RICS guidance note

RICS Professional Guidance, Global

Security

2nd edition

rics.org/guidance

Security

RICS guidance note, Global

2nd edition

Acknowledgments

RICS would like to thank the following for their contributions to this guidance note:

Lead authors

Gary Hellawell, Carillion (TPS)

Mark Whyte, Control Risks

Co-author

David Parkinson, Consultant

Editor

Alan D White, Consultant

Published by the Royal Institution of Chartered Surveyors (RICS)

Surveyor Court, Westwood Business Park, Coventry CV4 8JE, UK

www.ricsbooks.com

Produced by the Facilities Management Group of the Royal Institution of Chartered Surveyors.

ISBN 978 1 78321 060 2

Typeset in Great Britain by Graham Land Creative Limited.

Contents

RICS guidance notes

International standards

RICS is at the forefront of developing international standards, working in coalitions with organisations around the globe, acting in the public interest to raise standards and increase transparency within markets. International Property Measurement Standards (IPMS – ipmsc.org), International Construction Measurement Standards (ICMS), International Ethics Standards (IES) and others will be published and will be mandatory for RICS members. This guidance note links directly to and underpins these standards and RICS members are advised to make themselves aware of the international standards (see www.rics.org) and the overarching principles with which this guidance note complies. Members of RICS are uniquely placed in the market by being trained, qualified and regulated by working to international standards and complying with this guidance.

RICS guidance notes

This is a guidance note. Where recommendations are made for specific professional tasks, these are intended to represent 'best practice', i.e. recommendations which in the opinion of RICS meet a high standard of professional competence.

Although members are not required to follow the recommendations contained in the note, they should take into account the following points.

When an allegation of professional negligence is made against a surveyor, a court or tribunal may take account of the contents of any relevant guidance notes published by RICS in deciding whether or not the member had acted with reasonable competence.

In the opinion of RICS, a member conforming to the practices recommended in this note should have at least a partial defence to an allegation of negligence if they have followed those practices. However, members have the responsibility of deciding when it is inappropriate to follow the guidance.

It is for each member to decide on the appropriate procedure to follow in any professional task. However, where members do not comply with the practice recommended in this note, they should do so only for a good reason. In the event of a legal dispute, a court or tribunal may require them to explain why they decided not to adopt the recommended practice. Also, if members have not followed this guidance, and their actions are questioned in an RICS disciplinary case, they will be asked to explain the actions they did take and this may be taken into account by the Panel.

In addition, guidance notes are relevant to professional competence in that each member should be up to date and should have knowledge of guidance notes within a reasonable time of their coming into effect.

This guidance note is believed to reflect case law and legislation applicable at its date of publication. It is the member's responsibility to establish if any changes in case law or legislation after the publication date have an impact on the guidance or information in this document.

Document status defined

RICS produces a range of professional guidance and standards products. These have been defined in the table below. This document is a guidance note.

Type of document	Definition	Status
Standard		
International Standard	An international high level principle based standard developed in collaboration with other relevant bodies	Mandatory
Practice Statement		
RICS practice statement	Document that provides members with mandatory requirements under Rule 4 of the Rules of Conduct for members	Mandatory
Guidance		
RICS Code of Practice	Document approved by RICS, and endorsed by another professional body/ stakeholder that provides users with recommendations for accepted good practice as followed by conscientious practitioners	Mandatory or recommended good practice (will be confirmed in the document itself)
RICS Guidance Note (GN)	Document that provides users with recommendations for accepted good practice as followed by competent and conscientious practitioners	Recommended good practice
RICS Information Paper (IP)	Practice based information that provides users with the latest information and/or research	Information and/or explanatory commentary

1 Introduction

1.1 RICS and facilities management

This guidance provides information about the management of security issues and is one in a series for facilities managers giving practical assistance to the sector.

There is an increasing realisation that the efficient management of facilities enhances the operational performance of organisations. It follows that in defining service delivery each element of the service specification should align with operational requirements and be integrated through the business planning process with strategic objectives. This ensures an optimal contribution to business objectives.

A well defined security strategy is a key business enabler, supporting orderly operations and reducing potential risks to the organisation.

This guidance deals with the threat to the physical security of buildings and the occupants. Other aspects of security relating, for example, to financial crime and data theft will be addressed in future guidance or information papers relating to those specific issues.

1.2 The approach

The guidance provides facilities managers with practical information when considering the security needs of an organisation. It describes current best practice in the planning and supply of appropriate and effective security services.

The guidance is not designed to provide an absolute solution for every situation but will give an understanding of the need for security and the processes that support its operational application. This will assist facilities managers in identifying security issues relevant to their organisation and enable them to follow the appropriate course of action. Consultation with other relevant bodies may be necessary, including local government, national government and security consultants with the appropriate level of experience, before a decision is made.

The principles outlined in the guidance are applicable internationally, subject to an overlay of local operating practice and procedures.

1.3 Security

The design, construction and management of buildings will have an affect on an organisation's vulnerability to the diverse range of security threats, whether to its physical assets, intellectual property, data, staff or customers. Security measures applied sensibly and proportionately will provide tangible benefits, contributing to the bottom line of an organisation by creating resilience to the range of threats.

In consequence, there is now an accepted emphasis on integrating security into the design and management of an organisation's activities and operations. This requires a broad understanding of the issues and actions that need to be taken in order to create and maintain a secure and safe environment.

Furthermore, facilities managers should have a clear understanding of regulation, legislation and standards covering a wide range of security and resilience issues. They will be aware of employers' duties of care, corporate manslaughter legislation and the resultant requirements for operational risk strategies, which such legislation may require in particular regions.

1.4 The role of the facilities manager

As with most support services, facilities managers provide a focal point when determining the needs of the organisation for security and the capability to support new or revised security measures.

This will apply during the planning and detail design process for a new building and equally where existing systems are to be replaced or upgraded with an impact upon design, construction and management. It is essential that facilities managers are involved with the design team at all stages in the life cycle of a property so that the agreed solution is manageable, sustainable and flexible to operational change as the organisation responds to market movement and customer demands.

This approach will allow the appropriate level of investment to be allocated, risk-based decisions to be made about the approach, and security strategies to be applied at different stages of delivery.

Most organisations will focus on the protection of asset value and the cost of asset replacement. However, facilities managers should ensure with the operational management that there is an understanding of the site and the infrastructure that is required to support the organisation's activities and how any loss would impact upon current and future business activities. They will be in a position to advise on the need for security in these areas and as a consequence make a valuable contribution to security design, planning and delivery.

Effective security design and management depends upon an understanding of the organisation's business and operational needs. This will allow security to be designed, developed and managed in the context of the built environment and the ability of the infrastructure to support the technical security systems, physical measures and associated procedures. The process will be assessed and checked through the security risk management system, where the required level of security will be determined in the context of the organisation's attitude to risk.

The relationship between the facilities manager and the management structure of the organisation should allow information to be communicated to and understood by appropriate level managers within the organisation.

It is important that security is delivered on a consistent basis and that where measures are no longer compliant or fit for purpose, there is a process to initiate change. The facilities manager should be in a position to initiate this change and assist the risk and decision-taking process. In the same way, the facilities manager will be in position to oversee and comment upon the implementation of changes in security and how these may affect operations. There may also be an impact on the attitudes of employees and visitors who might feel adversely affected by changes in approach and the facilities manager will be in a position to comment accordingly.

The challenge for the facilities manager, together with the management team, is to create an environment and culture that is inclusive and communicates information to aid the understanding of all stakeholders.

The systems and processes should recognise the positioning of stakeholders in the decision-making process and in this way engender ownership of the security planning process through the management team and across the wider organisation.

