security of an IBNS casing and operating system should result in the activation of the system and thus the degradation of the banknotes contained within. IBNS activation should result in the degradation of all banknotes, through dye, glue or similar, contained within the casing.

Additional optional neutralisation measures include:

Use of unique marker in order to achieve traceability of degraded banknotes

- Remote activation and/or trigger activation.
- Audible alarm.

Personal Protection

Each Company should complete a formal documented risk assessment in order to assess the activity undertaken by a CViT crew, the risks associated with such activity and the need to issue personal protective equipment.

Deployment of PPE will be based upon the findings of the risk assessment and therefore not necessarily universal.

Currently the following items are included within the definition of PPE, however, this is not an exhaustive list and may be subject to change to address new risks:

- Helmets.
- Body Armour.
- Radios.
- Gloves.
- Personal Alarms.
- Protective Shoes.
- Uniforms.
- Body Cameras.

Operations

Contracts: Ensure written contract exists

A clear written contract between the CViT company and the customer should be drawn up and signed by both parties.

The contract should give the terms and conditions on which work is to be undertaken and should indicate the insured liabilities of the company, which should not be unlimited other than required by law.

The contract should normally be agreed and exchanged before work commences or, in urgent cases, as soon as practicable thereafter.

Copies of all contracts should be kept in accordance with current Legislation and Standards.

Information received whilst tendering for any contract should be kept permanently confidential. Agreements entered into later should not override this obligation.

Any alteration to the contract which results in a change of operational requirements should be endorsed by the company and the customer.

Service Schedule: Establish a schedule of operational instructions

In consultation with the customer, the company should formulate a schedule of operational instructions for the CViT service.

CViT staff should be familiar with the service schedule and the operational practices.

Control & Equipment

Drivers

- Equipment including uniform entered on inventory and signed for by driver.
- Driving licences to be checked every 6 months.
- Company to maintain accident record.
- Requirement to declare driving convictions.
- Training must be under supervision.
- Completion of training documented and records signed by trainer and driver.

Provide assistance & communications for CViT crews

A process should exist to provide or procure assistance and advice for CViT couriers, i.e. company control rooms and SaferCash or similar organisation. Retraining to be given if a break of three months or more from CViT duties.

CViT vehicles should be equipped with telephone, radio or another appropriate communication system(s). Procedures should be in place to allow regular checks of essential communications equipment.

Ensure all equipment is fit for purpose

Equipment used in the connection with CViT operations should be fit for purpose and maintained in accordance with the manufacturer's recommendations. Procedures should be in place to allow regular checks of essential equipment.

CViT & ATM services

Crews should perform simple and regular anti-surveillance measures whilst travelling between service locations:

- Whilst driving from a branch to a service site, and whilst driving between service sites, crews should remain vigilant at all times and be aware of any suspicious vehicles following them and make full use of rear mirrors etc.

- Simple anti-surveillance measures should routinely be taken to identify any suspicious vehicles, i.e. driving a number of times around a traffic roundabout, coming off at junctions and immediately rejoining the carriageway, driving around the block. Crews should make an initial surveillance of the area once arriving at or near the site.

Once arriving at site full observations should be undertaken:

Before exiting the vehicle the crew must visually survey the immediate area around the collection location and satisfy themselves that it is safe to commence the collection.

Vehicles should park as close to the customer premises as possible:

- During any collection/delivery the vehicle must be parked in the position that offers the best possible visibility and security for the crew.

- Where feasible or prearranged, full use should be made of any dedicated parking area for CViT services.

- All crew members must be aware of the location of the service and be fully aware of the details of the delivery/ collection.

When first leaving the vehicle, the local environment should be observed at all times

Whilst a crew member exits the vehicle and proceeds to the customer location they should, as much as they can, maintain full 360 degree observations of the environment to anything or any person that may pose a threat.

Correct PPE and equipment should be utilised

When a crewmember is operational outside of a vehicle, they must wear their protective helmet with the chinstrap correctly fastened and the visor fully down. Body armour (where issued and in use) must also be worn. Crew should ensure they carry all necessary equipment issued to them.

