



National Protective
Security Authority

Security Overlay to the RIBA Plan of Work

Overlay prepared in association with the
National Protective Security Authority (NPSA)

RIBA 
Architecture.com

This publication has been created by representatives from the National Protective Security Authority (NPSA) with assistance from the Police Crime Prevention Initiatives (Police CPI) and the Royal Institute of British Architects (RIBA).



National Protective Security Authority (NPSA)

NPSA is the UK's National Technical Authority for physical and personnel protective security. Our mission is to make the UK less vulnerable and more resilient to national security threats. Our work helps keep our citizens safe, protects the economy and our science and technological advantage, as well as the infrastructure upon which daily life depends. We help organisations understand the range of threats they and the UK face, for example from terrorism, espionage, and hostile foreign states, and importantly what they can do to minimise their risk through how they operate day to day.



Police Crime Prevention Initiatives (Police CPI)

Police CPI is a police-owned organisation working on behalf of the UK Police Service. Over the last 30 years, it has delivered a wide range of crime prevention and demand reduction initiatives, the longest running being Secured by Design (SBD). It works with the Home Office, Ministry of Housing, Communities and Local Government, local authorities, British and European standards authorities, trade associations, test houses, certification bodies, the construction industry, manufacturers, and companies involved in security products – both within the UK and those in countries that supply the UK – and many other organisations. Police CPI maintains close working links with the National Police Chiefs' Council (NPCC) National Leads and Committees.



Royal Institute of British Architects (RIBA)

The RIBA is a global professional membership body driving excellence in architecture. It serves its members and society to deliver better buildings and places, stronger communities and a sustainable environment. Being inclusive, ethical, environmentally aware and collaborative underpins all that they do.

© Royal Institute of British Architects 2023

All rights reserved. No part of this publication may be reproduced in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the copyright owner.

While every effort has been made to check the accuracy and quality of the information given in this publication, neither the RIBA, NPSA nor any individual or organisation named in the acknowledgements accept any responsibility for the subsequent use of this information, for any errors or omissions that it may contain, or for any misunderstandings arising from it.

Foreword by RIBA President	5
Preface by NPSA	7
Introduction	8
CHAPTER 1. Security Over a Building's Lifecycle	10
CHAPTER 2. Security Stakeholders and Project Team Members	14
CHAPTER 3. Understanding the Threats	20
CHAPTER 4. Security Risk Assessment	24
CHAPTER 5. Security Requirements	28
CHAPTER 6. Security Strategy	32
CHAPTER 7. Security Plan	46
CHAPTER 8. References and Guidance	50
Glossary	52
Credits and acknowledgements	56
Appendix A: Security Overlay to the RIBA Plan of Work	58
Appendix B: Example Risk Registers	60



Foreword by RIBA President

Architects, engineers, and other construction professionals deal with a wide range of issues when designing a building. Currently key challenges, including designing for the circular economy and embodied carbon; modern methods of construction and supply chain engagement all impact on the greater design project that is conceiving and delivering world-class projects that produce long term value for clients and society.

Of course, design must address much more than the immediately apparent issues of the day. Security and how this affects the principles of good design has become an ever more important consideration at early stage design. Indeed, in recent years, terrorist attacks and new crimes, such as cyber attacks, have underlined the need to be constantly vigilant, and ensure that security matters are properly addressed when designing a building.

The purpose of this publication is to flag the ever-changing security landscape, highlighting that even the smallest of projects will have security threats that need to be considered. There are two key messages for architects. The first is that every project has its unique risks, arising from a broad range of threats. These need to be teased out and set into the client's brief so that the design team can embed security considerations into their initial ideas. The second, and related, is that many security measures need consideration and integrating proactively into the design strategies as early as possible.

This Overlay is produced for everyone involved in the built environment industry. I hope it provides helpful practical guidance on the best ways to embrace security requirements. Where it is already available, the Overlay provides links to include the latest information for designers; or when to contact experienced security advisers who can provide more specific and pertinent project advice.

We live in challenging times, and I am delighted that the RIBA has been able to work collaboratively with NPSA and Police CPI to produce this Overlay to industry.

Simon Allford
RIBA President 2021-23



Preface by NPSA

Security measures are not something that can be added to a project as it nears handover. They need to be considered from the outset prior to the client creating their RIBA Stage 1 Project Brief and a major challenge for security professionals is explaining that every site comes with different risks from a security perspective.

This publication gets this point across succinctly, underlining the importance of undertaking a Security Risk Assessment before the Project Brief is prepared to tease out the risks relevant to a specific project. As threats are constantly evolving, it stresses the importance of regular reviews through the life of a project to give ongoing resilience to a building and its occupants.

The need to consider the Security Requirements in the Project Brief, so that the client can consider the risks identified, and how these are framed to the design team responsible for preparing the design for a project, are all well laid out in the Overlay.

I was also pleased to see that the Overlay stresses the role of the Security Strategy in shaping the design and ensuring that security measures are coordinated with the rest of the design proposals. This promotes a security-mindedness approach to recognise that security threats, vulnerabilities and the potential risks are something we all need to consider and understand.

The Security Plan is an important document, setting out how security measures should be operated and maintained during the life of the building, and it was great to see that the Overlay considers the importance of framing this plan during the briefing process.

Finally, security risks change on a regular basis and the Overlay counsels everyone to revisit the Security Risk Assessment frequently to make sure that it is current and relevant.

NPSA is delighted to have collaborated with the RIBA and Police CPI to create the Overlay which we are confident will become a valuable industry document to support better long-term security outcomes for everyone involved in the lifecycle of a building. On a personal note, I would like to thank the RIBA for their outstanding leadership of this work, promoting the importance of security across all stages of a building's design and operation.

NPSA Director

This Security Overlay to the RIBA Plan of Work is for everyone involved in the safe and secure design, construction and operation of any building, including:

- Architects and designers (e.g., landscape, interiors, public realm, wayfinding)
- Clients (e.g., developers, investors, financiers)
- Engineers (e.g., structural, civil, mechanical and electrical, environmental)
- Contractors and subcontractors
- Planning and building control professionals
- Specialist security advisers
- Technology and data systems suppliers
- Building operators and managers
- Stakeholders with an interest in building and infrastructure security matters.

'Security' is defined as measures that can be taken to eliminate or reduce threats to any building, its occupants, and contents, ranging from:

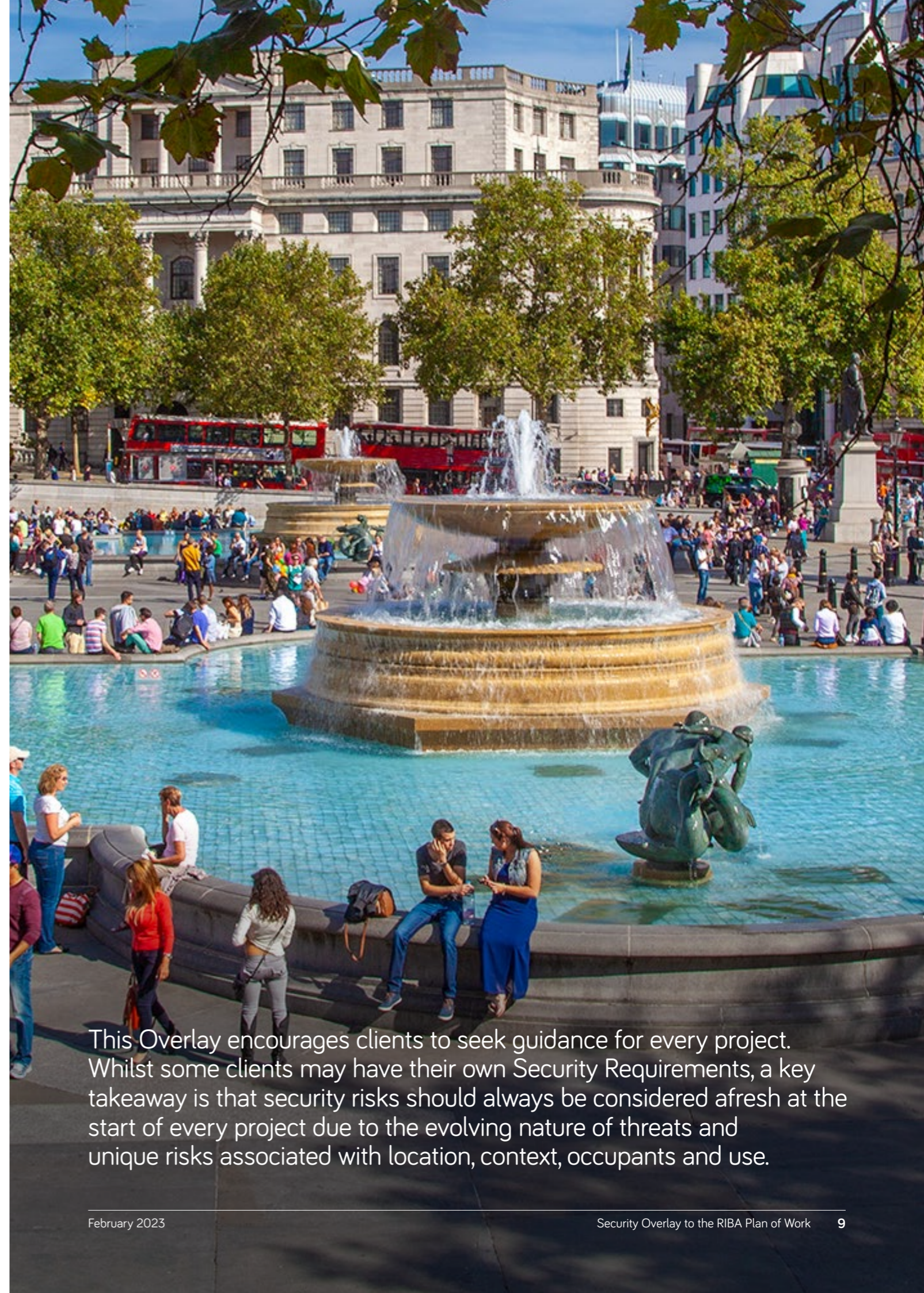
- property related crime, such as vandalism and opportunistic theft
- crimes against the person, including robbery and assault
- targeted theft of office equipment
- terrorism, industrial espionage, and civil disruption.