1.5 Security plans

Security planning is an ongoing management activity that requires regular review to ensure that it remains relevant to the threat and changes in the use of buildings and operations. The facilities manager should recognise the changes in building management that may initiate the need for a review in security and will be in a position to advise the organisation about operational vulnerabilities, together with what aspects of security need to be reviewed.

The extent of reviews will be influenced by the level of change affecting the organisation but the entire security profile should be examined periodically to ensure that standards are maintained and systems are fit for purpose. Periods between reviews can be based on the importance of the site and the operations it supports and be prioritised accordingly.

Security plans should be included in the business operational planning and management process and be continuously monitored and reviewed. Good practice dictates that security plans should be reviewed at least on an annual basis.

Ownership of the security plans should be defined as part of this process and should be placed at the most appropriate level of the organisation depending upon the potential risk to business. This could mean that a main board director has the key responsibility, but wherever the responsibility lies, it is essential to identify the individual and thus define ownership as well as operational and reporting responsibilities.

2 Development of a security strategy

2.1 Key business drivers

Security strategy will be driven by the business needs of an organisation and will, therefore, be an essential aspect of the business planning cycle, particularly relating to risk and budget.

It is important to ensure that the security strategy is proportionate to the organisation's needs and operation. An over-emphasis on security will be costly and perhaps adversely influence the perceptions and attitudes of customers, clients and employees and might negatively impact on the effectiveness of the organisation's operations.

In order to ensure that there is no ambiguity or uncertainty, the strategy should clearly communicate the organisation's culture and approach to security. The culture will reflect organisational practices and allow all parties to understand that security requires good communication routes through the business, with an opportunity for engagement and consultation. This should be driven by the senior management team with support throughout the management structure.

The security strategy should be agreed and signed-off at the most appropriate level in the organisation, ensuring that all risks, as well as the risk of non-compliance, are clearly understood. The service delivery can then be managed against measurable outputs, focusing on the business plan of the organisation.

Regardless of the technologies and processes that an organisation may adopt, it is important to consider how the security strategy complements its needs and sector requirements in terms of regulatory expectations. It is clear that those engaged in the leisure industry, for example, will need to adopt a low profile but effective security strategy that protects their assets from a number of diverse threats but does not adversely affect the experience of their customers.

In the financial services sector, the potential impact of the loss of data and information will be of great concern. Strategies will be influenced by the operational requirements of the regulatory bodies, which call for a risk-based and demonstrable approach to security. Equally, ISO 27001 accreditation may be considered an imperative in the secure management of information systems and the strategy will reflect this requirement. Organisations engaged with government contracts will be required to adopt a strategy that reflects the standards specified to protect government assets in their particular region of operational activity.

Although it is advisable for a risk-based approach to be considered when developing the strategy, this should be done in the context of these predetermined standards that may be defined and imposed upon the organisation by a third party.

Risks can be categorised in various ways but they are most commonly defined as those threats that, should they materialise, have the potential to cause loss to the organisation. Typically, they can be considered under the headings of:

- general acquisitive crime
- terrorism
- low level criminality and criminal damage
- anti-social behaviour; and
- protest and disorder.

Within many organisations, natural threats such as flooding may also be considered. These risks can further be considered in relation to their impact upon the organisation's employees and physical assets, the ability to maintain continuity of business and the ability to meet statutory and contractual liabilities.

2.2 Principles of a security strategy

The security strategy should reflect the organisation's needs and be cost effective and sufficiently robust to counter the perceived threats. A considered process of planning and consultation will ensure that security is proportionate and that unnecessarily restrictive measures are discarded. The strategy ensures that security reflects the organisation's profile and culture while remaining compliant with regulatory requirements.

The ability to integrate the full range of measures, though not always possible, promotes a strategy of defence in depth. The individual measures serve to provide a specific form of protection to defeat a threat; however, where they overlap they are more likely to defeat a wider range of threats from the more determined attack.

This approach serves to support the following principles:

- *Deterrence* – The effect of security on an adversary's decision making process.
- *Detection* – The ability to identify and monitor an attack.
- *Delay* – Time taken for an adversary to counter security measures to access an asset of value and ability to respond.
- *Detention* – The ability to respond to an adversary and detain them before escape.

These principles are not exclusive and others could be equally valid, but they reflect the main issues in applying security in the built environment and across organisations.

2.3 Proportionality

It is advisable to ensure that security reflects not only the potential threats that an organisation may face but also the attitudes to risk, while taking into consideration the issues of image, reputation and customer/client expectations. This will allow security measures, physical or procedural, to be applied in a manner that is proportionate to the organisation and the protection of assets.

Failure to address security in the context of the level of protection it offers can result in unnecessary expenditure and the possibility of creating an oppressive environment.

2.4 Integration and coordination

The integration of security measures will ensure that diverse threats are mitigated by an interlocking series of measures that provide defence in depth and a layered approach. It is advisable to coordinate security procedures, ensuring that there is an effective response to the security alarms, incidents and compromises in order to reduce the probability of a successful attack and increase the probability of detection, so reducing the loss or compromise of assets. It is worth considering engagement with other organisations – police authorities and security agencies – to ensure that security is effectively coordinated and integrated with local initiatives.

Security issues should integrate with other management activities including the organisation's operational, strategic and investment planning to ensure that it is considered at the appropriate level and included as part of the wider management processes and decision-taking.

3 Planning process

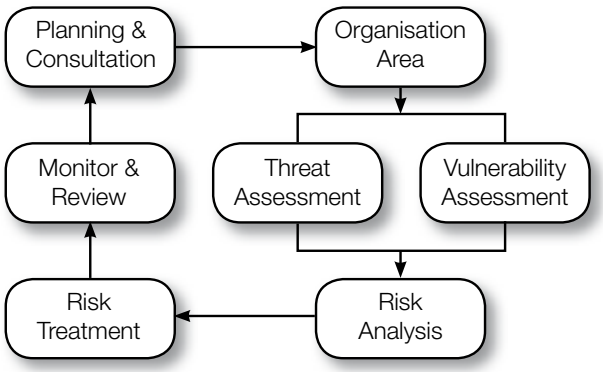
Security planning requires an understanding of not only the threat but also how it might affect the organisation from a financial and operational perspective. The challenge in the planning process is the ability to integrate physical and procedural security measures with cultural and business expectations in terms of the working environment and aesthetic appeal, as well as remaining compliant with the appropriate standards.

With current threats and the changing risk environment, as well as the possibility of regulatory sanction, the previously held inclination towards risk acceptance or feigned ignorance of security issues is not appropriate. As a consequence, it is universally accepted that security will be included in the planning of new projects and in the management of existing facilities.

This requires the cooperation and coordination of the designer and planning team with facilities managers and security experts, resulting in physical, procedural and electronic security measures being much less obtrusive than in the past and early dialogue will identify the most effective and acceptable solutions.

It is this position at the centre of the organisation and understanding of the operational and organisation requirements that can allow facilities managers to drive the security planning process and champion a consistent approach. Figure 1 highlights the circular nature of security planning and the need for a clear understanding of the organisation, its operation, the threat and aspects of risk.

Figure 1: The planning cycle



3.1 Organisation characterisation

The nature of the organisation and the sector in which it operates will define the potential threats, the attitude and approach to security and the way it should be delivered. It will also identify the need to comply with regulatory requirements and ensure that organisational and operational imperatives are addressed. The facilities manager is well placed to assess how security might impact upon day-to-day operations and the ability of the infrastructure to support security solutions. Whatever the sector or company, however, it may be helpful to adopt a common and scalable approach to the identification and management of risk with the steps described in sections 3.2 to 3.7.