The initial trip across the pavement should be without cash

Wherever operationally feasible, no cash should be carried by the courier on the initial trip in to the customer premises.

For a two man ATM operation, the first crew member will exit the vehicle, check security and secure the premises before any cash is transferred

Where required a survey of the exterior of the premises and front of the ATM will commence before entering the premises, crews must check the front and back of an ATM for foreign objects i.e. extra fascia's, mini cameras, card reader tampering.

First crew member will then enter the premises, secure the door and survey the area immediately around the ATM.

Access to the ATM room is controlled by the first crew member.

The first trip must be with a carry case which contains no money.

The ATM safe door must not be opened until both crew members are on site.

Couriers should continually assess and monitor the environment and any threats and make dynamic risk assessments as necessary

Throughout the length of the service the courier must remain vigilant and aware to threats and should continually assess the situation and options open to him/her.

All couriers should be trained in appropriate risk awareness and assessment, and those operating in higher attack areas should have received additional personal protection training.

All couriers should be alert to known and specific methods of attack and/or intelligence

A system needs to be in place to ensure all couriers are briefed and made aware of current and specific methods of attack and attack intelligence.

This information should be taken in to account by all couriers whilst conducting their dynamic risk assessments.

Couriers should not be kept waiting inside premises

The time a courier is exposed within a customer's premises should be kept to the bare minimum. Agreement should be reached with an individual customer for a CViT service to be afforded priority and the service not unnecessarily delayed.

All couriers need to remain alert whilst inside customer premises

Whilst conducting the service inside a customer's premises, the courier should remain alert to persons already inside the premises and those coming and going.

A service should be suspended or aborted when suspicious activity is noted within a premises

Suspicious activity should be noted and the situation assessed. A decision should be taken to suspend a service whilst any suspicious persons are noted and this communicated to the customer.

Full use should be made of any cash transfer equipment or secure area

Wherever possible, agree with the customer the most secure method for transfer of cash by utilising secure rooms, air-locks, cash docks, cash transfer chutes or similar devices.

Couriers should remain alert when returning to their vehicle

Couriers returning to their vehicle, or travelling between the vehicle and the customer premises, should as much as possible maintain full 360 degree observations of the environment to anything or any person that may pose a threat.

The outer door of an ATM room must be controlled at all times

Crew person 1 is always responsible for controlling the outer control door from inside the room/POD/bastion unit/premises.

If a 2 person crew, at no time during the service should both crew persons be on the pavement at the same time

Throughout the service crew person one must remain secured within the ATM room, or within the customer premises for a free standing machine.

The sequence of cassette values and denominations carried across the pavement should be changed and varied as necessary

Local agreement should be set up for the sequence of cassette movements to be changed as and when necessary, based on attack threat.

Surveillance

Overview

Surveillance plays a critical role in the protection of staff, the public and company assets. The level and frequency of surveillance and whether the surveillance is covert or overt should be determined using a risk based approach.

Training

It is essential people involved in surveillance work; whether this is to ensure staff are completing crew roles correctly or whether the purpose is to support crew roles by providing additional surveillance in high risk areas are trained and understand the importance of the role.

Consideration needs to be given to appropriate refresher training in line with advances to company operating procedures and technology used within the CViT industry.

Standard Operating Procedures

Operatives should be deployed in line with up to date assessments of risk in terms of customer location, service type and area; this will include recent attack data and suspicious incidents reported.

They should also liaise regularly with Industry stakeholders such as SaferCash, Grapevine, Vanguard control rooms and Industry Liaison Officers to keep in line with recent activity and threats.

Technology

Consideration should be given to adequate VSS recording of what the observation operative witnesses to support any failings or good practice identified following the surveillance.

Supporting Technology / Remote Surveillance

VSS equipment at all central, depot locations is required to protect the staff working in the location and business, customer assets. Additional remote surveillance of a depot location using an ARC facility is required.