Given the ever-changing nature of both threats and the technology used to mitigate them, it is not intended to contain technical information on a broad range of solutions; rather this Overlay considers and sets out the strategic tasks that need to be undertaken at each RIBA Stage.

The key benefits to the different members of any project adopting this Overlay go beyond ensuring that a building is safer for its occupant.

- 1) For **project teams**, this Overlay considers the threats and determines the project specific security risks from the outset using the Security Risk Assessment, leveraging security as an enabler for better outcomes on a wide range of topics, from operations to user safety.
- 2) For **clients**, ensuring the Security Risk Assessment is undertaken in advance of, or as part of, the briefing process, informs the Security Requirements that will drive confidence that effective measures are in place before the building is occupied, and mitigate against expensive retrofitting.
- 3) For **architects and design teams** integrating security measures into the design as early as possible, including physical and technological features, leverages the expertise of the wider security landscape and key stakeholder concerns to deliver a robust Security Strategy.
- 4) For **contractors** delivering the project in line with the Security Strategy, this brings a clearer understanding of why these measures are proposed and provides transparency of any risks for consideration during the construction phase.
- 5) For **operators**, they receive a building that is aligned to the Security Plan for effective day-to-day management that keeps occupants and visitors safe and avoids the need for any additional specialists, unsightly security measures, and associated costs.

Following this Overlay will ensure anyone involved in the design and construction of a building will be part of creating a secure information environment, minimising and managing the security risks associated with the volume of data typically prepared during project delivery.



This Overlay encourages clients to seek guidance for every project. Whilst some clients may have their own Security Requirements, a key takeaway is that security risks should always be considered afresh at the start of every project due to the evolving nature of threats and unique risks associated with location, context, occupants and use.

1.

Security Over a Building's Lifecycle

Security Over a Building's Lifecycle

This Overlay advocates four security related documents that should be produced during the life of a building. As the briefing, design, and construction stages progress (RIBA Stages 1 to 6 inclusive), these documents dovetail to align with the other core project information at each stage.

During RIBA Stage 7 some of the documents will continue to evolve as the building is used and as security measures are maintained or replaced to reflect the ever-changing security landscape. As the RIBA Plan of Work is circular, aligned to circular economy principles, at the end of a building's life a new RIBA Stage 0 considers its new use and security measures.

Each document is set out in detail as shown in Figure 1, but first it is important to understand the core purpose of each document and the sequence in which they are produced.

Security Risk Assessment

The **Security Risk Assessment** is both a process that defines the threats relevant to a particular project on a specific site, including the nature of the building, its occupants, and the risks associated with each, and is also the document which captures these.

Security Requirements

The **Security Requirements** are the client's specific briefing requirements related to security that should be derived from the **Security Risk Assessment**. They might be included as a section in the **Project Brief** or could be a standalone document. To ensure that the design team are given the right strategic direction, the **Security Requirements** should consider how the client might operate their completed building. This might be by producing a draft of the **Security Plan** or by including these in the **Security Requirements**.

Security Strategy

The **Security Strategy** is produced by the design team in response to the **Security Requirements**. It includes security measures incorporated into the design and records decisions made in relation to these. The **Security Strategy** should be coordinated with other Project Strategies and any measures should be incorporated into the **Concept Design**.

Security Plan

The **Security Plan** contains the day-to-day methodologies for managing security measures once a building is in operation e.g., the provision of a security guard at a building's reception or the timing for security walk rounds.



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.

Figure 1: Sequence for producing Security Related Documents

The Security Overlay to the RIBA Plan of Work (see Appendix A) highlights the RIBA Stages when these documents should be produced.

The client should produce a draft **Security Plan** at RIBA Stage 1 to ensure that any requirements are embedded into the design although this might be part of the **Security Requirements**. The **Security Plan** should be reviewed closer to occupation to ensure that it reflects the needs of potential users, best practice, current threats, and trends. Changes to the **Security Strategy** might need to be considered if the **Security Plan** is updated, reflecting the time lag between the early design stages and the date of occupation. In parallel, an update to the **Security Risk Assessment** might also be undertaken to make sure that risk owners are clear that these have changed.

The core purpose of these documents is to ensure that:

- Every project considers the specific threats related to a site and a building's activity by preparing a **Security Risk Assessment**
- The **Project Brief**, issued to the design team, reflects the project-specific risks in the form of the **Security Requirements**
- The design team's security measures in response to these risks are summarised in a **Security Strategy**
- The contractor refines the **Security Strategy** where specialist subcontractors need to complete the design for specific security measures
- The **Security Plan** is in place for the building's handover (RIBA Stage 6), is aligned to the **Security Strategy**, and is regularly updated during its lifetime to reflect changes to the security risks.



These documents, and the tasks to be undertaken during each RIBA Stage, are covered in detail in the following chapters. However, it is worth mentioning at this stage that the **Security Strategy** and **Security Plan** work together and as such, it may be necessary for the **Security Requirements** to consider key operational requirements for the design team to reflect on as they put together proposals for security measures e.g., a building's opening hours, whether a staffed security desk is to be provided or not, how a loading bay may be utilised, or how many of the buildings electronic systems are managed over their lifetime e.g., CCTV, Automated Access Control System (AACS), Building Automation and Control Systems (BACS), etc. These impact on the design measures that might be put forward and therefore need early consideration.

Crucially, using these documents is part of ensuring that security measures are carefully considered from the outset and integrated into the design of a building. This will help shape better designed and more secure buildings.

Information Security

In addition to the process of designing a building that delivers exemplar security outcomes, it is important to consider the security of the information used throughout the lifecycle of a project which may contain sensitive information regarding the building, its occupants and use.

Storage of this documentation and its access should be appropriately managed due to cyber security threats and other issues (see Chapter 4). It is crucial that those hosting the initial project information consider this from the outset. The Employer's Information Requirements, the Project Execution Plan, and the Building Information Management (BIM) Execution Plan are appropriate locations for related strategies to be set out.



Security Stakeholders and Project Team Members

Security Stakeholders and Project Team Members

Governance of security matters needs careful consideration because many stakeholders sit outside the core project team. This chapter sets out how to determine the various parties who need to contribute to security documentation.

Those leading a project need to be clear about roles and responsibilities, who is accountable for risks and sign off, and who is consulted or informed about security, taking in account a wide range of stakeholders who may have their own vested interests.

A project's external stakeholders will vary during the life of a building, through each RIBA Stage, and from project to project. Threats, and the likelihood of them occurring, are also constantly changing requiring ongoing adaption of guidance and early engagement with specialists, i.e. addressing the recent increase in cybercrimes requires new security approaches and the involvement of cyber security specialists. Consideration must also be given to project size and complexity, i.e. the project team and associated stakeholders involved with a nuclear power station would clearly be different to that for a home or a hospital.

All projects have threats that create security risks. Therefore every project needs to be clear about the roles required in relation to security and the responsibilities that each entail during the RIBA Stages. Project team members might include:

- Client Representatives
- Client Security Teams
- Client Security Adviser
- Design Team Members
- Design Team Security Specialists
- Contractors
- Specialist Subcontractors
- Facilities Management Companies
- End-User Security Teams
- Government Security Advisers.

However, there are many other parties that shape and influence the **Security Strategy** and the list below reflects the broader security landscape. This acts as a reminder to project and design managers on the importance of consulting outside the core project team to engage with stakeholders who may include:

- Town Planners
- Building Regulation consultees including emergency services
- Designing Out Crime Officers (DOCOs) - sometimes called Crime Prevention Design Advisors (CPDAs) or Architectural Liaison Officer (ALO)
- Professional Security Advisers
- IT consultants versed in cyber threats
- Industry Bodies such as the Construction Industry Council (CIC)
- Professional Institutions
- Suppliers
- Sector Bodies such as the British Council of Offices (BCO)
- Community Groups (who may be invited to engagement sessions)
- Insurers
- Health and Safety Bodies, including the Health and Safety Executive (HSE)
- Counter Terrorism Security Advisers (CTSA)
- National Protective Security Authority (NPSA)
- National Cyber Security Centre (NCSC).

It is important to recognise that the parties listed above have different and distinct roles and responsibilities. Some may:

- Be accountable to the client, perhaps a security consultant/professional security adviser within the client team preparing the **Security Requirements** or a draft **Security Plan**
- Help to shape the design and the security measures incorporated into the RIBA Stage 2 **Concept Design** and the **Security Strategy**, with design responsibilities, backed up by their relevant professional indemnity insurance such as a security consultant in the design team
- Comment on or influence the direction of proposals prepared by others.

Ultimately, a nominated representative within the client body must be the decision maker, ratifying the final solutions that responds to the risks and signs off on the proposals.

Designing Out Crime Officers (DOCOs)

DOCOs are police staff who provide specialist advice and guidance regarding the built environment at every stage of architectural design from pre-planning to the full development control process to minimise crime, disorder and anti-social behaviour. The relevant contacts can be found at [SBD National Network of DOCOs](#).