3.2 Threat assessment

The foundation upon which to formulate the security strategy and establish the most suitable approach is to assess the type and extent of potential threats. This will provide an indication of the level of security required.

3.3 Vulnerability assessment

An assessment of the existing security measures, through surveys, should determine the vulnerability to the threats that have been identified. This will provide an indication of the extent to which security measures already mitigate the threat.

3.4 Risk analysis

Analysis of the potential threats and risks will provide an indication of the strategies required to manage the risk, based upon the probability and impact of the threat materialising.

3.5 Risk management

Risk management is concerned with the assessment and prioritisation of risks to reduce the probability of incidents and minimise impact. A risk managed approach to security implies a detailed understanding of the risks faced and the application of proportionate and appropriate mitigation measures. This is in contrast to the blanket application of standard security measures with no consideration of local context.

3.6 Management and monitoring

Security issues should be managed and reviewed through a process of audits, inspections and reviews (see Appendix B).

3.7 Planning and consultation

Any changes that may arise as a result of changes in the threats to an organisation will require key stakeholders to be consulted. This will initiate the other aspects of the process that should be considered as part of security planning.

3.8 The design process

A formal design process provides a structure for planning and designing security measures in the context of a construction project. As an example, Figure 2 shows the Royal Institute of British Architects (RIBA) design process with security planning stages mapped against the key architectural, design and construction stages of a project, aligning key activities to ensure a consistent approach.

3.9 Security standards

The design of security systems and the quality will depend upon the standards demanded. Specific sectors and particularly those working to, or in support of government, will be required to meet pre-determined standards in the area of physical and technical security systems. They will have been assessed against particular threats and the ability to resist forcible and surreptitious attack.

These standards will establish the key design and installation features and determine the performance criteria they should be able to meet.

It is important to check whether an organisation is required to work to security standards when planning the security strategy. Appendix C provides a list of some of the standards that are applied to security systems but is not exhaustive and may be subject to change as the standards listed are reviewed.

Figure 2: Security integration with the RIBA Stages

Preparation	0	Strategic Definition	Threat and Risk Assessment Liaison and co-ordination with Counter-terrorism Security Advisors (CTSA's) and Architectural Liaison Officer (ALOs)
	1	Preparation and brief	Assessment Coordination with architects and structural engineers, and other design team members
Design	2	Concept design	Security Concept agreed Physical, Technical, Procedural
	3	Developed Design	Physical and technical security performance specification, drawings and budgetary figures, Developed coordinated security design
	4	Technical Design	Revised budgetary figures, statutory approvals, construction information, Produce tender fit documentation
Construction	5	Construction	Trade contractor list produced, Invitations to tender (ITT) issued, Requests for information (RFIS) evaluation and recommend contract award, Mobilisation
	6	Handover and Close Out	Design consultancy, snagging, witnessing and commissioning
Use	7	In Use	Rolling performance standards for systems

4 Sourcing

4.1 Introduction

Following the development of the security strategy, it is important to develop a sourcing strategy that supports the key outputs in accordance with the needs of the organisation and is geared towards delivering a value for money solution.

As defined by the security strategy, it is advisable that the sourcing strategy has the necessary flexibility to enable changes to be made as the demand changes in response to potential threats. It is important, therefore, for the sourcing strategy to be agreed with the organisation and signed off at the highest appropriate level, with subsequent reviews treated similarly.

It is essential to clearly communicate and manage all risks at an early stage as part of an ongoing risk management process aligned to the business risk management profile of the organisation.

The sourcing strategy should be developed in accordance with good supply chain practice and include an assessment of the degree of importance of the individual elements of the security strategy, balanced against the availability of potential suppliers in the marketplace.

The development of a security related sourcing strategy may be very simple, for example manned guarding, or very complex where issues such as national security and potential terrorism threats are involved. It is worth considering at the outset whether or not the skills for the development of such a strategy exist in-house or need to be outsourced to a specialist security consultant. Whatever course of action is chosen, the security and sourcing strategy must define the key responsibilities and the ultimate ownership of those responsibilities.

4.2 Procurement of services

Procurement is a core element of the facilities manager's remit and follows the development of the sourcing strategy discussed in section 4.1. The selection, planning and implementation of procurement activities constitute the basis of good financial management and value driven operation. Any effective procurement exercise is based on an understanding of the strategic considerations supported by proper analysis and risk management processes.

The following should be considered as a minimum:

- the specialist nature of the elements under consideration and the degree of technical competence required
- the potential damage caused by the failure of any of the elements
- the maturity of the market in delivering the services, either individually or collectively, and
- the availability and capacity of the market to deliver.

It is advisable for the sourcing strategy to define:

- those elements of the security strategy which are of such a specialist nature or technical difficulty that they have to be procured on an individual basis
- those elements which can be bundled as part of a generic facilities management package
- those elements that will need to be retained in-house
- the high level output requirements to be included in contract documentation; and
- any associated risks in defining the strategy.

It is helpful to create a framework of contracts and specifications to define the input and output requirements, and in addition, a process document that defines the inter-relationship of those contracts and the management processes that are in place, in order that all stakeholders are aware of their individual and collective responsibilities.

Facilities managers are recommended to brief themselves and all management staff with regard to any formal guidance tools and services that are available in setting efficiency standards, by outlining procurement principles and providing simple solutions to common issues.

4.3 Contract administration

A key function of the facilities manager is contract administration (including financial management) according to pre-agreed key performance indicators (KPIs) and service level agreements (SLAs) agreed with the organisation servicing the contract, whether internally or externally sourced. When entering into a new contract, it is recommended that facilities managers are instrumental in defining contract terms and conditions, ensuring that they align with the strategies that have been agreed previously with the organisation.

When taking over an existing contract, facilities managers are advised to carry out a review. Senior managers should be made aware of any risks that exist and recommendations should be made as to how those risks might be managed.

4.4 Benchmarking and reporting

Benchmarking is a means of comparing a product, service process or any activity with other examples from a peer group, with the intention of identifying best practice (or a best buy) and delivering services accordingly.

The process of benchmarking is concerned with obtaining performance and value and meeting customer requirements, as well as reducing costs.

Facilities managers have a major role to play in the benchmarking process and in the financial control and reporting processes.

Project financial control and reporting is essential in order to ensure that the agreed financial management plan is achieved, with the element of reporting being regarded as a mechanism for periodic control. This is deemed to be best practice financial management.

Facilities managers are advised to familiarise themselves with the requirements of the organisation's budget planning process, and to ensure that reporting is carried out periodically and regularly in support of the budget and business planning process.

5 Security operations

5.1 Skill and competency recommendations

The facilities management professional should have the skills and competencies necessary to understand the nature of the security threats to a facility, to understand sources of vulnerability and the issues of impact and probability in determining risk. In addition, skills are required to enable the planning and execution of a comprehensive and integrated facility security programme, with support from other professionally qualified security specialists, such as systems designers, when required.

5.2 Integrated security solutions

It is unlikely that a building or organisation will be subjected to a unique threat that will require a single security solution and it is often necessary to consider the integration of physical security measures with other technical and procedural solutions. This will establish layers of physical, technical and procedural measures that will interlock and provide a defence in depth. Management procedures should ensure that changes in threat and risk are tracked and any new counter measures developed.

5.2.1 Design

Each element of security should be subject to close planning in order to achieve the optimum effect and meet operational requirements. The facilities manager is ideally placed to comment on the potential impact of the security scheme on the management of buildings. The manager will advise on the capability and capacity to support the different systems and in conjunction with systems designers, contribute to the development of performance criteria and overall specifications.

