Loss Prevention Standards – Asset Class(es)

Security – Personnel Risk Management

Version: 1.0
Date: 31st December 2024

Losses relating to the workforce can include theft, collusion with thieves, fraud, arson, and other wilful damage.

This Loss Prevention Standard provides a summary of the relevant pre-employment checks undertaken in the United Kingdom, along with guidance on ways to reduce the exposure to such losses.

AVIVA

Security – Personnel Risk Management

Introduction

Losses or damage linked or attributed to workers and contractors is not widespread but not uncommon. Risk exposures include but are not limited to :

- **Theft.** Money, workplace equipment and stock, especially high value items such as electronic devices, tobacco, spirits, perfumes etc., are often targeted by dishonest employees and visitors, as per this theft by a security guard between November 2022 and January 2023.
- **Collusion.** Workers can work with criminals, or be coerced into providing access to premises, security codes, floor plans etc., to assist in a theft incident.
- **Internal Fraud.** Workers with access to financial systems may be able to manipulate accounts to defraud employers e.g. creating false sales, skimming etc.
- **Cyber.** Workers can carry out electronic theft or aid cyber criminals.
- **Arson and Wilful Damage.** Disgruntled workers, contractors and former staff can take retribution against perceived slights and inflict damage to property, including arson attacks as illustrated by this arson attack by a former employee in October 2022

Note: This document relates to workforce risk management and pre-employment checks with a focus towards property loss prevention and related risk management guidance and is not intended to address liability exposures or wider human resources procedural requirements.

Pre-Employment Screening/Background Checks

Checking the backgrounds of potential employees, prior to commencement of employment, can provide useful insight into an applicant's employment history, right to work in the country, and in some cases criminal history. It is also a good way to help assess the integrity and honesty of the individual.

There are a number of checks that can be completed, however some can only be undertaken where proportionate, and which reflect the responsibilities and duties of the advertised role.

Criminal Record Checks

These are a key means of checking whether candidates for roles have a criminal history that may not align with the nature of the proposed employment. Such checks are legally required for some roles, such as those involving children or vulnerable persons, however, can otherwise only be used when proportionate and relevant to the proposed role.

There are four levels of criminal record checks available:

- **Basic** – This is limited to unspent convictions and conditional cautions, and can be requested by any employer, organisation, or the applicant.
- **Standard** - Standard Checks provide information about spent and unspent convictions, cautions, reprimands, and final warnings, and can only be requested by the employer or recruiter for certain eligible roles. Refer to the Gov.uk Eligibility Guidance for Standard DBS checks for further guidance.
- **Enhanced** - Enhanced Checks provide the same information as a standard check, however, also includes any information held by the local police force for current and any previous addresses that are relevant to the proposed employment role. As with Standard checks, these can only be requested by the employer or recruiter and can only be carried out for certain eligible roles. Refer to the Gov.uk Eligibility Guidance for Enhanced DBS checks for further guidance.

- **Enhanced with barred lists** - These give the same information as an Enhanced Check, but also disclose whether the applicant is on a list of people barred from carrying out certain activities with children or adults). These checks can only be requested by an employer or a recruiter, and only carried out for eligible roles.

Whilst the eligibility to carry out Standard and Enhanced checks is legally limited, basic Checks can be freely undertaken and provide useful information that can avoid recruiting unsuitable persons.

Employees of third-party security guarding companies, licenced by the Security Industry Authority (SIA), will have been subject to Standard Checks, hence business and organisations should only procure security guarding services from an SIA licenced company.

Prospective employees can be asked about their criminal history, if considered necessary and proportionate. The extent to which an employer can base their decision to hire someone because of any spent convictions is however extremely limited, and legal or Human Resources advice may be necessary.

It is important to note the prospective employee does not need to volunteer any information unless asked, and spent convictions, warnings, cautions etc., do not need to disclosed after a specified period of time.

Note: It is also prudent to undertake regular ongoing criminal history checks to ensure a person's criminal history has not changed.

- For activities and roles in England and Wales, criminal history Checks are done by the Disclosure and Barring Service (DBS).
- For activities and roles in Scotland, criminal record checks are done by Disclosure Scotland.
- For activities and roles in Northern Ireland, criminal record checks are done by Access NI.

Reference Checks

A reference check helps ensure the prospective candidate is suitable for the role.

