RSA

Improving Site Security

Risk Bulletin

RCBM001 - November 2020

In order to assist you with the successful operation of your business, this best-practice risk control bulletin provides information and support in the area of marine-cargo site security. Non marine-cargo sites with similar risks, will also benefit from the guidance provided.

This guide makes reference to guidance and best practice published within the United Kingdom.

Further information is available from RSA's Risk Control Guide RCG017 – Security.

Fencing & Gates

- Mesh steel or steel palisade fencing should be fitted in accordance with BS1722 to the boundary.
- There should be no overhanging trees or shrubs that could give cover to thieves trying to gain access or to those wishing to cause malicious damage.
- Additional barriers or bollards should be placed between fence posts to deter against fence panels being removed for thieves to create a new point of entry/exit
- Where fitted, gates should:
  - be of commensurate strength to the fencing.
  - have their hinges capped by a disc of mild steel welded to the top of the pin.
  - be secured by a good quality closed shackle padlock to at least Grade 5 in accordance with BS EN 12320 - for example Assa Abloy Union 1k12 Conquest.
- Where practical the padlock should be further protected from cutting tools by the addition of a protective shrouds or cover.
  - always be securely locked outside of working hours.
- Where automated gates are used - operated by fob, proximity card, pin code pads, phone / remote access, induction loop or trip beam etc. - additional protocols / controls will need to be introduced to prevent tailgating and/or other methods of unauthorised access.

Barriers / Posts

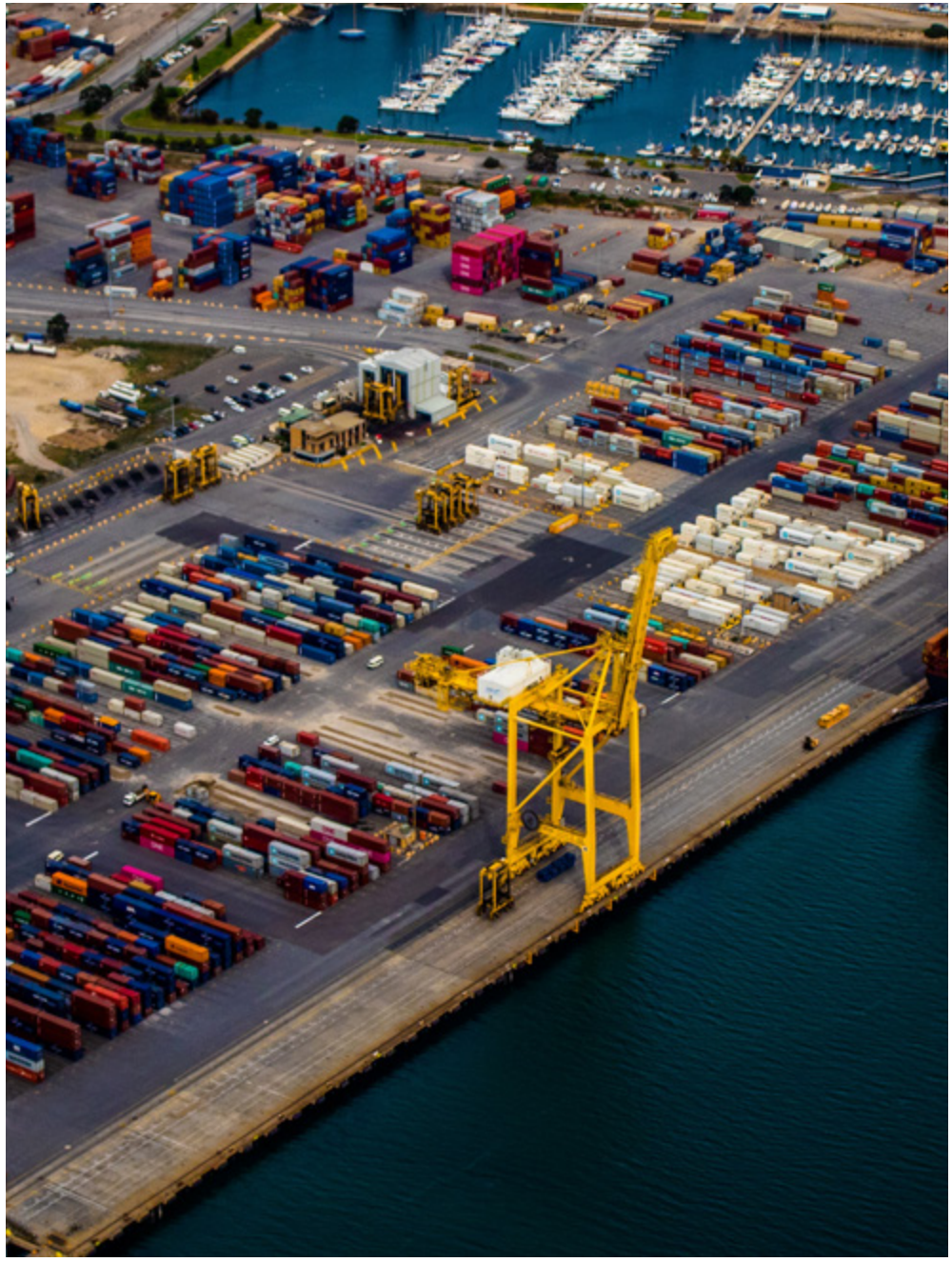
- Other features to consider are the use of traffic control barriers at the site entry and exit points, or telescopic or retractable posts / automated rising kerbs. The use of bollards, posts, fixed or removable barriers or strategically positioned planters should also be considered for anti-ram protection to shutter doors.