The following issues should be discussed by the facilities manager with a variety of operational managers and the feedback will have an impact on design:

- the threat to be overcome (facilities manager, operations managers and security adviser)
- the level of risk to be mitigated (operations managers, facilities manager and security adviser)
- investment available (business and facilities manager)
- operational requirement and the role of the security systems (facilities manager and security adviser)
- performance criteria (facilities manager and security adviser)
- systems specifications (security adviser)
- tender process (business, facilities manager and security adviser)
- system acceptance (facilities manager and security adviser); and
- operational management (facilities manager and security adviser).

5.2.2 Physical security solutions

Physical security solutions provide a level of deterrence to a threat and provide physical barriers to delay and defeat physical attack. The design of buildings will determine the resilience level to the more obvious threat such as terrorism and improvised explosive devices (IEDs) in their different forms, but will also influence approaches to issues such as control of access and the protection of the organisation's critical assets.

The perceived level of threat will determine the level of robustness and standards that should be applied. Such standards reflect the resilience of security measures to predetermined attack options measured by the amount of delay they offer. Recognising these factors in the planning process is one way to ensure the selected system is sufficiently robust and that unnecessary expense is not incurred through over-specification.

Physical security solutions include:

- perimeter security, e.g. fences, gates, barriers, taking into consideration materials and height
- fabric of the building, e.g. structural design
- doors, e.g. security and fire doors, including hinges and door frames, and secure rooms
- windows for crime reduction and blast resilience
- locks for resilience to surreptitious and physical attack; and
- document and data storage containers for resilience to surreptitious and physical attack.

The quality and standard of physical security measures is often sufficient to deter lesser threats, while at the same time creating a delay and possibly defeating a more determined attack. They will also provide a level of detection in identifying where an attack has been attempted and provide the prompt for a follow-up investigation. A key aspect of physical security is that it either directly supports and provides a platform for a technical solution or creates the environment where technical solutions can be deployed. It also provides the infrastructure and controlled environment within which procedural counter measures, such as patrols, checks and searches can be conducted.

5.2.3 Technical solutions

Technical solutions provide the ability to monitor assets, detect unauthorised access, or identify and record suspicious activity. They will deter lesser threats but also provide the basis for a response to a more determined attack. Where systems are integrated with building management and IT based operations, they can also be used as an audit trail for subsequent investigations and internal disciplinary action.

Technical solutions include:

- CCTV – internal and external including cameras, transmission links, processing, monitoring and recording
- perimeter intruder detection systems (PIDS) – fence mounted or sub-surface
- intruder detection systems (IDS) including sensors, alarms and monitoring
- search equipment – personal, parcel or vehicle; and
- automated access control systems (AACS) – PIN, proximity or biometric readers supported by passes and identity cards.

Systems should be developed in a manner that reflects an ability to meet specific organisational needs, perform in accordance with agreed criteria and be installed in accordance with the appropriate standard. Sustainability and maintenance of the systems is a key factor and it may be helpful to consider the repair and replacement of equipment as part of the procurement process.

5.2.4 Procedural solutions

Procedural solutions aim to deter a threat by increasing the probability of detection and, where possible, should also be integrated with physical and technical solutions to ensure they are practical and are mutually supportive. They may include searches, checks, surveys and inspections, and actions to be taken in the event of an attack and are often supplied through contracts and specific assignment instructions linked to key performance indicators.

Inevitably, there is a focus on the services provided by manned guarding and security patrols that will either simply monitor security systems or initiate and provide a response.

Where the organisation requires checks to be conducted, it is advisable to have the procedures in place that ensure that personnel have been cleared to the appropriate level before being given access. This is particularly relevant in the government sector but is also appropriate for the financial services and data protection sectors. It is important for the management of staff in these areas to have an interface with other management functions, in particular human resources, so that any changes to personal circumstances that affect security and access can be managed.

5.2.5 Employee participation and business culture

Employees invariably have an understanding of the organisation and can identify either aspects of the organisation or the supporting infrastructure that may be vulnerable. It can prove valuable to encourage employees to participate in the development of the security strategy and to give them the means of communicating their observations to the appropriate level of management, especially where a threat could come from persons employed or contracted by the organisation.

This can only be achieved by developing a security culture that makes them feel part of the solution and not the problem. Employees who are well informed and understand the potential impact on the organisation of an incident are more likely to be receptive to the adoption of new security measures.

Equally, a negative attitude will undermine security and create a vulnerability that could be exploited. A positive approach to security measures will be assisted by:

- positive leadership from management
- education and training
- notices and information
- tool box talks
- management openness and approachability through confidential systems; and
- recognition of positive contributions.

It is possible that some organisations do not wish to have overt security measures imposed upon employees and clients, believing that it may undermine the workplace culture. This creates difficulties and areas of potential conflict where recommended solutions are contrary to the culture of the organisation and require a degree of negotiation between interested parties and stakeholders. If an acceptable solution cannot be found, it is advisable to record the resulting risks and manage accordingly.

5.2.6 Counter-terrorism measures

Counter-terrorism measures (CTM) aim to limit damage to the building fabric and injury to the occupants when an explosive device is detonated. The need has been graphically illustrated by terrorist events worldwide, where the extent of damage and injury has sometimes been out of all proportion to the size of the explosive event, primarily because of the form of building construction employed. It should be stressed that there is an essential need for a measured assessment of each particular case based on its own qualities and requirements. Each case will invariably differ according to its location, the assessed threat it is deemed to face, and its relative and absolute security risk profile.

There are numerous ways to develop a CTM strategy, which will often include at least some of the measures and systems discussed above. In summary, the following reflect the key features that the facilities manager should be aware of and apply:

- physical security measures to deter and prevent attack
- provision of stand-off distances
- disguising, dispersal and/or duplication of essential facilities
- blast resistant glazing
- bomb shelter areas and escape routes
- public address systems
- avoidance of locations where a device might be concealed; and
- making safe and ease of repair.

Advice is available to all organisations through government, police and security agencies and there are a variety of organisations and individuals who can contribute to the development of CTM security measures and design, and sources of advice can be found in Appendix C.

If the site is regarded as belonging within the critical national infrastructure, then the Centre for the Protection of National Infrastructure (CPNI) can provide more detailed expertise about managing the particular security threats to the site. CPNI are also responsible for testing vehicle security barriers and other counter-intruder devices. They work closely with the Home Office Scientific Development Branch (HOSDB). In addition, there are some multidisciplinary design consultancies that can provide a one-stop shop for commercial security advice, risk assessment, explosion effects analysis and systems design to work with the architect and designers throughout all stages of a project.

5.3 Operational security issues

5.3.1 Security threat and risk assessments

Security risk management is an ongoing process that allows an organisation to understand its exposure to risk and make intelligence-led decisions. This requires a clear understanding of all the components of risk and how they will impact upon an organisation's activities, their operations and ability to comply with legal and regulatory requirements.

An adversary's capability and intent, and the ability to exploit vulnerabilities, can be determined by developing an appreciation of the organisation's security environment. The probability of an incident occurring and the impact upon operations will determine the level of risk and provide a basis for security planning and design.

5.3.2 Threat

The threat assessment is a judgment based upon available intelligence that provides an indication of the events that may affect an organisation and its assets. The information can be accessed from official government departments, historical records and open source research, and can address a range of activities. This intelligence will assist in determining the capability and intent of the threat and its probability, based upon the value of the asset, its usefulness in achieving an adversary's goals, publicity value, availability and ease of targets, and the adversary's perception of the possibility of a successful attack.

The range of threats is diverse and will impact upon different areas of the organisation. Consequently, it is necessary to understand and characterise the organisation in the context of its vulnerability to attack.