- There is no legal obligation on an employer to undertake reference checks other than for certain roles in the financial services industry, as required by the Financial Conduct Authority.
- Employers should however always seek at least one reference to ensure the applicant is appropriately qualified and/or experienced to perform in the role.
- It is standard practice for an employer to make a conditional job offer to a successful candidate, subject to satisfactory references being provided.
- An employer is not generally obliged to provide a work reference, however when provided, it must be fair and accurate, and employees can challenge a reference if they deem it unfair or misleading.
  - ✓ Damages can be sought in the event of an unfair or misleading reference being provided.
- The reference request should include as much information as possible relating to the persons suitability for employment, however the referee's response may be limited to basic information only e.g. details about the person's performance and whether their employment had been terminated, employment dates, salary, and job title etc.

Note: Employment references are protected under the Data Protection Act and the content of the reference, or any information related to it, cannot be disclosed to the applicant unless the employer who provided the reference consents.

In addition, consideration should be given to:

- Verifying skills and experience in the type of work to be undertaken.
- Membership of professional / trade bodies.
- Formal induction on first attending site and ongoing management / supervision of the individual.

Credit Checks

Undertaking a pre-employment credit check can help identify persons who are financially vulnerable, potentially increasing the risk of workplace theft, fraud etc.

- Various databases are available for credit screening including bankruptcy, County Court Judgements, voluntary arrangements, decrees, and administrative orders.
- This should be considered when the advertised role provides access to high value items, sensitive financial information, money etc., however the applicant should be asked for permission.

Note: It may be prudent to undertake ongoing credit checks to ensure the financial history of key workers remains satisfactory.

Other Checks

Qualifications and Credentials Check

In some instances, employers may wish to undertake verification of degree's, other professional qualifications, and/or educational background checks. This check is imperative for some sectors such as medicine, finance, law etc.

- Copies of certificates and educational history will be required to undertake such a check.

Adverse Media Checks

The Adverse Media Check enables prospective employers to search media sources for articles linking the candidate to criminal activity and other undesirable media such as racism, extreme political views, etc., all of which may pose a reputational risk to the organisation.

- Adverse media checks are required in the United Kingdom for financial institutions, however, are otherwise discretionary.

Right to Work Checks

All employers in the UK must conduct right to work checks before employing workers. This is to ensure individuals are legally allowed to work, and there are no restrictions on them undertaking the role they have applied for. Full details can be found at Home Office - Right to Work Checks, and the guidance should be closely followed.

Guidance should be sought from a Human Resources Specialist and/or the Home Office website above given the mandatory nature of this check, however such checks, whilst not directly likely to impact the exposure to physical loss or damage, may help prevent reputational loss to the organisation or business, and avoid significant fines.

Medical Checks

Medical checks can only be requested if the job requires it e.g. physical lifting, or the check constitutes a specific legal requirement of the job role in question, for example, where a person who drives for work would need to pass an eye test.

As with rights to Work checks, failing to undertake a medical check is unlikely to impact the organisation or businesses exposure to physical loss or damage. And whilst discrimination must be avoided, such checks allow for changes and enhancements to be made which allow the person to perform the role well and avoid future injury. This may help reduce the potential for Employers Liability claims and additional cost due to worker absence.

Identity Check

Identity checks normally would be covered as part of the Right to Work checks discussed above, however an additional document may be required if the right to work documentation does not include a photo, for instance a UK birth certificate.

Sanction Screening

These checks safeguard financial institutions from engaging in business with sanctioned entities. This reduces financial risk, such as money laundering, as well as reputational damage.

- ✓ A requirement for financial institutions with potential fines and legal repercussions for breaches.

Whilst the above checks are necessary for financial institutions, there is no legal requirement for other sectors to undertake such checks. The UK Government maintain a UK Sanctions list which can be cross checked where appropriate.

CIFAS Checks

The Credit Industry Fraud Avoidance System (CIFAS) is a fraud prevention service in the United Kingdom allowing persons to be screened to verify their identities against cases of previous identity abuse e.g. identity fraud, or where an identity is at risk of abuse.

- ✓ CIFAS checks are mandatory for financial services companies and some other sectors dealing with sensitive financial information. HR Guidance should be sought in these instances.
- ✓ Such checks should be considered in other sectors if there is a heightened potential for fraud e.g. access to financial systems.

Security Precautions

The following guidance focuses on the security precautions that should be undertaken to reduce the risks of workforce theft and unauthorised access to premises. Aviva Loss Prevention Standard **Arson Prevention** provides detailed guidance on managing the risks of arson.