Professional Security Advisers

The [Register of Security Engineers and Specialists \(RSES\)](#) provides a list of suitably qualified and experienced security professionals. RSES promotes excellence in security engineering by providing a benchmark of professional quality against which its members have been independently assessed.

Additionally the [Register of Chartered Security Professionals](#) has been established by Royal Charter granted to the Worshipful Company of Security Professionals and managed by [The Security Institute](#).

National Counter Terrorism Security Office (NaCTSO) and Counter Terrorism Security Advisers (CTSAs)

The primary role of the [CTSA network](#) run by NaCTSO, is to provide help, advice and guidance, on all aspects of counter terrorism protective security to specified industry sectors. NaCTSO and the CTSAs are responsible for the provision of protective security advice to Publicly Accessible Locations (where there may be large crowds who could be vulnerable to terrorist attacks) e.g., shopping centres, sporting stadiums, pubs and bars, transport hubs, etc.

National Protective Security Authority (NPSA)

[NPSA](#) is the UK government's National Technical Authority for physical and personnel protective security. They produce advice and guidance (available on their website) and also have advisers and other specialists who may be involved in providing direct advice to projects where there could be an increased risk from terrorism or other national security threats. NPSA also provides advice on the management of sensitive information relating to physical assets.

National Cyber Security Centre (NCSC)

The [NCSC](#) provides cyber security guidance and support helping to make the UK the safest place to live and work online. Advice and guidance is available on their website and some projects may have direct support from NCSC advisers.

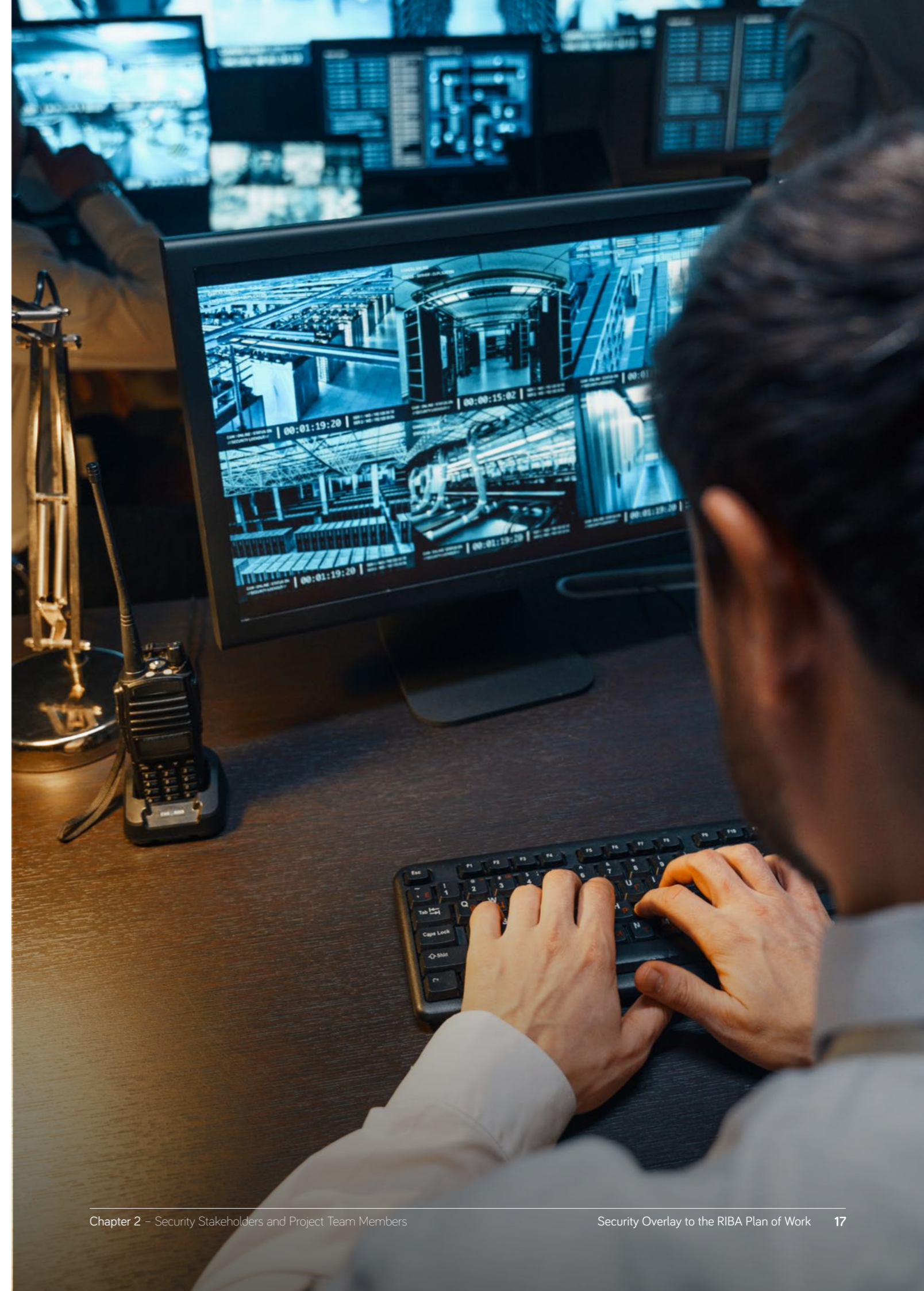


Figure 2 illustrates how different parties augment the project team during the project lifecycle. Many of these are within the initial project team and responsible for the capital phase. Other stakeholders become more involved when the building is occupied, requiring their views to be considered during the early project stages.

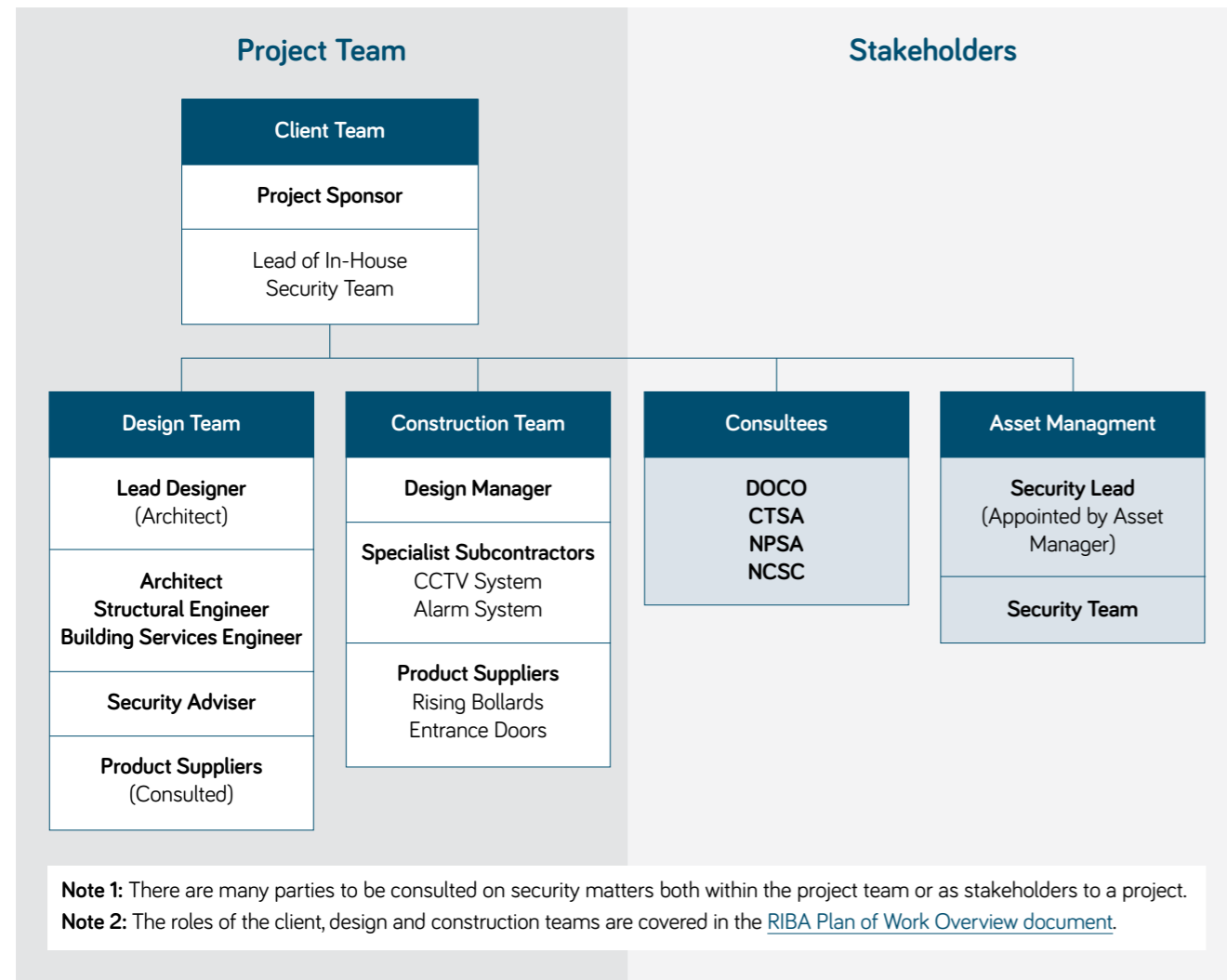


Figure 2. Generic organogram illustrating different project team members and stakeholders contributing to security matters

On large projects it is likely the client team may have an in-house security adviser or appointed one to assist with the preparation of the Security Risk Assessment and the Security Requirements. The design team may also have their own security specialist who can help steer the right security measures for inclusion in the Security Strategy and make sure that the right stakeholders are consulted. However, it is important for any client or building owner to realise that there are various bodies available to give advice to any project. Security advice might be sought during construction, or as noted above, at regular intervals when a building is in use to ensure that risks are constantly being re-evaluated.