5.3.3 Understanding vulnerability

Vulnerability is the level of weakness within an organisation's existing physical security measures and procedures that would provide an opportunity for a successful attack. It is therefore important to understand and quantify the existing security measures, and be able to assess their effectiveness in mitigating the threat. It is advisable to address the effectiveness of these measures and their level of compliance with the appropriate standards during the survey of sites.

5.3.4 Asset identification and value

It is possible to categorise organisational assets in terms of the tangible and intangible and these can be determined in the context of people, property, real estate and other physical assets; and also an organisation's information and data, whether in hard copy or contained within electronic information systems. It is also worth considering the impact upon intangible assets such as reputation and market position. The value of an asset in terms of loss depends on its importance to continued operations, the cost of physical replacement and the impact of loss to the organisation. It is advisable to consider the impact of aggregation and ensure that those low value assets, where found in high volume, if lost, do not have a significant impact upon the organisation. This principle applies to all types of assets and may influence the level of protection provided over and above that normally anticipated.

5.3.5 Assessing impact and probability

Impact and probability determine the level of security risk faced by an organisation from a specific threat, which allows the approach to its management to be considered. A scoring system can be devised using either qualitative or quantitative approaches, depending upon the availability of the appropriate information. As an example, a graduated scale of five stages can be used for both elements, which allows the risk to be addressed across a range of mitigating measures. The five stages relate to impact which could be from 'Catastrophic' (5), down to 'Minor' (1). Probability is considered from 'Almost certain' (5) to 'Unlikely' (1). These options are examined in 5.3.10.

This approach allows the equation *Probability* × *Impact* = *Pure risk* to be populated, which provides an indication of the level of risk and an indication of the level of management action required to address the risk.

5.3.6 Impact

The impact of a threat gives an indication of the cost and operational effect of an adverse event coming to fruition against an organisation. It can be helpful to determine impact by applying a monetary value to either replacing the asset, cost of lost production or of reducing the risk to an acceptable level. It may be more difficult to assess a value for intangible assets such as reputation, but it is worth considering that there remains a potential financial impact. By understanding the impact, the decision-making process is supported by providing an indication of the level of investment required to provide cost effective mitigation.

5.3.7 Probability

Assessing probability is the process of looking at how likely a risk event or condition is to occur. Various methods can be used, such as looking at the frequency with which incidents have occurred in the past, as well as local and regional trends, and by the availability of intelligence suggesting the probability of a threat materialising. Threats against similar organisations across a sector can also help provide an indication of probability. However, it is advisable to assess this in the context of local and regional influences and the commercial and political profile of those organisations.

The probability of the identified threat occurring is a function of the identified threat level (including capability and intent) through the threat's perception of an organisation's attractiveness as a target. This is based primarily on the value of the organisation's assets in the context of the threat's agenda. However, a secondary influence on the assessment of attractiveness relates to the probability of success and this is inextricably linked with the perceived vulnerability of the site.

Although some threats, such as criminality, are well recorded and can be assessed on the basis of occurrence, acts of terrorism are less predictable and their probability could change at relatively short notice. This will require flexibility in approach and careful consideration of contingency planning and emergency response as part of security planning.

5.3.8 Risk mitigation

Mitigation measures can be either probability or impact based, though there may well be an overlap between these. Probability mitigation measures address the threat and target, and methods of reducing the likelihood of an attack on an organisation and particular assets. This can be achieved by using 'soft' measures, such as policy changes, changes in procedures and by addressing the cultural approach within the organisation. Alternatively, they may take the form of 'hard' technical and/or physical measures, such as enhancing CCTV coverage, improving counter-terrorist measures or improving perimeter security. These measures essentially aim to reduce the chances of an event occurring.

Impact mitigation measures aim to reduce the consequences to an organisation in the event of a manifest threat. While physical mitigation measures may play a part in this respect, it can be valuable to focus on providing over-capacity in the organisation so that production or operations can continue in the event of an incident. It is advisable to use risk management techniques to inform organisation continuity plans, which can then feed back into a cycle that can be revisited as new threats emerge due to internal and/or external factors.

It is advisable to carry out a secondary risk assessment after mitigation measures have been implemented and when both the probability and impact might have been reduced, bringing the overall risk to a more manageable level. It can then be valuable to provide a more sophisticated assessment of risk reduction by apportioning various mitigation measures a quantitative score related to their perceived protective capacities which is fed into a matrix (see Figure 4). The risk assessment can then be used to provide the basis upon which security measures will be designed to mitigate the risk.

It is advisable to use this in order to assist the decision-making process in adopting the appropriate strategies, and influence the level of investment required.

It is worth considering the following options:

- enhance physical security and procedures
- focus on contingency planning
- increase organisation continuity planning; and
- transfer risk through insurance.

5.3.9 Qualitative versus quantitative approaches

Essentially, probability comes down to either a priori probability (pure mathematical probability such as flipping a coin) or statistical probability (such as the incidence of male versus female births), which is calculated on the basis of empirical evidence. As previously discussed, while data does exist on criminality and terrorism, mathematical calculation remains a difficult proposition and, therefore, judgments on probability will invariably contain a high degree of subjectivity. The more knowledge that is available about the threats, however, the more credible that judgment is likely to be.

When expressing levels of probability and impact, qualitative and quantitative statements are often used and these are expanded below. Whichever method is selected, it is important to understand the basis of the assessment.

Table 1: Quantitative statements of impact and probability: impact

Impact	Probability
Very high	Multiple deaths or total loss of operations/facilities. Catastrophic financial loss. Irreversible loss of market position.
High	Multiple severe injuries or loss of key operations/facilities. Significant financial loss with medium to long-term impact. Significant loss of reputation.
Medium	Multiple minor injuries, replacement costs with medium-term adverse publicity.
Low	Few minor injuries, minor loss of operations/facilities. No significant financial impact or adverse publicity.

See Figure 3 for a demonstration of how statements can express the likelihood of an event occurring against a specific threat, in this case terrorism.

Impact	Probability
Very high (75–100%)	There is intelligence indicating that the project has been specifically targeted by a group known to have the capability to conduct operations.
High (40–74%)	Attacks have been carried out in the region on a regular but infrequent basis. Projects with similar assets and facilities have been targeted.
Medium (10–39%)	There is a generic threat from attack but they are infrequent and not target specific.
Low (1–9%)	There have been few or no instances of attack.

Tables 2 and 3 similarly allow qualitative statements to reflect a scoring system and position in the risk matrix.

Table 2: Qualitative probability scoring statements

Almost certain	Current intelligence indicates that an event is imminent and targeted specifically against the organisation. Similar organisations in the area and across the sector have been attacked on a regular basis.
Likely	There have been incidents against similar organisations and/or the organisation has experienced similar attacks frequently in the past. It is believed that this organisation is of interest to individuals or organisations who may wish to conduct attacks for their personal/political objectives.
Possible	There is a generic threat to the sector but the organisation has not been specifically targeted. Incidents have taken place but are infrequent.
Rare	There is no indication that the organisation is subject to this form of threat and where they have occurred they are not target specific.
Unlikely	No known threat to the organisation and any incidents have been rare and not specific to this sector.

Table 3: Example of a risk square based on monetary value

Catastrophic	Organisation's continued operation is threatened, catastrophic financial loss, irreversible loss of market position. Major loss of life and injuries.
Major	Serious damage to the organisation and loss of market position. Serious financial and reputation loss. There will be loss of life and a number of casualties.
Significant	Damage to the organisation with some investment required to replace operation over short to medium-term. Adverse impact on reputation. There may be some loss of life and probably casualties.
Insignificant	Some financial impact with minor impact on organisation's operations. Possibly some casualties.
Minor	No operational impact and negligible financial implication.