CCTV

- For CCTV on sites with lower-value / non-thief-attractive cargo, the system should be
- Digital and image quality should be sufficient to allow recognition of persons and vehicle registration numbers. Images should be recorded (analogue systems should be replaced), the recording device should be securely protected to prevent tampering and there should be a maintenance contract in place to rectify faults within 24 hours.
- For CCTV on sites with higher-value / thief-attractive cargo high value should be remotely monitored, installed and maintained by a company which is acceptable to the Police and recognised by the National Security Inspectorate (NSI) as a Gold installer of CCTV systems.
- This should be installed in accordance with BS8418 and have remote monitoring of detector activated CCTV systems, with ISDN line signalling with Redcare monitoring or secondary wire free signalling capabilities.
- Lighting for all systems should be adequate to allow viewing and capture of CCTV images (see Lighting).

Security Guarding

- Security guards employed should be Security Industry Authority (SIA) licensed personnel supplied by companies approved by the National Security Inspectorate (NSI) or Security Industry Authority Approved Contractors Scheme (SIA-ACS).
- Guards should have access to panic alarms or personal attack alarms, especially if they are lone workers, linked to a suitably accredited monitoring station.

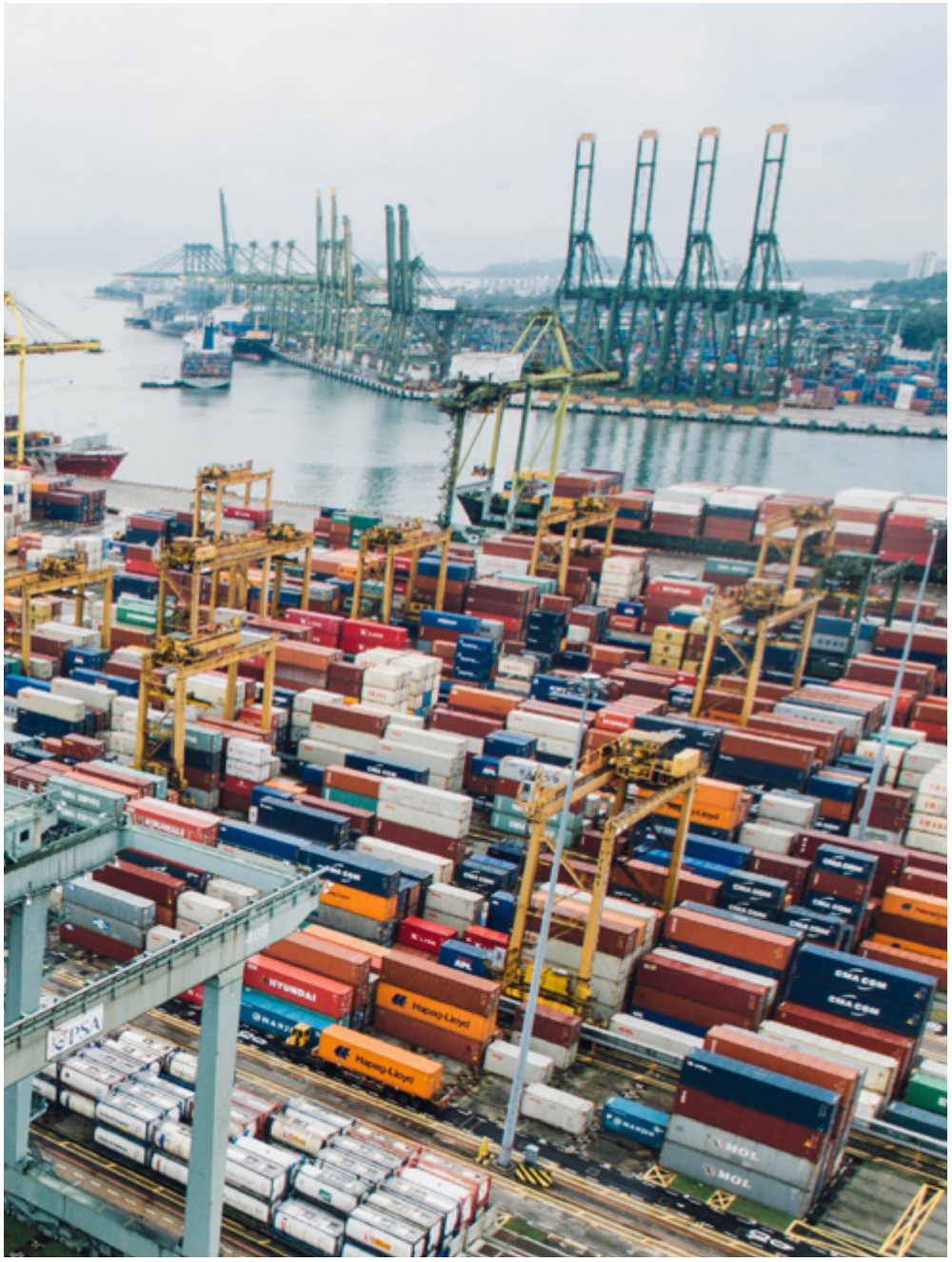


Site Access

- There should be procedures in place to control access to the site, ensuring that any persons entering are authorised to do so and are who they say they are. All third parties and vehicles should be logged into and out of the site and a record of such access retained (including vehicle registration numbers).
- Procedures should also be in place to control exit from the site, ensuring that persons removing cargo are authorised to do so [see fencing / gates section].
- Where possible site access should be restricted to one point only with all other site access points locked whenever they are left unsupervised

Vehicles & Trailers (if left on site overnight or at weekends)

- Vehicles and trailers should be parked in an area covered by the CCTV system and/or in view of security guards.
- Hard-sided vehicles and trailers should be parked rear to rear or with the rear against a building to prevent access to the doors.
- Vehicle immobilisers and/or alarm systems should be fully operational.
