

SA HB 188:2021

STANDARDS
Australia



Handbook

Base-building physical security handbook — Terrorism and extreme violence

This is a preview. Click here to purchase the full publication.



SA HB 188:2021

This Australian Handbook was prepared by HB-188. It was approved on behalf of the Council of Standards Australia on 08 December 2021.

This Handbook was published on 17 December 2021.

This Handbook was issued in draft form for comment as DR SA HB 188:2020.

This is a preview. Click here to purchase the full publication.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

ISBN 978 1 76113 636 8

Handbook

Base-building physical security handbook

This is a preview. [Click here to purchase the full publication.](#)

extreme violence

First published as SA HB 188:2021.

© Standards Australia Limited 2021

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This document was prepared by Standards Australia Committee HB-188.

This document provides guidance on identifying and assessing relevant sources of building risk associated with threat sources (especially terrorism, civil commotion, and malicious damage) and implementing suitable controls to mitigate the likelihood and consequences related to these threat sources. This document is structured with the following sections which are based on the recommended risk management process described in AS ISO 31000:

- (a) Identification of physical threats.
- (b) Security risk assessment.
- (c) Risk treatment.
- (d) Testing, evaluation, monitoring and review.

This is a preview. Click here to purchase the full publication.

Contents

Preface	ii
Introduction	v
1 Scope and general	1
1.1 Scope	1
1.2 Application	2
1.3 Referenced documents	2
1.4 Terms and definitions	5
2 Identification of physical threats	10
2.1 Identification of threats	10
2.1.1 Threat concept	10
2.1.2 Threat identification	11
2.1.3 Threat environment – external inputs	12
2.2 Threat types – weapons and tactics	12
2.3 Arson	13
2.3.1 Overview	13
2.3.4 Common types of arson attack	14
2.3.5 Vulnerable areas in building design susceptible to arson	14
2.4 Hostile vehicle attack	14
2.4.1 Overview	14
2.4.2 History of hostile vehicle attacks	15
2.4.3 Hostile vehicle attack impacts	15
2.4.4 Common types of hostile vehicle attacks	15
2.4.5 Vulnerable areas in building design susceptible to hostile vehicle attacks	16
2.5 IED threats	16
2.5.1 Overview	16
2.5.2 History of IED attacks	17
2.5.3 Impact of IED attacks	17
2.5.4 Common types of tactics using IEDs	17
2.6 Chemical, biological and radiological (CBR) agent threats	19
2.6.1 Overview	19
2.6.2 History of CBR attacks	19
2.6.3 CBR attack impacts	20
2.6.4 Common types of CBR attacks	20
2.6.5 Vulnerable areas in building design susceptible to CBR attacks	21
2.7 Sabotage	22
2.7.1 Overview	22
2.7.2 History of sabotage attacks	22
2.7.3 Sabotage impacts	22
2.7.4 Common types of sabotage attacks	23
2.7.5 Vulnerable areas in building design susceptible to sabotage attacks	23
2.8 Cyber attacks	23
2.8.1 Overview	23
2.8.2 History of cyber attacks	24
2.8.3 Cyber-attack impacts	24
2.8.4 Common types of cyber-attacks	24
2.8.5 Vulnerable areas in building design susceptible to cyber-attacks	25
2.9 Armed attacks	25
2.9.1 Overview	25
2.9.2 History of armed attacks	25
2.9.3 Armed attack impacts	26
2.9.4 Common types of armed attack	26
2.9.5 Vulnerable areas in building design susceptible to armed attacks	26

This is a preview. Click here to purchase the full publication.