A crucial role of setting out the project team is identifying who within the client team is responsible for signing off the Security Strategy and Security Plan. This is an important role given the risk-based methodology used to determine the risks and the range of mitigations or security measures that should be proposed.

Security Advice and Guidance

Advice can be provided to the client and design teams during any RIBA Stage. Advice is most effective when it is project specific, provided in response to the specific risks captured for a project in the **Security Risk Assessment**, **Security Requirements**, the security measures incorporated into the **Security Strategy**, or included within the **Security Plan**.

Advice can be verbal or written and can be sought formally from professional advisers (chargeable – see Professional Security Advisers), and informally through other entities (for free) including Design Out Crime Officers (DOCOs) who will be aware of and alert to crimes taking place locally making them well placed to advise on the threats or counter terrorist experts, such as CTAs and NPSA who are aware of current terrorist threats. A Planning Application Protocol is in place between the CTSA and DOCOs enabling them to work together effectively to provide formal responses to relevant planning applications.

A wide range of guidance information is available from security bodies, industry organisations, and the government on **Security Requirements** and measures and matters to be considered when developing a **Security Strategy** or **Security Plan** (see Chapter 8 for a list of relevant guidance).

3.

Understanding the Threats

Understanding the Threats

The threats posed to any **Physical** or **Digital Asset** and the **Assets** within it, including people and property, may include:

- Theft and Burglary
- Fraud (outside the remit of this publication)
- Internet-facilitated crime, such as hacking, viruses and phishing
- Trespassing
- Vandalism and Arson
- Anti-Social Behaviour
- Assault, Robbery and Violent Theft
- Intimidation/Harassment
- Extortion and Kidnapping
- Mass Protests and Demonstrations
- Terrorism
- Global or Commercial Espionage
- Sabotage
- Disclosure or unauthorised access to sensitive information.

In many instances, criminals are opportunistic and there are several strategies that can be used to minimise the crimes listed above. If buildings contain high value items, such as artwork or computers, additional thought must be given to the most appropriate measures and the means that criminals might use to carry out their threats e.g., ram raiding of store frontages is a common way for criminals to gain access to valuable property. Using the SBD framework and specifying accredited products, is a straightforward way of ensuring these risks are managed although it may need to be combined with other approaches to address all of the risks identified. Cyber security brings a new generation of risks that must be considered in different ways.

Terrorist groups may seek to attack buildings and people to advance their political agendas. Those looking to carry out espionage will work under the radar, with these threats creating different risks and requiring different measures to mitigate them.

The threats noted above:

- Are constantly evolving due to a wide range of factors, including technology, cultural, and generational issues
- Vary depending on the location of a building and its surrounding context
- May change depending on the function of a building and what its occupants will be doing.

For this reason, the likelihood of these threats occurring varies enormously from project to project resulting in every building having its own unique set of security risks. It is therefore difficult to produce prescriptive guidance for those considering the appropriate measures to eliminate, mitigate, or manage the risks for a specific building. The best means of doing so is to undertake a **Security Risk Assessment**. This should consider the likelihood of each threat occurring on a project, the vulnerabilities of a specific site, and the risks associated with a particular threat, during the life of a building.

It should also be noted that threats may be created during the design and/or construction phases such as sensitive information being made available to criminals or terrorists. These threats should be considered in the risk assessment to ensure they are managed.

Further Information

- For advice on crime contact your local police crime prevention office, DOCO, or view the [SBD website](#)
- For advice on the threat from terrorism or espionage contact your CTSA, security adviser or view the [NPSA website](#) or the [ProtectUK website](#)
- For cyber security advice and cyber threat updates view the [NCSC website](#).



4.

Security Risk Assessment

Security Risk Assessment

The best way to determine the security risks associated with a project on a specific site is to conduct a **Security Risk Assessment**. This achieves several objectives through:

- Encouraging the client to consider the specific security threats for the site
- Setting out the risks associated with relevant threats
- Considering the risks associated with the building's proposed uses
- Creating an audit trail of decisions made and any associated assumptions
- Informing the development of the **Security Requirements** and the **Security Plan**
- Potentially forming part of corporate resilience initiatives
- Informing the design team of the perceived risks and the client view
- Ensuring adjacent sites and their occupiers and/or purposes are considered
- Setting out the owners for each risk so it is clear who is responsible for eliminating, mitigating, or managing a risk at a specific project stage.

The **Security Risk Assessment** should holistically address physical, people, process, information, and technical security aspects related to the design, construction, and operation of the building. It may be negated by a physical measure incorporated into the design, and the **Security Strategy**, or a procedural measure, included within the **Security Plan**.

On many projects it may be a simple process to produce a list of the risks arising from the threats (*see examples in Appendix B*). Projects with significant threats may require a more comprehensive risk assessment, perhaps as part of a risk workshop, facilitated by someone with the relevant experience of teasing out the detail of each threat. A risk register should be produced setting out who owns each security risk, and who is responsible for eliminating, mitigating, or managing it.

As a project moves through the design stages and into construction and use, the owners might change, which underlines the importance of keeping the risk register up to date during the life of the building. In addition, people move on, and the risk register is an important way of conveying how risks were determined and explaining to those new to a specific project the decision-making processes and outcomes.

The process of determining risks is part of instilling a security culture underpinned by exemplar leadership behaviours. At the start of a project there are a broad range of individuals and organisations available to assist in the preparation of a **Security Risk Assessment** (*see Chapter 2*).

Preparing a Security Risk Assessment

When preparing a **Security Risk Assessment**, consider project team members experienced in security matters, risk managers, those who might be providing comments, and those responsible for sign off e.g., insurers might have prescriptive requirements to comply with terms and conditions of their policies whilst local crime officers might be providing general advice for consideration. This should also highlight who will prepare mitigation measures and who within the client team is responsible for signing off the **Security Strategy** and **Security Plan** for a project.

The **Security Risk Assessment** should also consider the likely behaviour and information sharing practices of the project team. Inappropriate and/or insecure sharing of design and construction information can significantly affect the security of the occupied building.

A Security Needs Assessment might be carried out as part of the BREEAM process during this stage. This exercise could be part of the **Security Risk Assessment** although it has methodologies and deliverables to be complied with in order to achieve the relevant BREEAM credits.

The **Security Requirements** (see Chapter 5) are specific security related matters that need to be shaped within the **Project Brief**. It should be noted that not every threat can be tackled by the design team or the contractor during the relevant stages and some of the risks identified will need to be addressed in the **Security Plan**.

Once the **Security Strategy** and **Security Plan** have been prepared, the risk register should be updated to check that the identified risks have been eliminated, mitigated, or the means of taking them into the next project stage are identified. The client also needs to acknowledge that security measures put in place during the design process might impact on the building's operation, requiring additional scrutiny during the design stages. This can be managed effectively by pre-empting these topics during the briefing process. This is particularly important where clients look to technology, rather than humans, to provide security solutions e.g., providing security airlocks to access a building rather than a receptionist or security guard.

Those responsible for using, managing, or maintaining a **Physical Asset** should remember that the threats, and therefore the risks associated with it, will change over time and other aspects can change the risks e.g., a new tenant in a building might change the risk profile requiring new security measures to be taken or current ones to be adjusted. For this reason, the **Security Risk Assessment** should be reviewed on a regular basis to ensure that is up to date and reflects the current risks to a building.

Even the smallest or most innocuous of projects can have unseen or unperceived security threats and the more rigorous the initial **Security Risk Assessment**, the more tailored the **Security Strategy** will be to the specific threats.



RIBA Stage 0

Outcome: The best means of achieving the **Client Requirements** confirmed.

The primary reason for RIBA Stage 0 is that a new building might not be the most effective means for a client to achieve their requirements or several sites might be under consideration. In this context, the crucial security task at Stage 0 will be understanding the threats associated with each option being considered, which might include comparisons of these options. Accordingly, an initial **Security Risk Assessment** might have to be undertaken, considering at a high-level, the security risks associated with the threats arising from each option. Some of the reasons why a site, an existing building, or another option, should be discounted on security grounds include:

- Insufficient space to securely park commercial vehicles on site
- The crime profile of the area might present an unacceptable risk
- It might not be feasible to locate a gatehouse for security staff far enough away from the building
- There may be the need for legitimate public access to the site e.g., a Public Right of Way
- Utility provisions may not be secure.

The RIBA encourages **Project Risks** to be considered as part of Stage 0 and common sense would dictate that security risks would be delivered into this category and would come from diverse sources.



5.

Security Requirements

Security Requirements

The **Security Requirements** are the client's requirements in relation to security related matters. For smaller projects, these requirements might be simple in their nature and some clients may not wish to go beyond statutory requirements, such as consulting with a local DOCO or requesting the design team to specify products complying with the Police Preferred Specification.

It is always good practice for a client to consider security at the outset e.g., the need for locking systems on doors and windows to comply with the requirements of insurance companies or setting out how sensitive areas of a building will be accessed. If the right security measures are not installed at the outset, they can be difficult and expensive to retrofit, e.g., it is difficult to conceal cables when finishes have been completed, resulting in unsightly additions. The client also needs to consider the security of information about the design and operation of the building and how to prevent access to this particularly sensitive information.

On a design and build tender, the **Security Requirements** might form part of the **Employer's Requirements**, requiring anything that might not be included in the tender documentation to be addressed and designed after the **Building Contract** has been signed. In these circumstances, the **Security Requirements** should be reviewed before being issued as part of the tender documentation.