Both qualitative and quantitative approaches to assessing risks will produce results that can be plotted on a simple risk square as shown in Figure 3.

5.3.10 Risk matrix

The use of a risk matrix allows risk to be categorised within predetermined parameters that will determine where they sit in relation to other risks and how they should be managed in the context of 'High', 'Medium' and 'Low' risks. It is advisable that this categorisation reflects an organisation's risk strategy and the approach to the subsequent management. Figure 3 shows a typical example of a risk matrix.

Figure 3: Risk matrix

PROBABILITY	Almost certain	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
	Likely	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH
	Possible	LOW	MEDIUM	MEDIUM	MEDIUM	HIGH
	Rare	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
	Unlikely	LOW	LOW	LOW	MEDIUM	MEDIUM
		Minor	Insignificant	Significant	Major	Catastrophic
	IMPACT					

Figure 4: Example of a risk management matrix

RISK REF	ASSET	LOCATION	THREAT	PROBABILITY	IMPACT						RISK	MITIGATION MEASURES			RESIDUAL RISK (following application of E, E or AM mitigation measures)			RISK OWNER
					DENIAL OF SERVICE	LOSS OF REPUTATION	LOSS OF LIFE	FINANCIAL LOSS				ESSENTIAL (E)	DESIRABLE (D)	ADDITIONAL MEASURES (AM)	ESSENTIAL	DESIRABLE	ADDITIONAL MEASURES	
Gen 1	London Head Office	Canary Wharf	Terrorism	Likely	Major	Major	Major	Major			H	HVMM Security Doors, Turnstiles, Locks EACS, IDS, Guards, Postal Scanners, Hand Searches CCTV, Policies, Training	Hand Held FX Search Equipment, Archway FX Detection Equipment	Video Verification on ACS, Crime/ Security Analyst, Integrated C³I Facility	M	M-L	L	
Gen 2			People Crime	Possible	Significant	Significant	Significant	Minor			M	Security Doors, Turnstiles, Locks EACS, IDS, Guards, Hand Searches, CCTV, Policies, Training	Staff Lockers, Cashless Vending, Staff & Contractor Vetting	Crime/Security Analyst, Lone Worker Protection C³I Facility	L	MIN	MIN	
Gen 3			Property Crime	Likely	Significant	Minor	Minor	Minor			M	Security Doors, Turnstiles, Locks EACS, IDS, Guards, Hand Searches, CCTV, Policies, Training	Property Marking (DNA Tags) Register	Smartwater, Smokecloak, RFID Tagging Integrated C³I Facility	L	MIN	MIN	
Gen 4			Environment	Possible	Significant	Minor	Minor	Minor			M	CCTV, Policies, Training, Continuity & Resilience Coordination & Plans		Integrated C³I Facility	L	MIN	MIN	
Gen 5			Single issue	Possible	Significant	Significant	Significant	Significant			M	Security Doors, Turnstiles, Locks EACS, IDS, Guards, Hand Searches, CCTV, Policies, Training	Intelligence Screening Staff & Contractor Vetting	Crime/Security Analyst Integrated C³I Facility	L	MIN	MIN	
Gen 6			CBRN	Unlikely	Major	Major	Major	Major			M	Security Doors, Turnstiles, Locks EACS, IDS, Guards, Hand Searches, CCTV, Policies, Training	Air Filtration	Air Sampling/ Detection Integrated C³I Facility	M-L	L	MIN	
Gen 7			Disorder	Possible	Significant	Minor	Minor	Minor			M	Security Doors, Turnstiles, Locks EACS, IDS, Guards, Hand Searches, CCTV, Policies, Training	Intelligence & Coordination	Crime/Security Analyst Integrated C³I Facility	L	MIN	MIN	

6 Continuous improvement

The continuous improvement process is driven from a number of areas of activity but principally from the need to continually innovate in the delivery of facilities management services, and the strategic changes driven by the business needs of the organisation.

The facilities manager, in providing advice to an organisation, must have either personal knowledge or access to specific and relevant market knowledge of security and security service provision, and be able to utilise that knowledge in a way that meets the demands of the business planning process and mitigating risk, as appropriate.

At each review stage, it is advisable to question the relevance of service provision against contemporary standards to ensure that service provision is at all times appropriate.

It is recommended that the facilities manager investigates developing risks in the market place that might influence the security planning process. Such risks can be specific to the industry or environment or more generic in nature such as the ever-changing threat posed by terrorist activities, which might not affect the client directly but could have an impact indirectly in terms of distribution, utility supplies, etc.

In this context and in considering the provision of security services, it may be helpful for the facilities manager to make reference to:

- technical innovation – including technology development supported by IT and its relationship to the service delivery process
- process innovation – including new methods of working, analysis and rectification; and
- organisational innovation – including contractual methodologies and people development.

This is one way of ensuring that the facilities manager is confident that risks are properly identified and that methodologies are in place to manage those risks with an appropriate balance between risk and cost.

Appendix A: Organisational security plan

In order to ensure that the security policy is developed in a consistent manner and effectively across the organisation, policy and plans should be supported by the senior management team. It should also be integrated with other management policies and procedures. The security plan should flow logically from the threat and risk assessment and deliver the mitigations to the risks listed in the security risk register.

There follows a list of suggested areas for inclusion within a corporate security plan. Within each section, the roles and responsibilities for the planning, execution, delivery and monitoring of performance should be included, noting particular areas that may be outsourced.

Background

Explain the nature of the organisation and the need to operate in a safe and secure environment.

Policy statement

Encourage support for security as an integral part of the organisation's activities to be supported by all members of staff, employees and third party contractors.

Reflect the need for sector compliance and regulatory influences that should be considered during the development of security policies and plans.

Include a 'security vision', which explains the end state that the organisation is seeking to achieve.

Organisation and responsibilities

Detail the breakdown of the responsibility for security throughout the organisation.

Security objectives

Clearly state the objectives of the security strategy in terms of prevention of loss and the protection of stakeholder interests.

Security concepts

Include in this section any guiding concepts and principles that are applied, such as:

- integration of systems
- standards and compliance
- fraud prevention and investigations
- physical resilience
- scalability
- command and control
- surveillance and detection; and
- security zoning.

Procedural security

Include in this section any procedural and human element that will unite physical and technological measures and may cover the following activities:

- manned security operations
  - reception and screening
  - mail and packages
  - truck and van deliveries
  - information and intelligence
  - lock-up and close down procedures; and
  - contingency planning.
- technical security
  - surveillance plan
    - external CCTV
    - fixed cameras viewing points of entry
    - pan, tilt, zoom cameras viewing external environs
    - technology enhancement – intelligent video analysis
  - access control plan
  - intruder detection plan
  - detection systems (x-ray, explosive detection); and
  - integration with external agencies.
- physical security
  - perimeter protection
  - anti-vehicle measures; and
  - door and glazing systems security.
- security plan compliance audits
- security testing and exercises.

Appendix B: Security survey and audit process

This Appendix outlines the processes and activities to be considered as part of a security survey and audit. They can be equally applied to an individual part of the system, or applied as an organisation-wide process to review all aspects of security.

