Control Risks

Security requirements for UK property and planning

Determining security requirements for real estate developments

Across the UK, compulsory security requirements for real estate developments are increasing in response to the developing security environment, from terrorist attacks to cyber and digital threats. Many major real estate developments will now have Secured by Design (SbD) conditions, and others will have much more specific security requirements imposed by any number of stakeholders including but not limited to the client, planning commissions, local and regional governments, and citizen groups.

All developments are different and depending on the unique circumstances of the project, each of these stakeholders and their requirements can materially impact the cost and timings of a successful completion. For those navigating the uncertainties of planning policy, understanding this crucial component is key to guarding against lost time, ballooning costs and ultimately ensuring the protection of the development and the end users.

What are the relevant security requirements?

Depending on the type, scale, and location of the project there are different frameworks, authorities and codes that may need to be addressed for security policy at different stages of the development. Some of the most prominent within the UK are listed below:

National Planning Policy Framework (NPPF)

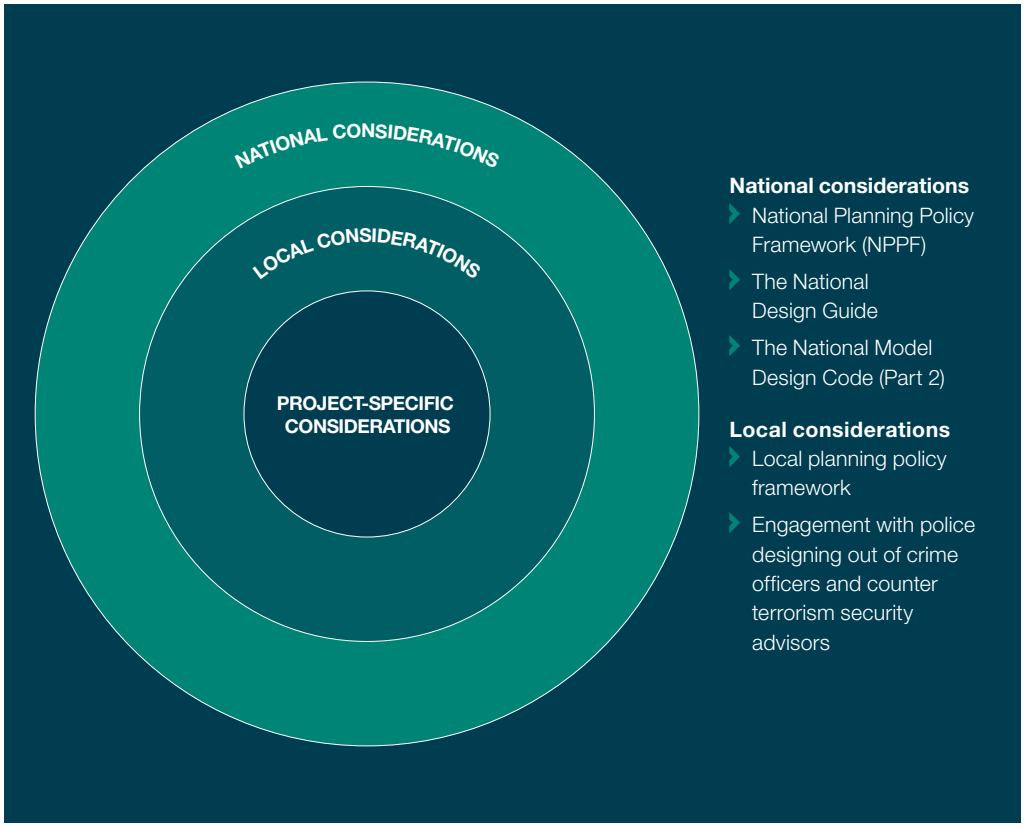
The requirement for planning authorities to consider security is stated in the National Planning Policy Framework (NPPF): *"planning policies and decisions should aim to achieve healthy, inclusive and safe places which... are safe and accessible, so that crime and disorder, and the fear of crime, do not undermine the quality of life or community cohesion…".*