Some statutory processes will require security matters to be addressed e.g., submitting a Planning Application. CTAs can request that security related planning conditions are placed on the build. However, security is not generally 'codified' which is why **Security Requirements** are best determined and defined for every project. A 'one size fits all' approach may miss the specific security risks of a project, its site, and occupants.

Although most of the statements in the **Security Requirements** will be descriptive, such as 'provide a secure boundary', some clients may wish to specify prescriptive security requirements whilst others may have to describe what they are seeking to achieve, leaving the detail to the design team. Examples may include instances where:

- A client may have an agreement with suppliers for multiple projects requiring a specific doorset or bollard to be specified at entrances and included within the **Security Strategy**
- The client may be agreeable for the design team and/or contractor to select the manufacturers if the equipment provided complies with national and international standards set out in the **Security Requirements**
- A particular sequence of doors in an entrance lobby might have been developed as part of global approaches to reduce tailgating possibilities
- A client may wish for security and/or operational reasons to limit the suppliers for specific products, systems, or services.

Prescribing **Security Requirements** should always be carefully considered. Risks can be managed in a variety of different ways and while some solutions may work in one context, they may not work successfully in another. This will avoid implementing approaches that may be restrictive or costly to balance the integration of appropriate and innovative security measures into the building's design more effectively and elegantly.

On larger projects most design teams will be familiar working with the client's **Security Requirements** and are likely to have security specialists in their team. They will also be more familiar with the stakeholders consulted from a security perspective. Some clients may have clear security measures they wish their design team to adopt, whilst still caveating that the design team must use their experience in responding to the **Security Requirements**. Ultimately, if a client has a specific **Security Requirement**, or even an approach they do not want to be taken, it should be included in the **Security Requirements**. This can avoid unnecessary discussions and decision-making during the design process. An important consideration for the Security Requirements is how they relate to the **Security Plan**.

The final consideration for the **Security Requirements** is to note that during the early design stages the design team will make regular reference to the **Security Requirements** and will suggest any derogations or other issues as they prepare the **Security Strategy**.

The **Security Risk Assessment** should be produced during RIBA Stages 0 and/or 1. The **Security Requirements** would be produced during RIBA Stage 1.

The **Security Risk Assessment** should also consider the security of information and the risks presented during the design period when many parties may have access to sensitive information. The Client Information Requirements and the Project Execution Plan (PEP) should set out proposals to deal with the risks identified.



RIBA Stage 1

Outcome: Project Brief approved by the client and confirmed that it can be accommodated on the site.

RIBA Stage 1 will only go ahead if the best means of achieving the **Client Requirements** is a building project. If this is the case, and any unworkable options from a security perspective have been discounted at Stage 0, the commencement of Stage 1 is the perfect time to undertake a more detailed **Security Risk Assessment**. This ensures the specific threats can be identified and the risks for each considered in the development for the **Security Requirement** and incorporated into the **Project Brief**. A new building will require a more rigorous check against Secured by Design criteria.



6.

Security Strategy

Security Strategy

The purpose of a **Security Strategy** is to summarise all discussions and decisions related to security matters, so that the basis for the security measures included in the design proposals are clear in the future. It is important that the rationale behind your **Security Strategy** is clear.

The **Security Strategy**:

- Captures the design team's response to the **Security Requirements**, including any derogations that may be required, setting out options regarding security measures and the reasoning behind the agreed final measures
- Sets out options considered for security measures and the reasoning for the final measures that are included
- Allows a broad range of security stakeholders to comment on the measures which can be captured in the strategy, including in-house security teams, local police forces, insurers, facilities management, and on-site security teams
- Is used to coordinate the different security systems in the building flagging areas where decisions are required
- Develops as the design progresses through RIBA Stages 2, 3 and 4 with more detail being added at each stage
- Can be used by the contractors' specialist subcontractors to assist them in the completion of the design of several specialist systems during RIBA Stage 4
- Might be included in the **Building Contract** as an **Employer's Requirement** document
- Can be used to refine the **Security Plan**.

The **Security Strategy** should be reviewed and commented on by the client as part of the stage report reviews during Stages 3 and 4 which will be signed off by the client. Whilst it is not commonplace for the client to review Stage 4 information, they may appoint a client monitoring team on larger projects to review and comment on the design proposals. Some clients may have in-house operations or asset management teams who should comment on the **Security Strategy** during Stages 2, 3, and 4 with the **Security Plan** in mind.

RIBA Stage 5 relates solely to contractor logistics, the administration of the **Building Contract** and construction activities. However, it also includes the completion of the **Building Manual** which will be essential in bridging information into the **Security Plan**.

There is no prescribed format for a **Security Strategy** as the security measures considered and recorded may vary depending on the type of threat identified i.e. terrorism, espionage, or criminality.

The main topics that need to be considered during the development of the **Security Strategy** are:

- Crime
- National Security Threats such as terrorism, espionage, and hostile foreign states
- Cyber Security
- Information Management.

The following principles can be used to address these topics but are not an exhaustive list. Further guidance can be obtained from relevant stakeholders.



Crime Prevention Through Environmental Design (CPTED) is a multi-disciplinary approach to crime prevention that utilises urban and architectural design and the management of the built and natural environment to prevent crime. It is founded on the basis that the physical environment can be engineered to influence behaviour, which will reduce the opportunity, incidence and fear of crime, especially that of an opportunistic nature.

CPTED is a preventative, pro-active model, and not a reactive one and therefore can lead to a more aesthetically pleasing secure environment where security is built into a **Concept Design** rather than added later. CPTED works best when there is an interaction with the Police DOCO at the earliest possible opportunity. CPTED starts with an assessment of the existing space/environment before design commences, then goes on to assess movement control and surveillance, physical security during the design process, and finally the management and maintenance of the built space/environment.

The four main principles of CPTED are:

1. Natural surveillance

Natural surveillance can be achieved by designing the placement of physical features, activities and people in such a way that maximises visibility of the space and its users. Strategies include designing streets and public spaces to increase pedestrian and bicycle traffic, ensuring potential problem areas, such as pathways, bus stops and ATMs, are well lit, and positioning windows in new buildings to directly overlook pavements and carparks. This approach can also be adopted within internal spaces of buildings.

2. Natural access control

Natural access control can be incorporated into the built environment, by denying access to crime targets. It can significantly reduce the opportunity to any perpetrator by creating a perception of risk and the fear of being seen and apprehended.

This can include the use of structures, including but not limited to:

- physical barriers (including locks)
- landscaping
- lighting, supported with signage to signpost access to the required controllable access points.

3. Territorial reinforcement

Territorial reinforcement is a design approach which identifies how physical design can produce or extend a sphere of influence over a building or space, assisting in the development of a sense of ownership.

When a space is clearly marked as public, semi-public, or private, it creates appropriate ownership of that space. By using buildings, fences, pavement, security signs, lighting and landscape to express ownership and define public, semi-public and private space, natural territorial reinforcement occurs.

4. Maintenance

Well maintained urban environments, whether public open space or building or surrounding location, will give the impression of care and continued use of space and give the impression of a reduced tolerance to crime and disorder. This also includes, maintained and good working order of lighting, paint, signage, fencing, pedestrian routes, windows and doors.

Further CPTED advice on how crime prevention measures might inform the **Security Strategy** can be found on the [SBD website](#).

Terrorist attacks may involve the use of improvised explosive devices, forced entry, vehicle as a weapon or chemical, biological and radiological attacks on a building, infrastructure, surroundings, or the people working within or near it. It is important to understand the security measures required to deal with these different threats as they may impact on the **Security Strategy** approach.

Improvised Explosive Device (IED)

Improvised Explosive Devices (IEDs) may be delivered via a vehicle, person or via the postal system. The effects can include a blast load and fragments from the device, resulting in damage to the building's interior and exterior, and injury to people inside or outside the building.

The following are ways to manage the risks:

- Maximising the distance from a potential vehicle borne IED to the building to reduce the blast load and potential damage to the building and injury to people
- Design buildings robustly for the effects of blast
- Reduce likelihood of small IEDs detonating inside the building, by managing access
- If required, keep mail screening away from the critical functions of a building.

Forced Entry

Those undertaking physical attacks on buildings may try to enter a building to cause terror and/or harm the occupants inside. It is best to stop or delay the attacker(s) entering an area or building using appropriate measures such as locked doors. Forced entry may involve the use of weapons or manual/powerful tools to overcome these barriers. It is recommended that advice is sought from security specialists when assessing security risks to define the type and likely methods of attack.

Vehicle As a Weapon (VaW)

Vehicle As a Weapon (VaW) attacks target people in areas accessible to vehicles, such as the publicly accessible locations or the wider public realm.

To mitigate hostile vehicle attacks, consider:

- Physical measures to restrict vehicle access, limit vehicle speeds around your building (predominantly to protect staff and visitors but also the building itself) or protect more densely populated or iconic area
- Implementing a hostile vehicle mitigation scheme around a building and its high footfall areas, manages this risk by reducing the impact of a vehicle attack to varying degrees (and reduces casualties and/or building damage).

Chemical, Biological, Radiological (CBR) Attacks

The challenges posed by chemical, biological and radiological (CBR) materials from a protective security point of view are various and complex. However, potential issues resulting from a CBR incident will be less significant the more the threat can be excluded from a facility.

Key mitigation involves:

- Good access control into critical facilities (such as plant rooms)
- Protection of air intakes into buildings and its distribution thereafter
- Consider how mail enters a building and if it needs to be screened. If required, keep the mail screening away from the critical functions of a building.

For all threats it is important to consider how security measures can be accommodated into the design from the outset. Additional considerations for site planning and building design are identified below.