Premises Access

- Visitors, whether invited or not, should only be able to access reception areas via designated walkways, remote from stores of combustible goods or flammable gases etc.
- Visitors should not be permitted to access the buildings or yards areas without authorisation, and/or accompaniment.
  - ✓ Sufficient warning signage should be displayed to this effect in prominent locations.
  - ✓ Workers should be empowered and encouraged to challenge unauthorised persons and remove to sterile nominated areas.
- Where access by unauthorised persons is viable, ensure appropriate secured compounds are used to house flammable gases, fuel tanks, waste areas, pallet stores etc., safely.

Cash Handling

- Eliminate the use of cash, thereby removing the risk. Where this is not possible, reduce the use of cash as far as achievable and restrict access to cash and codes/keys to safes to minimal persons.
  - ✓ Ensure a safe key policy is in place stipulating storage requirements. Except when access is required, e.g. for depositing or removing cash, safes should be kept locked, and any key(s) removed and held in the personal custody and control of an authorised person. Outside normal business hours, and whenever the premises are otherwise left unattended, the key(s) to any safe, or if it uses a code / combination lock details of the code(s), must not be left within it.
  - ✓ Refer Soldsecure for a range of approved security products.
- Ensure receipts are recorded for all company purchases on company expenses and routinely audit all transactions.

Access Control

Ensure codes and keys to premises are closely controlled.

- Maintain a register of keyholders and keyholder rules detailing how keys should be stored, carried etc.
- Limit access to secured areas to the minimal number of persons necessary.
- Routinely review the list to ensure keyholders remain limited and appropriate.
- Undertake routine checks to ensure keys are being carried and stored as per site rules.
- Ensure rules are in place to remove keys and change codes immediately upon persons leaving the business, or who are no longer authorised to access the facility.
- Codes should be changed routinely in addition to the changes recommended above. The frequency of changes should be based on a risk assessment and the value and theft attractiveness of contents and stock.

Housekeeping

Ensure stores of combustible goods, waste stores, flammable gases are organised and adequately separated to reduce the fire load in high risk areas.

- Such stores should also be secured, remote from site fencing and site access points to help reduce the potential for ignition and malicious damage.
- Refer Aviva Loss Prevention Standard **Housekeeping** for further guidance.

Video Surveillance Systems

A detector activated Video Surveillance System (VSS) is an excellent means of detecting unexpected/unauthorised movement and activity in and around buildings and should be considered.

- Where permanent security guarding is not present, VSS should be monitored by an accredited Remote Video Response Centre (RVRC) and preferably achieve level 1 police response.
- The VSS should be positioned to cover all points of the site perimeter, entrances, and all internal areas other than rest rooms and changing rooms.
  - ✓ Cameras should utilise night vision technology to ensure clear images can be seen and recorded.
  - ✓ Cameras should also be tamper-resistant to avoid masking or shielding.
  - ✓ To achieve level 1 police response, the system will need to be installed, maintained, and monitored to the requirements of **BS8418: Design, Installation, Commissioning and Maintenance of Detection-Activated Video Surveillance Systems (VSS)**. **Code of Practice**.
- To ensure the best quality of service, the Installer and RVRC should be members of a UKAS third-party accreditation/approval scheme, such as those provided by the National Security Inspectorate (NSI), or the Security Systems and Alarms Inspection Board (SSAIB). This is required for police response.
- The incorporation of an audio challenge facility, which would allow the RVRC to issue warnings to any unauthorised persons attempting to access the site or behaving suspiciously, should be considered.

Security Response/Guarding

Should there be anticipated delays in police response in some localities e.g. remote areas, it may be more appropriate to utilise a security company to provide keyholder and VSS detection response services, rather than rely on police response.

Regular security patrols of the site by the security company can also provide a significant deterrent to intruders.

- Any such providers should be members of the Security Industry Authority and provide their services in accordance with the requirements of **BS 7984-3:2020 Keyholding and Response Services - Provision of Mobile Security Services. Code of Practice,** and have SIA Approved Contactor status**.** They should also be members of a UKAS third-party accreditation scheme, such as those provided by the National Security Inspectorate (NSI), or the Security Systems and Alarms Inspection Board (SSAIB).

Intruder Alarms

Intruder alarms are an essential means of securing premises and preventing unauthorised access.