The National Design Guide

The National Design Guide highlights the need to consider security through a *"risk assessment and mitigation at an early stage of the design process, so security measures can be integrated into positive design features".*

The National Model Design Code (Part 2)

The National Model Design Code (Part 2) has a whole section on SbD and counter terrorism whereby it states *"the design of town centres, shopping streets and other public spaces needs to take account of potential terrorist attacks. Preventing hostile vehicles reduces the risk of vehicle-borne attacks and road traffic collisions involving pedestrians. Urban design principles and detailed landscape design solutions need to be considered at the early design stages to mitigate risks".*



How do these security requirements affect projects?

National Planning Policy Framework (NPPF)

The NPPF clearly states that security must be considered in all projects. How that is applied varies by planning authority which creates challenges for developers and consultants supporting these projects. For example, in Greater Manchester all major developments require a 'Crime Impact Statement' provided by Greater Manchester Police. This paid-for service is mandatory and still usually results in SbD being a condition of the application. In London, it is common for developments to be mandated with the requirement for SbD certification. Counter terrorism requirements may also be stipulated if the Counter Terrorism Security Advisor (CTSA) is engaged.

Designing Out Crime Officers (DOCO) and Counter Terrorism Security Advisors (CTSA)

Decisions on which security conditions apply stem from the level of engagement from either the local police force DOCO and/or the CTSA. On most major developments these parties will be invited to comment on the application, either proactively by the developer's design team, or via direct engagement from the planning authority.

CTSAs will commonly be engaged on any project which attracts large congregations of people. They would then seek specific conditions to protect the development from terrorism threats. DOCOs would consult on most major developments and typically seek the requirements for the project to achieve SbD certification.

The uncertainty is challenging for developers. Counter terrorism mitigation measures can be extremely expensive and considering them after Royal Institute of British Architects (RIBA) Stage 2 can have considerable implications for projects. Historically, there have been significant variations in the application of SbD requirements. Some developments will have more onerous security requirements mandated than others, even when the developments have comparable risk factors. For more complex developments, the generic non-risk-based requirements of SbD may not be suitable but are conditioned anyway; during a data centre development Control Risks worked on, SbD was made a condition when the security requirements already far exceed those requirements.

Typical security challenges on projects

Prescriptive physical security requirements that are not achievable by the facade design. SbD may require accessible elements of the facade to be certified to LPS 1175 SR1 or SR2. While highly secure, most facade systems have not been tested to this standard. Typically, the main European systems have been tested to EN 1627 RC2 or RC3, which is usually not accepted by DOCOs. This can lead to more testing or a re-design causing delays and further expense.

What to consider: engage in and organise early coordination with the architect, to mitigate these challenges. Consider involving security consultants to ensure the required expertise of understanding facade security requirements.

A simplistic approach to security that doesn't consider site-specific risks. The Secured by Design Commercial Guide 2023 states "where justified by the results of a crime risk analysis, some sections of this guide allow for the adoption of enhanced measures that are commensurate with an increased risk". This means that the level of physical security can be increased by DOCOs. You might think that if security can be increased because of higher risk, it can be reduced if the risk is lower. This is not allowed and can lead to inefficient and unsustainable design.

What to consider: design teams can manage this risk by producing a detailed threat, vulnerability and risk assessment, going beyond the risk analysis typically produced by police forces.

No consideration for operational security responses to managing risk. SbD will not consider operational security measures. While a development may plan on certain operational security measures these can be cut back when sites open, for example tenants might complain about high service charge costs.

What to consider: understanding the requirements early in the design means these elements can be planned from the outset and spare the project's team any surprises further down the line.

Different approaches to the application of SbD guidance. Historically there has been a huge difference in how DOCOs apply the requirements of SbD depending on which London borough they are based in. This variation highlights the importance of flexibility and adaptability when navigating security requirements, as guidance may be interpreted and applied differently across the city.

What to consider: using security consultants who have experience working with DOCOs from across London and the UK is one way to mediate such demands.