Site Planning

- 1) Locate the building on the plot of land or design the building to maximise the distance from unknown unchecked vehicles.
- 2) Consider a complete perimeter around the building consisting of vehicle security barriers or landscaping features that prevent vehicle access and plan in the location of the physical barriers and security gatehouses.
- 3) Plan in the location for search and screening of people, vehicles and mail which all require different space constraints and security measures.
- 4) Consider if the hostile vehicle measures need to blend into the public realm or adhere to the 'look and feel' of existing surroundings. Their appearance may dictate where they are located.
- 5) Design the road network around the building to minimise the maximum speed of vehicles approaching the building by introducing bends, corners and chicanes in the road layout.
- 6) Understand if and how surrounding roads, pedestrian spaces and privately owned land might be changed to reduce vehicle speeds or restrict vehicle access (traffic management).
- 7) Engage with neighbours to understand their requirements and develop integrated security measures or meet with community groups to present proposals and seek comments.

Building Design

- 1) Design the structural frame to be resilient to prevent progressive collapse following a blast.
- 2) The façade design will be the most vulnerable element of the building:
 - a) Limit the percentage of solid and glazed facades with the site planning, i.e. roadside facades having less glazing.
 - b) Use laminated glass to minimise glass fragments from a blast load.
 - c) Provide robust fixings to the structural frame to help retain the façade and minimise hazards.
- 3) Carefully consider the necessity of atria and whether these introduce avoidable risk of falling glass.
- 4) Consider materials used to create internal partitions. For smaller threats inside the building, some materials may create a greater hazard e.g., the use of glass in these areas could increase injury levels.
- 5) Consider using physical barriers between unauthorised and authorised users of the building by installing access control gates, doors, and walls.
- 6) For defined entry points, consider search and screening measures for both people and vehicles.
- 7) Create barriers around and throughout the building to delay or prevent attackers from progressing. Consider lock down requirements in the building design.
- 8) Consider designing in protected space for people to evacuate to. These should be located away from vulnerable facades, and the ground and first floor.
- 9) Locate key **Assets** i.e. control rooms, muster points, heavily populated areas, away from the vulnerable facades, and the ground and first floor.
- 10) Consider separate air ventilation systems to control rooms, reception areas and other critical rooms, and consider air intake at height if the risk of CBR needs to be reduced.

Espionage (State or Commercial)

Attacks that are surreptitious in their nature will often be more challenging to mitigate due to the increased awareness and skill of the attacker and the subtlety of the methods used. A methodology has been developed by NPSA that uses a layered approach of products which have been tested to resist such attacks.

This methodology centres on three elements:

- 1) Implementing effective barriers.
- 2) Controlling access.
- 3) Detection of attacks.

Only when all three are used in unison with each other can an effective protective layer be formed.

When considering mitigations for surreptitious attacks, the location of rooms where sensitive information or equipment will be stored or used, or where sensitive conversations will be held, needs consideration including the protection of information about the design.

Sensitive Projects

Sensitive projects where the client will work with government classified material (or other sensitive materials) are likely to employ a specialist security adviser with access to further NPSA guidance on the process and details of security products which have been tested to withstand surreptitious attack. It is recommended that you consult with a specialist security adviser if there is a requirement to include protection from surreptitious attack in the design.

Sensitive Rooms

Location of rooms containing sensitive information needs additional scrutiny.

- 1) Access to the secure room should be via an area under control of the building occupant i.e., not a shared entrance or public area.
- 2) They should ideally be located on a floor between two floors under the occupant's control i.e., the middle floor of a three-story building.
- 3) They should not share a dividing wall in a shared occupancy building or party wall shared with another building.
- 4) They should have no windows.
- 5) There may be special requirements for the vents and/or cabling to the secure room.
- 6) They will need to be fitted with doors and locking systems tested to withstand surreptitious attacks.

Further advice on how protective security measures might inform the **Security Strategy** can be found in the [NPSA guidance – Protecting Your Assets](#).



Buildings are beginning to deploy more systems that are connected to the Internet e.g., using smart building technologies aligned to IoT (Internet of Things) devices and sensors to undertake a broad set of use cases. Small projects might have voice activated technologies that are connected whilst larger projects will have significant IT infrastructure, including comms rooms and cabling for connecting their devices, and provision for wireless networks.

With building automation systems increasingly using cloud based solutions and linking to other software packages, including dynamic maintenance and asset management software and/or links to sensors within the building, the protocols used to maintain the cyber security of these systems need to be considered during the design process.

Where cyber risks are identified it is recommended that clients appoint IT specialists experienced in cybercrime to advise on the most appropriate solutions to provide protection in this evolving arena. Best practice and further advice can be sought from the [NCSC](#).



Information will be collected or created during each stage of a project. It is important to understand where this information is being stored and who needs access to it as this may impact the safety, security, and resilience of a building. Guidance on security minded information management can help to mitigate this can be viewed [here](#).

The UK BIM Framework (*see further information below*) and its associated standards also provide advice on how to store and structure information, and how to manage its security by considering different levels of access to information, password protocols, and other means of limiting access to sensitive information. This is particularly important during RIBA Stages 4 and 5 when hundreds of project team members may have access to project information and are able to review and download contents.

If the information needs to be shared more widely or within the public domain, it is important to ensure that any sensitive information is excluded from this information. Advice on Sensitive Information in Planning Applications (SIPA) is available from the [GOV.UK website](#) (*see further guidance below*).

UK BIM Framework

The UK BIM Framework is managed by the British Standards Institute (BSI) and is about more than Building Information Modelling (BIM). It provides the standards related to information security matters and how a client should consider these.

[ISO 19650 BIM Standard](#) helps organisations involved in the design, construction, operation and decommissioning of **Assets** to reduce the risks associated with sensitive information which could impact on the safety, security and resilience of a building. As part of this Standard, BS EN ISO 19650-5:2020 sets out the principles and requirements for security-minded information management. It also covers the security-minded management of sensitive information that's obtained, created, processed and stored during the lifecycle of a building. Many of the measures to deal with this are practical and pragmatic i.e., having sensitive security-minded information in separate folders that can be accessed by the full project team or add passwords to documents such as the **Security Strategy** or **Security Plan**.

Sensitive Information in Planning Applications (SIPA)

A major consideration for anybody preparing information that will be published into the public domain is ensuring that any sensitive information is excluded from the information, i.e. it is not the job of a Planning Authority to redact sensitive information and the final information to be published may not be seen by advisers. Those publishing such information should carefully consider the labelling that is added, such as 'security room' or the level of detail shown. It would be prudent to also prepare a redacted version of the document for the Planning Authority to upload to their portal.

Similarly, when tendering, as information will be issued to many parties it should be carefully reviewed to ensure that any sensitive information is redacted.



Procurement Considerations

Procurement considerations are made from the outset of a project and impact each RIBA Stage in different ways. This may influence the information that is produced, when it is produced, and when it is issued for tender.

The procurement route has an impact on the **Security Strategy** because it determines who might complete aspects of the design associated with the **Security Strategy**. It may also impact on the products specified and who specifies them. It might also determine how security measures are incorporated into the **Building Contract**, notably:

- On traditional forms of procurement, the design team will manage all security measures, including those that might be designed by the contractor
- On management or construction management contracts, certain packages might be secured early requiring security interfaces and coordination to be considered earlier
- On design and build forms of projects several topics need consideration, including:
 - Product specification: can these be specified descriptively or do the products need to be prescribed to achieve the security outcomes?
 - Stage 4 Design: Not all aspects of the Stage 4 Design will have been undertaken or complete before the **Building Contract** has been agreed. Consider if security measures that will be designed after the **Building Contract** have been covered in the contract documentation.

The client needs to consider how the selected procurement route impacts on the **Security Strategy** and, if additional measures are required, to mitigate any risks. This may involve:

- Asking the design team to specify products to ensure that the right level of quality is achieved
- Considering the design intent information to be incorporated into the **Employer Requirements** to ensure that every security measure has been considered
- Using the **Security Requirements** to make sure client goals are clear and unambiguous - these can cover gaps in the design information and place obligations on the contractor to close them out
- The contractor briefing their supply chain on the importance of information security (view [NCSC guidance on how to assess supply chain cyber security](#)).

As noted above, the client may employ a client monitoring team to review the **Contractor's Proposals**. This team might include a security consultant.

Other aspects may need to be considered before the building is occupied. This includes checking if all Planning Conditions related to security have been discharged and ensuring occupants are trained to use the security measures that have been installed.



RIBA Stage 2

Outcome: Architectural Concept approved by the client and aligned to the Project Brief

RIBA Stage 2 is the most important one for the development of the **Security Strategy** as it involves integration of security measures into the design, coordination with other **Project Strategies** such as fire and acoustics, and ensures allocation within the **Cost Plan**.

During Stage 2, the architect or designer will produce the **Architectural Concept**. This concept cannot sit in isolation and needs to take cognisance of many factors, including: the **Client Brief** and any **Security Requirements**; the site and its surroundings; the **Strategic Engineering** considerations e.g., plantroom sizes and locations.

The measures produced by the design team in response to the **Security Requirements** will be wide ranging and require input from architects, landscape architects, structural or building services engineers, and security consultants and advisers. They will need to be presented to the client team for comments. They also need to be costed to ensure they are affordable. Some risks may require several options to be developed and discussed, and the pros and cons of each considered before a decision is made on the right approaches. A DOCO, CTSA or security consultant might be consulted before the **Concept Design** progresses too far to ensure that best practice security measures are incorporated into the design.



RIBA Stage 3

Outcome: Architectural and Engineering Information Spatially Coordinated.