- Tractor units should be detached from trailers (unless adequate security devices are fitted to the tractor unit) and detached trailers should be fitted with king pin or airline locks. [Conversely, where the tractor unit has adequate security devices, leaving it coupled to the trailer could make it more difficult to remove the trailer.]
- All keys (vehicle cab, rear doors, king pin lock etc) should be removed from vehicles and locked in a secure key cabinet in an alarmed building. The cabinet should be securely fixed to a solid wall or within a floor-anchored safe with a nominal cash rating of at least £2,000. Where biometric key cabinets are used, these should be capable of signalling an alert if tampered with and/or be protected by monitored CCTV.



Lighting

There should be adequate continuous lighting outside of daylight hours to all external areas. This lighting should be of anti-vandal construction and external power cables should be protected within steel conduit. Maintenance procedures should be in place to ensure spent, damaged or faulty light bulbs are immediately replaced.

Security Manual

The site should have a Security Manual, which should be up-to-date, communicated to all relevant staff and evidenced as being adequately actioned. Such a Manual should show all procedures appropriate to the activities undertaken within the premises and in a form that permits easy reference by relevant personnel.This should include (where applicable):

- Site checks including premises perimeter fencing, lighting, anti-arson measures and locking up procedures.
- Authorised key-holder names and contact numbers, plus any other relevant emergency contact numbers/details.
- A logbook recording all security incidents and the subsequent response.
- Response to be given to signals received from Intruder Alarms and other systems such as access control or CCTV including, where appropriate, procedures for any “on-site” control room or alarm receiving centre.
- Use of access codes.
- Action to take in the event of faults to systems such as the Intruder Alarm or CCTV, including contact details for relevant fault repair companies.
- Criteria for selection of installers of intruder alarm systems and CCTV systems.
- Controls on issue, deletion and monitoring use of cards/fobs issued for use with any access control system.
- Checks that any vehicles and/or trailers left unattended on site are locked, with the keys placed within the key cabinet or safe.

For further advice please speak with your normal insurance advisor.