Planning conditions that stipulate counter terrorism mitigation. While any project at risk of terrorism should consider the related risks and suitable mitigation early, those that don't could suffer huge implications. For example, the requirement for blast enhanced facades could fundamentally change the appearance of the building and contradict other planning conditions. It would also make the project significantly more expensive to build and could cause project delays.

What to consider: conducting a detailed security threat, vulnerability and risk assessment at RIBA Stage 1 is vital to avoid such complications.

Considering security holistically

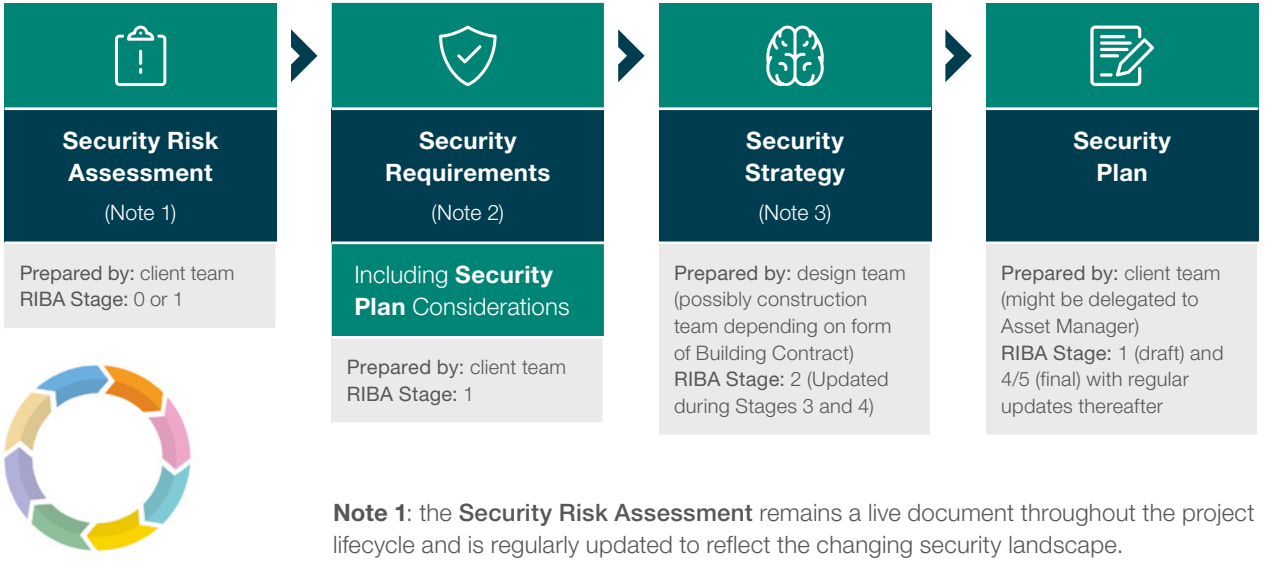
The key to avoiding these issues is the early engagement of suitably qualified security professionals. In 2023 RIBA and the National Protective Security Authority (NPSA) released the security overlay to the RIBA Plan of Works. It is clear that RIBA Stage 0 (Strategic Definition) requires a high-level security risk assessment and RIBA Stage 1 (Preparation and Briefing) requires a full security risk assessment, establishing project security requirements and a security plan. Without establishing these requirements from the outset, and including the requirements within planning applications, projects will be highly challenged.

Risk-based security design

Security must be considered for all projects, and it must be done in a risk-based manner. Conditioning SbD for all major projects, regardless of its nature, or when suitable security measures have already been included (when designed by qualified individuals) is not efficient or sustainable.

With the prospect of Martyn's Law[1], a Parliamentary Bill intended to ensure public premises and events are better prepared for and ready to respond to terrorist attacks, developers must consider security requirements holistically.

1 https://www.gov.uk/government/news/martyns-law-introduced-to-parliament-to-better-protect-the-public-from-terrorism



RIBA
Plan of Work
Security Overlay

Note 1: the **Security Risk Assessment** remains a live document throughout the project lifecycle and is regularly updated to reflect the changing security landscape.