With the strategic aspects of the **Security Strategy** signed off by the client at RIBA Stage 2 and significant heavy lifting in relation to the **Security Strategy** realised, it is essential during RIBA Stage 3 that the lead designer, and the other members of the design team, maintain their vigilance.

During RIBA Stage 3, more coordination will be undertaken and the types of tasks that might occur would include:

- Coordinating security measures into the design e.g., ensuring that foundations for bollards are not clashing with existing or new underground services
- Preparing a Crime Impact Statement to submit with the Planning Application
- Preparing a SBD application to ensure that security matters can be signed off prior to or during the period the planners are considering an application
- Checking that the systems connecting to each other such as lift, CCTV, access or other systems have been coordinated and that both the operation, and the physical and cyber security requirements of these systems, have been considered
- Reviewing vehicular access in greater detail to make sure that the proposals in the **Concept Design** are robust
- Considering more detailed proposals for entrances including the products to be specified.



RIBA Stage 4

Outcome: All design information required to manufacture and construct the project completed.

The RIBA Stage 4 outcome clarifies all the tasks required to finalise the design information needed to manufacture and construct the project. Security related tasks in this stage might include:

- The preparation of information by the design team for the relevant aspects of the security measures, e.g.:
 - the final locations for alarm points or any fixtures and fittings
 - detailed drawings for landscape or other external features
 - design intent information for the façade packages including the preparation of specifications
- The preparation of information by the specialist subcontractors appointed by the contractor to develop and complete the design of building's automation and security systems e.g., detailed drawings of CCTV, PA, and other systems
- Reviewing information produced by the contractor. On design and build contracts this might be information produced by the design team and specialist subcontractors.



RIBA Stage 5

Outcome: Manufacturing, Construction and Commissioning completed.

RIBA Stage 5 relates primarily to the tasks required to manufacture and construct a building, including administration of the **Building Contract**, quality checks, and regular inspections, both on and off-site. At this stage it is important to check that agreed security designs are implemented correctly, otherwise the level of protection expected might be compromised.

On some projects, the contractor's Logistics Plan may need to consider risks related to the site e.g., the ability to access the site from adjacent buildings. If this is deemed a project risk, it can be identified during the **Security Risk Assessment**.

A specialist will undertake the commissioning of security systems. However, the means of training the building's owners and/or users in these systems needs consideration, as the increasing complexity of these systems requires greater training before they can be operated effectively and efficiently.

During Stage 5, the contractor will prepare the information to be handed over on completion. This will include details of the different security measures that have been incorporated into the building. This information might be incorporated into the **Security Plan**.

Other aspects may need to be considered before the building is occupied. This includes checking if all Planning Conditions related to security have been discharged and ensuring occupants are trained to use the security measures that have been installed.



Security Plan

Security Plan

Various parties may refer to a **Security Plan** using a different term e.g., a security manager might use the term when referring to a response plan. For the purposes of this publication, the **Security Plan** is the document used by the building user and/or operator/maintenance team to gain information on how security measures should be operated and maintained. It might be a standalone document or an appendix to a larger document such as the **Building Manual**.

The **Security Plan** performs several functions. It should set out how the security measures included in the **Security Strategy** will be managed and maintained. In many instances, these aspects will be subcontracted to external organisations e.g., the provision of security guards or the need to staff a reception area. It is important that when these companies are bidding for the relevant contracts that the intended security operation of the building is clear.

The **Security Plan** needs to consider:

- Access control for unknown vehicles/people
- How access points and reception facilities will be managed, including out of hours
- If staff or technology will be used to manage security aspects on a day-to-day basis and how control rooms will be managed
- How to communicate all its aspects to all users of the building
- Maintenance requirements for security measures, including preventive maintenance to ensure that all measures operate effectively
- Aspects related to an emergency response plan - who to contact and/or steps to be taken.

The **Security Plan** needs to contain operational, maintenance, and asset information as outlined below.

Operational Information

Information on how each building system contributes to the **Security Strategy**. This is important because if a security measure is not used as intended, it may compromise the **Security Strategy** and the safety of the **Built Asset** or the **Assets**. This information might recommend visits from suppliers, designers, or security consultants to review the building in operation to ensure that everything is working as intended. This is also useful as part of any **Feedback** loop allowing future buildings to benefit from a client's experience of using a building.

Maintenance Information

Information on who to contact if maintenance of any security measure is required. This is important for events such as a turnstile in an entrance not working or a door not locking, as these create security risks. In addition, many security measures should have regular maintenance undertaken to make sure that this does not occur. The **Security Plan** can outline these aspects. Increasingly, new building management systems include predictive analytics to further avoid maintenance problems and reduce energy use, and these might all be set out in the plan.

Asset Information

When a building is handed over, digital information on the **Built Asset** will be handed over to the client. This information should already be compliant to BS EN ISO 19650-5:2020 which sets out how information on certain systems or spaces can be subject to additional security measures.

The **Security Plan** should consider where and how the client will store this information, who will have access, and how passwords or authentication tools will be managed to create a secure information environment.

The **Security Plan** is not a static document. It should be subject to regular and rigorous reviews to ensure it is aligned to the latest threats and the risk of them occurring. The client may carry out regular **Security Risk Assessments** to ensure that the risk register and **Security Plan** are up to date. This can include **Feedback** from security teams, comments from users, reviews of similar buildings, or discussions with security consultants and bodies. The important consideration is that security is dynamic and that a culture of security will ensure that a **Physical Asset** and its **Assets**, including occupants, always remain safe.

The client may wish to consult with security bodies (*see Chapter 2*) when preparing an updated **Security Plan** prior to a building's occupation. This is to ensure that it reflects early discussions or, given the time lag between buildings being designed and occupied (which can be three to five years or more), that new best practice requires changes to the security measures previously implemented.



RIBA Stage 6

Outcome: Building handed over, **Aftercare** initiated, and **Building Contract** concluded.

RIBA Stage 6 is about closing out the **Building Contract** during the one-year (typical) Defects Liability period. It might only be relevant from a security perspective if there are any defects to be rectified in any of the security measures, or if longer-term maintenance of these systems (e.g., three years) is a requirement of the **Building Contract**.

Feedback sessions as part of **Aftercare** initiatives, may be arranged, and security stakeholders should be involved to provide comments on the process, including how design decisions were made. Depending on the operation of the building, they should also be invited to make observations on security measures so these can be adopted or adapted for future projects.



RIBA Stage 7

Outcome: Building used, operated, and maintained efficiently.

RIBA Stages 6 and 7 occur concurrently. By the time Stage 6 has been concluded, the project team for capital phase (CAPex / design and construction) will be complete and focus will be on the operational phase (OPex).

The **Security Plan** is a core Stage 7 document as it sets out all the key aspects related to security during this stage. Importantly, it should cover training of building staff so that security measures are operated effectively. The **Security Risk Assessment** might be regularly revisited during Stage 7 to reflect changing threats and new methodologies for mitigating the risks associated with these. There is also benefit to including the **Security Strategy** as part of the documentation available to the Stage 7 team, as this will include the rationale behind the security measures which can also be useful for informing replacement strategies.



8.

References and Guidance

The following resources and publications provide invaluable reference and guidance information in addition to the contents of the RIBA Plan of Work Security Overlay.

Online Resources

Association of British Insurers: www.abi.org.uk

British Insurance Brokers' Association (BIBA): www.biba.org.uk

Business in the Community: www.bitc.org.uk

Health and Safety Executive: www.hse.gov.uk

Loss Prevention Certification Board (LPCB) and the Red Book: www.redbooklive.com

National Counter Terrorism Security Office (NaCTSO): www.protectuk.police.uk

National Federation of Small Businesses: www.fsb.org.uk

National Protective Security Authority (NPSA): www.npsa.gov.uk

National Security Inspectorate: www.nsi.org.uk

The RIBA Plan of Work 2020 Overview: <https://www.architecture.com/knowledge-and-resources/resources-landing-page/riba-plan-of-work>

Security Industry Authority: www.gov.uk/government/organisations/security-industry-authority

Security Service: www.mi5.gov.uk

Secured By Design: www.securedbydesign.com

Further reading

[CPNI: Public Realm Design Guide Hostile Vehicle Mitigation Third Edition](#)

[IET & NCSC: Code Of practice Cyber Security in the Built Environment 2nd Edition](#)

[Chartered Institute of Building \(CIOB\): The role of security in the construction industry](#)

[NCSC: Joint ventures in the Construction Sector guidance](#)

[NCSC: Construction Guidance](#)

[UK Government Guidance: Design processes and tools](#)

[UK Government Guidance: Crown development – dealing with security sensitive information](#)

Major Infrastructure Projects Terminology

Table 1 outlines the core terms and tasks associated with security, including their purpose and how they relate to other security aspects.