For surveillance during customer visits the level of surveillance and evidence gathering equipment used is at the discretion of each company but will likely include the use of body worn cameras in areas deemed to be of a higher risk.

Wider Industry responsibility

They should also liaise regularly with Industry stakeholders such as SaferCash, Grapevine, Remote monitoring control rooms and Industry Liaison Officers to keep in line with recent activity and threats.

Attack Management

Attack Management – Policy and Procedures

Each company will have in place procedures and policies for dealing with and mitigating the threat of attack.

Preparing in advance of any attack

The impact on individuals who are the victims of any attack will vary depending on a number of factors every attack must be managed as having the potential of being a serious incident.

Prior to any attack primary focus should be on how to prevent the attack occurring. This is achieved by detailed accurate risk assessments conducted by trained experienced members of staff.

Liaison should be made with Police forces. Risk assessments must be dynamic and constantly reviewed. Contingency plans compiled with the Police and to include relevant staff should be implemented and tested.

Training for staff in the event of an attack

Initial training must equip staff with the knowledge on how to reduce the chance of attack and also give a detailed knowledge and skills on the procedures to be adopted following any attack.
They will be trained to operate all security systems and have basic driving skills to be able to use defensive driving techniques to prevent any attack.

Staff to be made aware of what actions they take to secure and preserve evidence.

The initial training and licensing must be constantly updated and the requirement to renew the SIA license must be vigorously enforced.

Staff must receive the appropriate training as regards their actions in the event of a depot attack The contingency plan must be tested regularly and documented to ensure compliance.

Actions to be taken immediate post attack

All Managers attending attacks trained to a sufficiently high standard to offer support to the victims of crime. This support should be through the Human Resources (HR) department and consideration given to liaising with the Police who are investigating the crime. The skill of staff diffusers must not be taken for granted and should be regularly tested and refresher training provided.

Company attendance at scene of attack

Deploy resources quickly to attend the scene of any attack. Liaise with Police and, if appropriate the crew, at the scene and have detailed knowledge of operational procedures and security systems.

Post Attack Site Survey Review

In all attacks an immediate risk review must be completed before a further collection or delivery is made. A further detailed review of the initial site survey risk assessment must be completed.

Provision of post attack care/counselling support

Provide post attack care and counselling support. It is essential that this activity is offered and if taken up is provided only by competent persons. Some organisations may use competent Operational employees; many will use the HR Department to undertake this task.

Police and Court Liaison

From the outset of any attack close liaison must be maintained with the Police. The company must make available to the Police any relevant information in their possession; statements taken by the company must be made available to the Police. Consideration for the payment of rewards should always be brought to the notice of the investigating officers prior to any reward payment being made. Where a member of staff is to attend Court to give evidence. The appropriate support should be given.

Media Management

The disclosure of any information whether it is for external circulation or internal circulation must be tightly controlled. Companies should not disclose any information unless it has been through their own media department. Each company should have a dedicated system to ensure press releases are only released having consulted with the Police.

SaferCash / Grapevine

Both of these organisations play an important role in the prevention and detection of CViT offences. They are an extremely useful conduit for CViT information/ intelligence and recorded crimes. Report incidents and attacks to SaferCash / Grapevine as soon as is practicable for any robbery or attempted robbery. SaferCash also has the facility to record and disseminate fast time intelligence.

Internal Investigation

CViT companies are responsible for the safe storage of cash and valuables inside Cash Handling Facilities and for the transport of those commodities.

No matter what level of physical security is in place, nor the level of vetting of employees, there is always the risk that a rogue employee, or employees, will breach that security and steal cash or valuables entrusted to the company for safe keeping.

An individual company can be seriously damaged by the dishonest actions of its employees and the reputation of the Industry as a whole might be tarnished if it does not have systems in place which allow discrepancies to be quickly and routinely detected.