The process is divided into six key components:

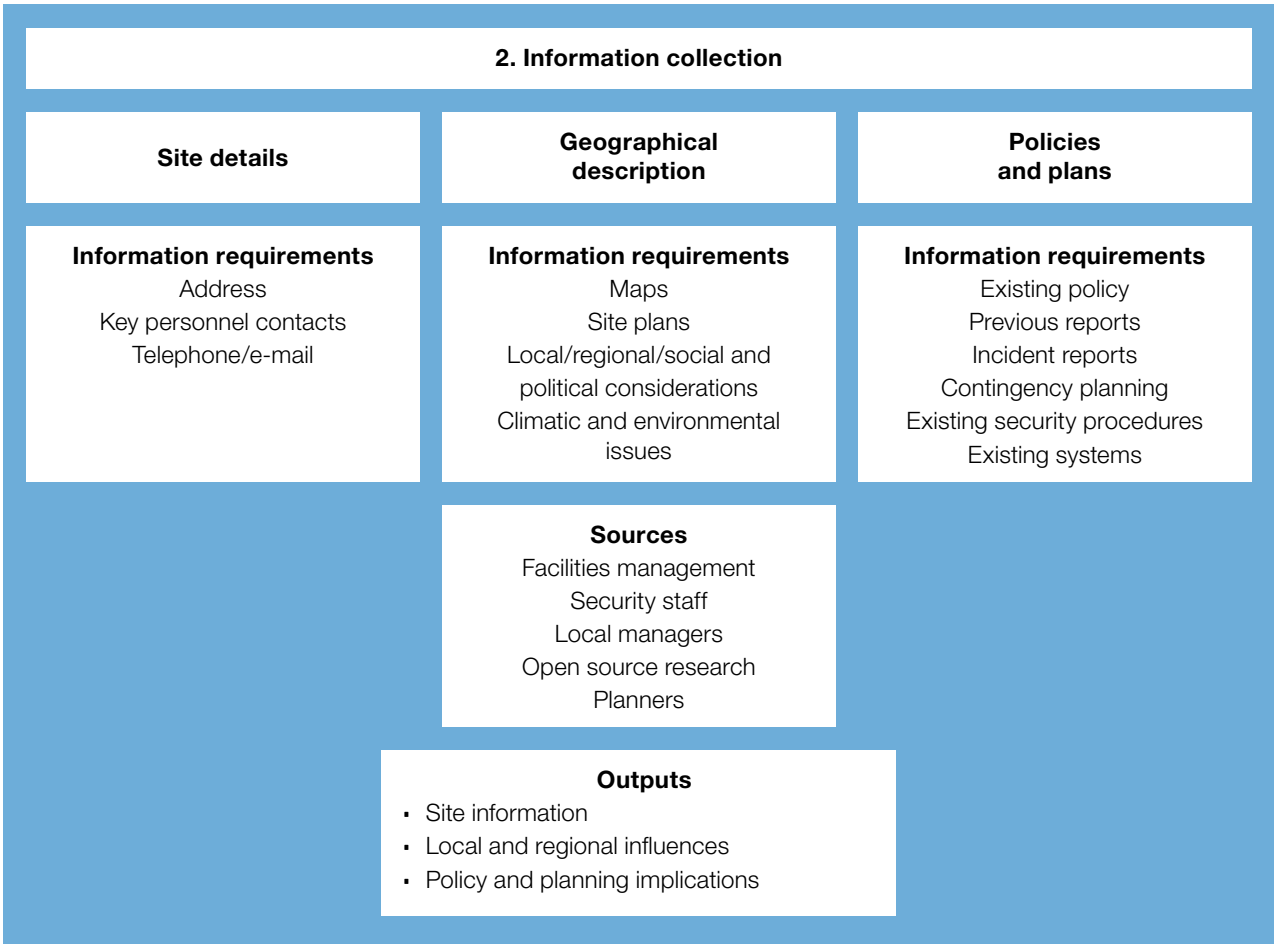
1. Planning and coordination – understand the organisation, its assets and imperatives.
2. Information collection – identify the issues and activities that may influence the current approach to security.
3. Conduct the survey – examine the effectiveness and performance in the context of the threat, approach to risk and regulatory compliance.
4. Technical
5. Procedural
6. Produce and disseminate reports – collate and report findings with illustrative support and make recommendations to reduce risk and mitigate threat.

1. Survey planning and co-ordination

Organisation characterisation	Threat assessment	Risk assessment
Activities Organisational awareness Regulatory/legal compliance Cultural imperatives Customer & employee expectations	**Activities** Open source research Agency liaison Market appreciation Management consultation	**Activities** Asset identification Asset characterisation Define probability/impact Define risk appetite Establish risk management strategy
Stakeholders Senior managers Business area managers HR Legal M&E Service providers	**Stakeholders** Senior managers Security agencies Police Security consultants	**Stakeholders** Business area managers Risk managers Security staffs

Outputs

- Organisational understanding and buy-in
- Threat awareness
- Approach to risk
- Compliance requirements


2. Information collection
Site details
Geographical description
Policies and plans
Information requirements
Address
Key personnel contacts
Telephone/e-mail
Information requirements
Maps
Site plans
Local/regional/social and political considerations
Climatic and environmental issues
Information requirements
Existing policy
Previous reports
Incident reports
Contingency planning
Existing security procedures
Existing systems
Sources
Facilities management
Security staff
Local managers
Open source research
Planners
Outputs
Site information
Local and regional influences
Policy and planning implications

3. Conduct survey

(a) Physical

Fences	Lighting	Buildings	CTM
Class (SEAP) Height Length Base Conditions Toppings	Standard (BS) Type Glare Flood Lux levels Access points Activation methods	Role Resilience standards Roof structure Floor Construction Doors/locks (SEAP, LPCB, ACPO)	Threat criteria Stand-off Building resilience Glazing Barriers and blockers (PAS 68/69) Search regimes Existing systems

Outputs

- Systems effectiveness, vulnerability
- Levels of compliance
- System shortfalls and ability to defeat threat

4. Technical

CCTV	PIDS	IDS	AACS
Standard (BS) Type (analogue, digital, ethernet, IP) DPA compliance Operator training Monitoring procedure	Standards Sensor Tamper detection False alarm rates Integration with lighting and CCTV	Standards Sensor Type Integration with lighting CCTV & response force Alarm type	Standard Type (Card, proximity, biometric) Sensors Management

Outputs

- Systems effectiveness, vulnerability and levels of compliance
- System shortfalls and ability to defeat threat
- Policy and management accountability
- Technical performance and design protocols

5. Procedural

Security management	Information security	Personnel security	Access control
Roles and responsibilities Training Licensing Policy development Threat and risk management	Compliance BS27001 Storage Management Reproduction	Vetting Management HR interface Reporting Confidentiality policy	Policy Passes (See AACS) Search regimes Booking-in Vehicle parking

Outputs

- Understanding of roles and responsibilities
- Levels of compliance
- Possible vulnerabilities

6. Produce and disseminate report

Collate findings	Brief stakeholders	Produce report

Stakeholders
Management team

Outputs

- Illustrated report with reference to the threat and risk
- Details of system performance and structural resilience
- Level of integration and support between systems
- Compliance with current standards
- Vulnerabilities and recommendations to reduce risk and mitigate the threat

Appendix C: Security standards

The following is a list of some security standards that facilities management surveyors may wish to consider when undertaking security planning and contributing to design. The list is not exhaustive and will change as technologies improve and threats change. These standards are current as at publication.