- Ensure intruder alarms are set during periods of unoccupancy.
- The Intruder alarm system should be programmed to provide a part setting facility to enable alarm detection in high risk / unattended areas to be set independently whilst the premises are in use elsewhere.
  - ✓ Part setting of the intruder alarm allows alarm protection to be provided to potentially vulnerable parts of a premises whilst other areas are in normal use.
- To achieve level 1 police response, the system will need to be installed, maintained, and monitored to the requirements of **PD6662: Scheme for the application of European Standards for intrusion and hold-up alarm** systems and **BS 8243:2021 – Design, installation and configuration of Intruder and Hold-up Alarm Systems designed to generate confirmed alarm conditions**.
- To ensure the best quality of service, the Installer should be members of a UKAS third-party accreditation/approval scheme, such as those provided by the National Security Inspectorate (NSI), or the Security Systems and Alarms Inspection Board (SSAIB). This is required for police response.
- Refer Aviva Loss Prevention Standard **Intruder Alarms – Guidance for Customers** for further guidance**.**

Secured Stores and Compounds

High value and/or theft attractive goods such as electronic equipment, tobacco, spirits, perfumes, designer clothing etc., should be separated from other stocks and held in secured stores or compounds.

- Such compounds should be of robust construction and be fully enclosed.
- Access to the stores should be limited to minimal persons.
- Access codes or locks should be changed regularly, including when workers leave the business.
- Stock levels should be catalogued, and stock checks/audits regularly undertaken.
- Particularly high valued goods should be subdivided rather than storing in single blocks, this helps spread the risk.
- Any external openings to security stores/compounds such as doors and windows should be fitted with security bars or grilles.
  - ✓ **LPS 1175: Requirements and Testing Procedures for the LPCB Certification and Listing of Intruder Resistant Building Components, Strongpoints, Security Enclosures and Free-standing Barriers** provide useful guidance on security compounds and security shutters.

Site Inspections

Regular security inspections should be undertaken to help identify tampering or potential breaches of security protections.

- These security inspections should focus on perimeter, physical and detection security measures and should be recorded.

Personal Searches

Personal searches can be undertaken, provided workers are aware such a policy exists and give express consent to the personal search.

- Use of a search authorisation form is recommended to record the authorisation to undertake a personal search, should this be later challenged.
- The search should be conducted by a member of the same sex with a same sex chaperone, and in a private area. The search should not involve physical contact, rather workers should be asked to empty their bags and pockets.
- Theft of company property should be defined within employment contracts as gross misconduct to allow for appropriate disciplinary action to be taken.

Note: Given the potentially contentious nature of this action, HR guidance should be sought before introducing a personal search policy.

Enhanced Security

Security measures should be enhanced immediately following a 'bad leaver' incident if there is any suspicion that the person may seek retribution. This should result in closer observation, controlled access, updating security codes and locks and reminding workers to be vigilant.

Cyber Security

Cyber security exposures should be reviewed to ensure appropriate protections and procedures are incorporated including data access approval management.

- ✓ Refer Aviva Loss Prevention Standard **Cyber Security - Top 12 Tips to Protect Against Cyber Attacks** for further guidance.

Key Action Steps

- A system of background checks/pre-employment screening should be introduced, if not already in place, reflecting the variety of roles and the exposures to loss or damage these roles create, notwithstanding and legal or regulatory requirements.
- Arson and theft related losses in particular are often attributed to people with previous offences in this regard and a robust pre-employment screening process may help identify such persons prior to full employment.
- The system of pre-employment checks should be routinely reviewed to ensure compliance with new or changing requirements and guidelines.
- Ensure access to the premises and specific areas is restricted as far as achievable.
- Operate a strict key and code management policy, updating regularly, particularly when persons leave the organisation.
- Use secured stores and compounds for storing high value/theft attractive goods.
- Eliminate or restrict access to cash and high value/theft attractive goods to minimal persons.
- Adopt a part setting facility to enable alarm detection in high risk / unattended areas to be set independently whilst the premises are in use elsewhere.
- Ensure the site VSS covers all areas of the premises.
- Undertake security inspections for breaches or tampering of security measures.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners, including:

- Reputational risk: **Riskeye**

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- www.gov.uk/employing people
- Home Office - Right to Work Checks

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

Relevant Aviva Loss Prevention Standards include:

- ✓ **Arson Prevention**
- ✓ **Housekeeping**
- ✓ **Intruder Alarms – Guidance for Customers**
- ✓ **Security – Doors and Windows**
- ✓ **Cyber Security: Top 12 Tips to Protect Against Cyber Attacks.**

To find out more, please visit Aviva Risk Management Solutions **or speak to one of our advisors.**

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential, or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

31st December 2024

Version 1.0

ARMSGI2202024