These systems should be both a part of the normal ongoing audit trail carried out during the day to day running of the company as well as the procedures in place to allow spot checks to be carried out, both on processes, staff and the cash being held or transported.
Companies must ensure that they have the ability to be able to properly investigate any discrepancy detected. This may mean utilising the skills of employees as well as employing an external expert. Collaborative working between companies is important for sharing information on methods and staff involved in criminal activity.

The whole process of internal investigation needs to be transparent so as to gain the confidence of all parties including staff, management, unions and customer.

Dismissal

Organisations should ensure they have robust processes in place to reclaim equipment and uniform when employees leave the business.

Records should be maintained of employees who have been dismissed for theft or dishonesty to ensure they are not subsequently re-employed.

Physical Security

Access Control

- To ensure all pedestrian and vehicular access is effectively controlled and monitored thereby reducing the risk of intrusion or unauthorised access.
- Access into any premises and to the secure areas will be controlled via a suitably effective access system that is controlled either remotely by an approved third party or from within the CViT / Cash Centre premises.
- Each company must have a robust and proven Access Control Policy (ACP) that outlines procedures for (i) out of hour access. (ii) access requirements for visitors,(iii) identification protocols, (iv) pre-notification of attendance requirements.
- Entry to the secure area should be via a personnel transfer unit (PTU), or similar facility e.g. biometrically controlled airlock.
- Access to any secure area will be restricted to one-person entry at any one time.
- All entry/exit points shall be monitored by VSS.
- Visitors must be escorted at all times when visiting any secure area.
- A written record will be kept of the time and date of entry and exit of both staff and visitors.

Alarm Systems

To secure a facility and optimise speed of response to incidents, all CViT Branches and Cash Centre's will have full electronic alarm systems installed that shall be remotely monitored. The premises should be protected by an intruder/ hold-up alarm system, connected to a certified ARC e.g. BS 5979, BS 9518, BS EN 50518, and has Police response i.e. has a current URN.

Central site (Depot location)

All CViT depots must have an alarm system as part of the site, anti-attack deterrent. The complexity of each system will depend on factors such as; the number of staff working in the location, the value stored on site, the location of the depot as well as the contractual or regulatory requirements of customers and stakeholders.

Alarm systems must be tested and maintained, with the facility to escalate Alarm faults identified for quick resolution to ensure continuing site and people security.

The site alarm system will be monitored by an off-site facility (ARC).

Each site must have the facility to quickly raise an alarm internally that will trigger a response from Police or other Security related organization instantly; an example of this would be a Personal Attack / hold-up Alarm system.

A program of internal tests / risk assessments is required to ensure continued robustness of the operation against various forms of attack.

Crew / Vehicle

Each CViT vehicle must have an alarm system capable of raising an alarm to the remote monitoring centre and crew role completing cross pavement activity to and from customer premises must have a mobile alarm that can also be activated and triggers an alarm in the remote monitoring centre.

External / Internal cameras

VSS should be installed to cover external areas of a Branch or Cash Centre using Analytical software to give an alert of a breach of the perimeter at the site and National Control Centres/Monitoring station:

- Internal and external VSS equipment must be installed and managed in compliance with the Data Protection Act.
- Covert cameras will only be used in accordance with the above.

A survey should be complete to ensure that all areas requiring VSS have suitable and effective coverage. Sufficient lighting levels should be available both internally and external to ensure VSS coverage and recordings are of suitable quality. Consideration should be given to some lighting remaining on in designated areas when the branch is closed, (to facilitate out of hours remote monitoring of the branch).

Physical security measures that deter and defend against ram-raid attacks.

All CViT branches / Cash Centre's will have anti-ram measures installed following a site specific risk assessment. Historically such anti-ram measures may have included large boulders, motorway barriers, stressed cables, bollards or similar.

Construction, Design and Build

Best practice is to apply requirements in BS 7872.

Perimeter Fencing

Best practice is to apply requirements in BS 7872.

Vehicle Gates

Best practice is to apply requirements in BS 7872.

Vehicle Bay – Shutters / Doors

Best practice is to apply requirements in BS 7872.