Standard	Application
BS 8220-1:200	Guide for security of buildings against crime. Dwellings.
BS 8220-2:1995	Guide for security of buildings against crime. Offices and shops.
BS 8220-3:2004	Guide for security of buildings against crime. Storage, industrial and distribution premises.
BS 7958: 2009	Closed-circuit television (CCTV). Management and operation. Code of practice.
BS 5266-1:2011	Emergency lighting. Code of practice for emergency lighting of premises.
BS EN 50131-1:2006 + A1:2009	Alarm systems. Intrusion and hold-up systems. System requirements.
DD CLC/TS 50131-7:2010	Alarm systems. Intrusion and hold-up systems. Application guidelines.
BS 8243:2010	Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions. Code of practice.
PD 6662:2010	Scheme for application of European standards for intruder and hold-up alarm systems.
BS EN 50132-1:2010	Alarm systems. CCTV surveillance systems for use in security applications. System requirements.
BS EN 50132-7:2012	Alarm systems. CCTV surveillance systems for use in security applications. Application guidelines.
BS EN 60839-11-1:2013	Alarm systems and electronic security systems. Electronic assess control systems. System and component requirements.
BS EN 50133-7:1999	Alarm systems. Access control systems for use in security applications. Application guidelines.
BS EN 50131-6:2008	Alarm systems. Intrusion and hold-up systems. Power supplies.
BS EN 50486:2008	Equipment for use in audio and video door-entry systems.
BS 5357:2007	Code of practice for installation and application of security glazing.
BS 1722-10:2006	Specification for anti-intruder fences in chain link and welded mesh (applicable for heights of at least 2.4m).
BS 1722-1:2006	Specification for chain-link fences.
BS 1722-12:2006	Specification for steel palisade fences.
PAS 24:2012	Enhanced security performance requirements for doorsets and windows in the UK.
PAS 68:2013	Impact test specification for vehicle security barriers.
PAS 69:2013	Guidelines for the specification and installation of vehicle security barriers.

Appendix D: Counter terrorist and security advice

The following organisations and individuals provide a source of information and support for facilities management surveyors when managing aspects of counter-terrorist and security advice.

ALO – Architectural Liaison Officer

Police Architectural Liaison Officers (ALOs) provide a wide range of impartial advice on crime related subjects to planners, developers, builders, landlords and estate/facility managers, etc. ALOs do not profess to be experts in all aspects of building, construction and planning, and as such will not seek to unduly interfere, obstruct or direct architects and others in the control of a project. The sole aim of an ALO is to assist in the identification and reduction of the potential criminal effects of the design and physical characteristics of a new build or regeneration scheme.

CPNI – Centre for the Protection of National Infrastructure

CPNI is a government authority that provides protective security advice to businesses and organisations across the national infrastructure. Their advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services safer.

CTSA – Counter-terrorism Security Adviser

A CTSA's core role is to identify and assess local critical sites within their force area that might be vulnerable to terrorist or extremist attack; then devise and develop appropriate protective security plans to minimise impact on that site and the surrounding community. There are now over 200 CTSAs across the UK, with most police forces having at least two. Most CTSAs work within or alongside their force special branches.

Home Office

The Home Office is the government department responsible for internal security matters, counter-terrorism and policing policies.

JTAC – Joint Terrorism Analysis Centre

JTAC was created as the UK's centre for the analysis and assessment of international terrorism. It was established in June 2003 and is based in the security service's (MI5) headquarters at Thames House in London.

MI5

The security service, more commonly known as MI5, is the UK's security intelligence agency. It is responsible for protecting the country against covertly organised threats to national security. These include terrorism, espionage and the proliferation of weapons of mass destruction. In addition, it provides security advice to a range of other organisations, helping them reduce their vulnerability to threats.

MI6

The Secret Intelligence Service (SIS) provides the British government with a global covert capability to promote and defend the national security and economic well-being of the United Kingdom. SIS operates worldwide to collect secret foreign intelligence in support of the British government's policies and objectives.

NaCTSO – National Counter Terrorism Security Office

NaCTSO is a police unit co-located with the Centre for the Protection of the National Infrastructure (CPNI). Funded by and reporting to the Association of Chief Police Officers (ACPO), NaCTSO contributes to the UK government's counter terrorism strategy (CONTEST) by supporting the 'protect and prepare' strands of that strategy.

OSCT – Office for Security and Counter-Terrorism

OSCT was established in 2007 in the Home Office, in order to bring more cohesion and greater strategic capability to the fight against terrorism. OSCT's primary responsibilities are to support the Home Secretary and other ministers in developing, directing and implementing the counter-terrorist strategy (CONTEST) across government; deliver aspects of the counter-terrorism strategy directly, e.g. legislation, policing, borders, protective security policy; facilitate oversight of security service/police counter-terrorist operations in the UK, and manage CT related crises.

SBD – Secured by Design

Established in 1989, SBD is owned by the Association of Chief Police Officers (ACPO) and is the corporate title for a group of national police projects focusing on design and security for new and refurbished homes, commercial premises and car parks as well as the acknowledgment of quality security products and crime prevention projects. SBD focuses on crime prevention at the design, layout and construction stages of homes and commercial premises and promotes the use of security standards for a wide range of applications and products.

RICS HQ

Parliament Square, London SW1P 3AD
United Kingdom

Worldwide media enquiries:

e pressoffice@rics.org

Contact Centre:

e contactrics@rics.org
t +44 (0)24 7686 8555
f +44 (0)20 7334 3811

Advancing standards in land, property and construction.

RICS is **the world's leading qualification** when it comes to professional standards in land, property and construction.

In a world where more and more people, governments, banks and commercial organisations demand greater certainty of **professional standards and ethics**, attaining RICS status is the recognised **mark of property professionalism**.

Over **100 000 property professionals** working in the major established and emerging economies of the world have already recognised the importance of securing RICS status by becoming members.

RICS is an **independent** professional body originally established in the UK by Royal Charter. Since 1868, RICS has been committed to setting and upholding the **highest standards of excellence and integrity** – providing **impartial, authoritative advice** on key issues affecting businesses and society.

RICS is a **regulator** of both its individual members and firms enabling it to **maintain the highest standards** and providing the basis for **unparalleled client confidence** in the sector.

RICS has a worldwide network. For further information simply contact the relevant RICS office or our Contact Centre.

United Kingdom
Parliament Square
London SW1P 3AD
United Kingdom
t +44 (0)24 7686 8555
f +44 (0)20 7334 3811
contactrics@rics.org

Europe
(excluding United Kingdom and Ireland)
Rue Ducale 67
1000 Brussels
Belgium
t +32 2 733 10 19
f +32 2 742 97 48
ricseurope@rics.org

Asia
Room 3707 – 09
Hopewell Centre
183 Queen's Road East
Wanchai
Hong Kong
t +852 2537 7117
f +852 2537 2756
ricsasia@rics.org

Americas
One Grand Central Place
60 East 42nd Street
Suite 2810
New York 10165 – 2811
USA
t +1 212 847 7400
f +1 212 847 7401
ricsamericas@rics.org

South America
Rua Maranhão,
584 – cj 104
São Paulo – SP
Brasil
t +55 11 3562 9989
f +55 11 3562 9999
ricsbrasil@rics.org

Africa
PO Box 3400
Witkoppen 2068
South Africa
t +27 11 467 2857
f +27 86 514 0655
ricsafrica@rics.org

Ireland
38 Merrion Square
Dublin 2
Ireland
t +353 1 644 5500
f +353 1 661 1797
ricsireland@rics.org

Oceania
Suite 2, Level 16
1 Castlereagh Street
Sydney, NSW 2000
Australia
t +61 2 9216 2333
f +61 2 9232 5591
info@rics.org.au

Middle East
Office G14, Block 3
Knowledge Village
Dubai
United Arab Emirates
t +971 4 375 3074
f +971 4 427 2498
ricsmenea@rics.org

India
48 & 49 Centrum Plaza
Sector Road
Sector 53,
Gurgaon – 122002
India
t +91 124 459 5400
f +91 124 459 5402
ricsindia@rics.org