2.10	Violent protests.....	27
2.10.1	Overview.....	27
2.10.2	History of violent protests.....	27
2.10.3	Violent protest impacts.....	27
2.10.4	Common types of violent protests.....	28
2.10.5	Vulnerable areas in building design susceptible to violent protests	28
3	Security risk management.....	28
3.1	Security risk assessment.....	28
3.1.1	Overview.....	28
3.1.2	Risk assessment and tolerances	30
3.1.3	Stakeholders.....	30
3.1.4	Risk assessment methodology.....	31
3.1.5	Building security factors.....	32
3.2	Critical assets and functions.....	32
3.3	Vulnerability analysis.....	33
3.3.1	Overview.....	33
3.3.2	Vulnerability analysis — Measurement of security measures.....	33
3.4	Likelihood analysis.....	34
3.5	Consequence analysis.....	35
This is a preview. Click here to purchase the full publication.		
3.6	Risk ratings and documentation	38
4	Risk treatment.....	39
4.1	Risk treatment.....	39
4.1.1	Overview.....	39
4.1.2	Risk treatment strategies	40
4.1.3	Security-in-depth principles.....	40
4.2	Risk treatment in building design.....	41
4.2.1	Physical building controls.....	41
4.2.2	General architectural considerations in risk treatment.....	41
4.2.3	Higher risk areas and facilities	43
4.2.4	Security personnel and procedures.....	43
4.3	Controls in building design.....	44
4.3.1	Crime prevention through environmental design.....	44
4.3.2	Pedestrian perimeters.....	46
4.3.3	Vehicle perimeters.....	49
4.3.4	Access control.....	53
4.3.5	Security screening.....	56
4.3.6	Security lighting.....	58
4.3.7	IED attack protections.....	60
4.3.8	Armed attack protections.....	62
4.3.9	Fire risk prevention	65
4.3.10	Video surveillance systems.....	68
4.3.11	Controls for chemical, biological or radiological (CBR) attacks.....	70
4.3.12	Intrusion alarm detection.....	72
4.3.13	Keys and locks.....	75
4.3.14	Information and operational technology controls	77
5	Testing, evaluation, monitoring and review	79
5.1	Overview.....	79
5.2	Methods for testing and evaluation.....	80
5.3	Testing and evaluation — Responding to identified risks	80
5.4	Continuous evaluation and improvement.....	80
5.4.1	Evaluation, improvement and maintenance	80
5.4.2	Heightened threat level.....	81
	Bibliography.....	82

Introduction

This document responds to an identified need for guidance in managing risks of physical damage caused by deliberate acts of extreme violence to buildings, including commercial, industrial, and largescale residential strata property. This document provides an overview of relevant advice and best practices, intended to be read in conjunction with existing Standards, Federal Government advice and other applicable information. Many of these resources are referenced throughout this document.

This is a preview. [Click here to purchase the full publication.](#)

NOTES

This is a preview. Click here to purchase the full publication.

Handbook

Base-building physical security handbook — Terrorism and extreme violence

1 Scope and general

1.1 Scope

This document provides guidance on identifying and assessing relevant sources of building risk associated with threat sources (especially terrorism, civil commotion, and malicious damage) and implementing suitable controls to mitigate the likelihood and consequences related to these threat sources.

Its focus is on reducing the physical damage potential to buildings that may result from such acts, as well as mitigating the associated impact on building core functions. The adoption of this document would seek to reduce the costs and business interruption associated with extreme violence events, primarily through the targeted design of building infrastructure and other physical controls.

The this **This is a preview. Click here to purchase the full publication.** addressed in

- (a) Arson.
- (b) Hostile vehicle attacks.
- (c) Explosive attacks.
- (d) Chemical, biological, radiological (CBR) attacks.
- (e) Sabotage.
- (f) Cyber-attacks.
- (g) Armed attacks.
- (h) Violent protests.

These events generally involve considerable premeditation and planning and would be regarded as deliberate attacks. For the purposes of this document, deliberate attacks are distinguished from opportunistic attacks (such as unplanned assaults or thefts), which this document does not address in detail. Perpetrators of deliberate attacks will be referred to as 'offenders' throughout this document.

Further, this document —

- (i) has been prepared as a guidance document, and is not intended to prescribe compulsory building or security requirements;
- (ii) is not intended to provide detailed guidance on mitigation of harm to people or safety procedures in relation to violent acts; however, some physical building elements described in this document can protect occupants and bystanders;
- (iii) is not intended to specifically address malicious insider threat. Threats can originate from a malicious insider, who utilizes their credentials and/or knowledge to execute an attack. This can include current and past employees, as well as contractors. The impact of malicious insider-perpetrated attacks can be especially severe, given the potential for close and often unsupervised access to key functions and infrastructure;
- (iv) does not address any other organizational, societal, security or safety risk; and
- (v) is not intended to apply to Class 1 buildings as defined by the National Construction Code.

For security risks that are not addressed by this document, refer to SA HB 167.