Secure Area Doors / Windows

Best practice is to apply requirements in BS 7872.

Tiger Kidnap

Policy and Procedures

Each company will have in place procedures and policies for dealing with and mitigating the threat of Tiger Kidnap.

Effective Practice Specification

- An annual assessment will be carried out on all job types and support tailored to roles which are deemed as most at risk.
- During vehicle and branch design mitigating the possibility of a Tiger Kidnap occurring should be at the forefront of policy.
- Regular branch Tiger drills should be conducted.
- All staff should have exposure to Tiger Kidnap training as soon as they are inducted.
- All staff should be subject to an annual Tiger Kidnap training refresher.
- A Crisis Management Team should be in place for dealing with, and providing, an effective Tiger Kidnap management strategy.

Media

Organisations should have a process in place to ensure employees are aware of how to respond to requests for information from the Media. Organisations should consider implementing a procedure that directs any approaches from the Media to a single point of contact who is trained in media communication skills.

Supply Chain

Ensuring the security and integrity of the supply chain by reviewing and monitoring critical suppliers' processes and the appropriate vetting of all staff involved in the supply chain. The supply chain must be able to demonstrate an understanding of the criticality of their product/service in the Cash and Valuables in Transit Service.

Supply Chain Customers

Customers must feel confident in the integrity of the supply chain and have the ability to audit and review the supply chain process.

Critical Suppliers

The processes and procedures of critical suppliers within the supply chain should be reviewed and monitored to ensure security and integrity.

Vetting

Appropriate levels of vetting must be conducted for employees involved in the supply chain process.

Corporate, Social and Environmental Responsibility
The supply chain must be challenged to continually improve its approach to the management of CSR.

Data Protection

Attention is drawn to data protection legislation.

Corporate Social Responsibility (CSR)

The Company will conduct all business in accordance with relevant legislation. The Company will act in accordance with local employment law and the Fundamental Conventions of the International Labour Organisation (where permitted by local legislation).

The Company will take reasonable steps to identify and minimise the environmental impact of the product/service and any associated operation. The Company will ensure compliance with all relevant environmental legislation and will act to prevent pollution and dispose of waste in a responsible manner.

Information Security

Recent high profile information security breaches and the value of information are highlighting the ever increasing need for organisations to protect their information.

Information is a key component to all organisations. Information can exist in many forms, from electronically stored corporate databases, right down to hand written notes. Information can be sent both electronically or by post.

There is a need to establish a comprehensive Information Security Policy within all organisations. It is important to ensure that the confidentiality, integrity, and availability of both vital corporate and customer information is protected.

To achieve this, the Information Security Management System ISO/ IEC 27001 can be used as a guide when developing internal policy around Information Security and Data Protection.

Business Continuity

Each company will have in place a Business Continuity Management System for dealing with and recovering from business disruptions.

Business Continuity Management - Business Continuity Management (BCM) demonstrates the CViT industry's duty of care to customers and emphasises due diligence to key stakeholders, including the general public. It helps safeguard the industry's reputation and will ensure that the industry can continue to operate whilst meeting expectations and obligations.

Best practice standards (ISO 22301) - All companies should base their Business Continuity Management System (BCMS) around the principles of the best practice standard ISO 22301 with a management framework that gives companies the essential controls to address risks and monitor and measure the organisation's ability to manage, and recover from, disruptions.

All companies should follow the Business Continuity Life Cycle

1. Manage the BCM Programme by embracing continuous improvement (Plan, Do, Check, Act).
2. Understanding the organization (Risk analysis and business impact analysis).
3. Determining BCM Strategies (Recovery Strategies).
4. Developing and implementing a BCM response: (Develop and maintain BCPs).
5. Exercising (testing), maintenance, audit and self-assessment of the BCM culture on a yearly basis.
6. Embedding BCM into the organization's culture, with clear roles, responsibilities and authorities.

For other information please contact:

British Security Industry Association

t: 01905 342020

e: info@bsia.co.uk

www.bsia.co.uk

About **the BSIA**

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.