Note 2: the **Security Requirements** are superseded by the Security Strategy and retained for future reference.

Note 3: the **Security Strategy** should be kept alongside the Security Plan and should contain the rationale and decision making behind the selection of certain measures.

Certainly, any development with a capacity over 800 people (enhanced tier) should take a detailed look at potential terrorism risks and include appropriate and proportionate mitigation measures from the outset.

Engaging with the planners, DOCOs, CTSAs and security professionals as early as possible is key to informing all stakeholders on the anticipated security risks and deciding how these should be managed. If security needs to be conditioned, it should be carried out in a risk-based manner. Conditions should also state that security requirements should be assessed and designed by appropriately qualified individuals, such as those recorded by the Register of Security Engineers and Specialists (RSES). The BRE SABRE scheme may be another way of demonstrating a risk-based approach to security design and management.

Developers and planners need to consider what security or building information is submitted into the public domain in planning applications. Whilst the local community has a right to know that any new development will be secure and have a positive effect on their environment, it shouldn't include information which would be useful to a potential threat actor carrying out virtual reconnaissance. We recommend sensitive information is excluded from applications. The DOCOs and CTSAs should be able to assist with these conversations.

Crime Prevention Through Environmental Design (CPTED)

Implemented at the planning and early design stage of a development, CPTED is a principle focused on effectively using the built environment to reduce crime by reducing the opportunity for it through the implementation of softer security measures. This is comprised of seven principles of physical security, surveillance, movement control, management and maintenance and defensible space, from the effective use of doors and windows to road layouts.

- **Physical security** ensures the individual buildings and spaces are built to withstand attacks via their physical features.
- **Natural surveillance** considers how the users of the space can observe the areas surrounding the property.
- **Movement control** restricts access to and from an area, which means threat actors feel an increased chance of getting caught.
- **Management and maintenance,** keep the development free from signs of disorder or disrepair to show the area is looked after and thus avoiding the 'broken windows' effect whereby visible signs of disorder can lead to further criminal activity.
- **Defensible space** focuses on clearly defining ownership within the development between public, semi-public, semi-private, and private areas.

The principles in CPTED promote having natural crime prevention strategies at the core of the built environment. It enables this through intentional design for safer communities and reducing the cost of additional requirements or support during the development's lifetime.

Successful projects define and address security risks early

No two projects are ever the same, and security requirements vary for a multitude of reasons. For large, complex projects it is critical to implement a risk-commensurate security design strategy early in the design process. We work with clients on detailed threat, vulnerability and risk assessments produced by our in-house analysts with in-depth local knowledge and experience. We study the project-specific vulnerabilities and determine gross risk.

The concept security design is produced with the aim of naturally designing out security risks by adopting CPTED principles. At this stage we also consider any other requirements that may be applicable, such as SbD, DOCO or CTSA guidance and Approved Document Part Q for residential developments.

All of this must be completed during or prior to Stage 2 and certainly before the planning application is submitted. We advise our clients that as part of the planning application there should be clear statements on how security risks have been considered and the principles of how security will be managed. These statements should provide the planners with the reassurance that the security provisions are proportionate and negate the need for additional conditions to be imposed on the project. This approach minimises the potential for late changes in design, increased costs and delays to programs.

About Control Risks

Our highly qualified team has extensive global experience supporting complex projects and negotiating security requirements between stakeholders. For more information contact our team:

Danny Spender
Principal
London
danny.spender@controlrisks.com

Douglas Cochrane
Director
London
douglas.cochrane@controlrisks.com

Tom Gardener
Consultant
London
thomas.gardner@controlrisks.com

Control Risks is a global specialist risk consultancy that helps create secure, compliant and resilient organisations, providing the insight and intelligence to realise opportunities and grow.

Contact us:
33 King William Street,
London, EC4R 9AT
United Kingdom

enquiries@controlrisks.com
+44 20 7970 2100

controlrisks.com