1.2 Application

This document applies to public, private and not-for-profit organizations of any size that have a need for physical protective security of buildings. This document is particularly relevant to commercial, industrial, retail, and large residential strata properties.

This document is intended for use by base-building owners, operators and managers involved in, or responsible for, the process of risk mitigation of deliberate physical acts resulting in damage to buildings. The term 'building owner' will be used throughout this document to collectively describe all intended users. It seeks to encourage a proactive approach to risk management through the advance identification and assessment of threats. Ideally, the guidance in this document should be applied at the early stages of building conceptualization, informing the embedment of risk controls in the building's core design. However, the concepts raised remain highly applicable throughout the lifecycle of building management and should inform periodic testing and security reviews.

The purposes for which this document can be used include the following:

- (a) Building design phase
- (b) A

This is a preview. Click here to purchase the full publication.
- (c) Retrofitting, redesign, repurpose or renovation of buildings.
- (d) During regular risk reviews, involving the assessment of existing risk mitigation and identification of areas for corrective action.
- (e) As part of a larger risk management framework and to support the process of business decision making and analysis.
- (f) Planning of special events on premises.
- (g) As part of a larger reporting program for building security and safety.
- (h) As part of targeted risk and security culture and awareness programs, or larger resiliency programs.
- (i) To assess the relevance of emerging, newly identified or recently highlighted risks such as terrorism or acts of extreme violence.

1.3 Referenced documents

The following documents are referred to in the text.

NOTE Documents for further reading are listed in the Bibliography.

AS 1851, *Routine service of fire protection systems and equipment*

AS 4145, *Locksets (series)*

AS 4811, *Employment screening*

AS/NZS 2201, *Intruder alarm systems (series)*

AS/NZS 2343, *Bullet-resistant panels and elements*

AS/NZS 4421, *Guard and patrol security services*

AS ISO 22300, *Security and resilience — Vocabulary*

AS ISO 31000, *Risk management — Guidelines*

AS/NZS IEC 60839-11.1, *Alarm and electronic security systems, Part 11.1: Electronic access control systems - System and components requirements*

AS/NZS IEC 62676, *Video surveillance systems for use in security applications (series)*

SA HB 167, *Security risk management*

SA HB 328, *Mailroom security*

ISO 9000, *Quality management systems — Fundamentals and vocabulary*

ISO 14971, *Medical devices — Application of risk management to medical devices*

ISO 15544, *Petroleum and natural gas industries — Offshore production installations — Requirements and guidelines for emergency response*

ISO 22341, *Security and resilience — Protective security — Guidelines for crime prevention through environmental design*

ISO 22398, *Societal security — Guidelines for exercises*

ISO 22399, *Supply chain security — Guidelines for exercises*

ISO Guide 73, *Risk management — Vocabulary*

ISO/IEC 16085, *Systems and software engineering — Life cycle processes — Risk management*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary (series)*

ISO/IEC Guide 51, *Safety aspects — Guidelines for their inclusion in standards*

ISO/TR 22100-4, *Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*

ANSI/ASIS/RIMS RA.1-2015, *Risk Assessment*

BS 1722-10, *Fences, Part 10: Specification for anti-intruder fences in chain link and welded mesh*

BS 1722-12, *Fences, Part 12: Steel palisade fences — Manufacture and installation — Specification*

BS 1722-14, *Fences, Part 14: Specification for open mesh steel panel*

EN 1627, *Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification*

EN 50130-5, *Alarm systems, Part 5: Environmental test methods*

EN 50131-2-2, *Alarm systems — Intrusion and hold up systems, Part 2-2: Intrusion detectors — Passive infrared detectors*

EN 50131-2-3, *Alarm systems – Intrusion and hold up systems Part 2-3: Requirements for microwave detectors*

EN 50131-2-4, *Alarm systems – Intrusion and hold up systems Part 2-4: Requirements for combined passive infrared and microwave detectors*

EN 50131-2-5, *Alarm systems – Intrusion and hold up systems Part 2-5: Requirements for combined passive infrared and ultrasonic detectors*

IWA 14-1, *Vehicle security barriers — Part 1: Performance requirement, vehicle impact test method and performance rating*

IWA 14-2, *Vehicle security barriers — Part 2: Application*