Table 1: Major Infrastructure Projects Terminology	
Term	Definition
Asset	An Item, People or Physical or Digital Asset that has potential or actual value to an organisation or individuals.
Digital Asset	Digital Information such as documents, spreadsheets, 3D models, Common Data Environments or Digital Twins need to be considered from a security perspective in the same way as a Physical Asset .
Physical Asset	A Physical Asset may comprise a building, multiple buildings (e.g. on a site or campus), a portfolio or network of assets, or a built infrastructure (e.g. roads, railways, pipelines, dams, docks, etc.) and may include associated land or water. Might also be referred to as built asset, however, Physical Asset positions this term better for the introduction of digital twins.
Security Needs Assessment	<p>A Security Needs Assessment (SNA) is a visual audit of a site and its surroundings to help identify threats and their associated risks.</p> <p>An SNA is frequently undertaken to achieve BREEAM credits for a project that requires BREEAM accreditation and can be carried out by a Suitably Qualified Security Specialist (SQSS) who conducts an evidence based SNA during or prior to Concept Design. SABRE - a BRE security risk management standard for new and existing buildings, infrastructure assets and managed space - may support the SQSS when developing the recommendations or solutions. This includes:</p> <ul style="list-style-type: none"> Establishing facility security requirements and understanding security risks Developing a strategic plan for security Designing an appropriate security system Implementation of plans and, for existing facilities, managing change at a facility.
Security Plan	<p>The Security Plan is a documented, systematic set of policies and procedures setting out how to achieve security needs or objectives identified in the Security Strategy for the operation of the asset. The Security Plan:</p> <ul style="list-style-type: none"> Will be developed after the Security Risk Assessment Detail how the measures selected after the Security Risk Assessment will be integrated with each other and operated Cover all aspects of security including physical, personnel, information, and cyber security Detail the policies and procedures for achieving the Security Requirements identified in the Project Brief.
Sensitive Project	<p>A Built Asset should be a Sensitive Project if it:</p> <ul style="list-style-type: none"> Forms part of the critical national infrastructure Fulfils a defence, law enforcement or national security or diplomatic function Is a commercial site involving the creation, trading, or storage of significant volumes of valuable materials, currency, pharmaceuticals, chemicals, petrochemicals, or gases Constitutes a landmark, nationally significant site Is a crowded place Is used or is planned to be used to host events of Security Significance. <p>Proximity to a Sensitive Project can raise the Security Risk to a project even though the project itself isn't sensitive.</p>

Table 1: Major Infrastructure Projects Terminology

Term	Definition
Security Requirements	<p>Project specific considerations related to security for incorporating into the Project Brief. Security Requirements can refer to:</p> <ul style="list-style-type: none"> Guidance to be reviewed during the design process Specific security tasks to be undertaken during the design process, roles and responsibilities, accountability for sign off, stakeholders consulted and/or informed about security.
Security Risk Assessment	<p>The Security Risk Assessment takes the threats identified and assesses the likelihood and impact these being relevant to a given site, prioritises them and identifies those which require mitigation.</p> <p>There is no set methodology for carrying out a Security Risk Assessment and it can be done as part of a project's main risk assessments. The resultant risk register may look to work in tandem with the Security Requirements by providing the initial steer to the design team in how each risk should be dealt with.</p>
Security Strategy	The Security Strategy outlines what security measures have been incorporated into the design based on the Security Risk Assessment and the Security Requirements . Crucially, it captures decision making so the reasoning behind the measures is clearly understood in the future.

Security Related Terms to the RIBA Plan of Work 2020

Table 2 considers how security aspects, covered in greater detail in earlier chapters, relate to the tasks associated with specific RIBA Plan of Work terms.

Table 2: Security Related Tasks to the RIBA Plan of Work 2020

RIBA Plan of Work Term	Explanation of Security Related Task
Aftercare	Aftercare is derived from the Soft Landings initiative and looks to how the team delivering the Physical Asset can help provide a better interface into the operational phase and collect Feedback for future projects.
Architectural Concept	Ensure that measures included in the Stage 2 Security Strategy are based on the Security Requirements and incorporated into the Architectural Concept .
Asset Information	Outline details of suppliers of measures included within the Security Strategy , including maintenance information, details and names of approved installers or repair companies, and considers any confidentiality or other security matters that may be set out in the Security Plan .
Building Manual	The Building Manual should contain details of how measures included in the Security Strategy are incorporated into the Building Systems and how these will be operated at RIBA Stage 7, which might be outlined in the Security Plan . The Security Strategy might be included as an appendix to the Building Manual to provide useful decision-making information to users.
Building Systems	Consider how Building Systems influenced by the Security Strategy and consider security guidance relevant to their design.

Table 2: Security Related Tasks to the RIBA Plan of Work 2020

RIBA Plan of Work Term	Explanation of Security Related Task
Business Case	Consider how the Security Risk Assessment and Security Requirements might influence the Business Case e.g., result in different sites having significantly different security risks due to their location and the nature of the occupants' work. Conversely, how other ways of dealing with the Client Requirements might reduce the security risks e.g., refurbishing a building or dispersing activities across several sites to provide resilience.
Client Requirements	Consider the Security Requirements that need to be included in the Client Requirements . The Client Requirements should be reviewed for compliance with any Security Requirements to ensure that they are aligned.
Cost Plan	Consider how measures incorporated into the Security Strategy are incorporated into the Cost Plan , including providing an Outline Specification of the key measures.
Design Programme	The Design Programme should contain key security related tasks, including: <ul style="list-style-type: none"> Workshops to consider measures to be included in the Security Strategy in response to the Security Requirements Meetings to review the Security Strategy Timescales for issuing the Security Strategy and receiving comments from stakeholders The period for incorporating measures from the Security Strategy into the Outline Specification.
Feedback	Obtain Feedback from the Security Requirements, Security Strategies and Security Plans from similar projects and consider the relevance of these whilst developing the Client Requirements . Undertake visits of precedent projects, including discussions with users and in-house security teams.
Handover	Ensure the Security Plan is in place for the building's handover and aligned to the Security Strategy with regular updates to reflect changes to the security risks.
Information Requirements	Consider the information required to ensure that the Security Strategy is effectively implemented at RIBA Stage 7 including how this strategy relates to the Security Plan .
Outline Specification	Include key measures from the Security Strategy in the Outline Specification such as: <ul style="list-style-type: none"> Door system specifications including locks and ironmongery Information on security and CCTV systems - Lighting systems and their controls
Planning	Consider if the Security Requirements and/or Security Strategy (depending on when planning consultations commence) will influence the views of the planners, particularly where a Sensitive Project is involved.
Planning Application	Consider security related consultations that may be carried out by the Planning Authority assessing the Planning Application . Ensure relevant information is incorporated into the Planning Application and consider pre-application discussions, particularly for Sensitive Projects . Determine the need for the Security Strategy to be submitted with the application.
Post Occupancy Evaluation	The Post Occupancy Evaluation should include consideration of the measures set out in the Security Strategy and the Security Plan . Have they been effective? What Feedback should be passed on the security stakeholders for incorporating into future security guidance documents?
Project Brief	Include Security Requirements within the Project Brief . Review the Project Brief for potentially contradictory requirements e.g., the requirement to have an open and accessible campus conflicting with the Security Requirements requiring a secure and safe campus.

Table 2: Security Related Tasks to the RIBA Plan of Work 2020

RIBA Plan of Work Term	Explanation of Security Related Task
Project Budget	Review any Security Requirements that need to be considered in the development of the Project Budget . This can include key threats and how their risks are mitigated e.g., bollards to mitigate hostile vehicle attacks.
Project Execution Plan	Include the details of key advisers or stakeholders identified with security roles and responsibilities in the Project Execution Plan , including an organogram of how security governance fits into the structure of the client and design teams.
Project Outcomes	Consider if any aspects of the Security Plan might influence the Project Outcomes set within the Project Brief .
Project Programme	Include key consultations with advisers or stakeholders with an interest in security as defined in the security governance in the Project Programme .
Project Risks	Consider the need for a Security Risk Assessment to determine security along with other Project Risks or consider security risks as part of a risk register discussed and developed at a risk workshop.
Project Strategies	Develop a Security Strategy in response to the Project Brief and consider what Building Systems are required in response to the Security Requirements . Consider the impact of security on other Project Strategies e.g., the Fire Strategy.
Responsibility Matrix	The client team should consider if advice related to security is required to shape the Security Requirements in the Project Brief . Consider security related tasks that might be undertaken by the design team, including security advisers required during the design stages, and ensure that their tasks are included in the Responsibility Matrix .
Site Appraisals	When considering different sites or building projects, including refurbishments, consider how site features might influence the development of the Security Risk Assessments such as: <ul style="list-style-type: none"> The location of the site The nature of adjacent buildings such as Sensitive Projects The links to public realm or other public amenities. <p>If necessary, obtain advice from a security specialist to assess the threats associated with each site.</p>
Stage Reports	The Stage Reports should contain a section on the Security Strategy outlining measures that have been considered, why these have been incorporated in the design, what risks they are managing or mitigating, and how these have been influenced through discussion with stakeholders. <i>(For more detail see Chapter 6, Security Strategy.)</i>
Strategic Engineering	Consider how the Security Requirements and initial thoughts for measures to be incorporated into the Security Strategy might influence the Strategic Engineering of the project e.g., blast protection, parking for cars and trucks, and protection of the public realm.

Credits and acknowledgements

Lead author

Dale Sinclair, WSP

Contributors

Arup
D J Goode & Associates Ltd
National Counter Terrorism Security Office (NaCTSO)
National Protective Security Authority (NPSA)
Police Crime Prevention Initiatives (PCPI)
The Royal Institute of British Architects (RIBA)
Thornton Tomasetti

Editing










Caroline Brock, Talent Lab

Design

Darkhorse Design



Appendix A: Security Overlay to the RIBA Plan of Work

 RIBA Plan of Work Security Overlay	 0 Strategic Definition	 1 Preparation and Briefing	 2 Concept Design	 3 Spatial Coordination	 4 Technical Design	 5 Manufacturing and Construction	 6 Handover	 7 Use
Stage Outcome at the end of the stage	The best means of achieving the Client Requirements confirmed If the outcome determines that a building is the best means of achieving the Client Requirements , the client proceeds to Stage 1	Project Brief approved by the client and confirmed that it can be accommodated on the site	Architectural Concept approved by the client and aligned to the Project Brief The brief remains "live" during Stage 2 and is derogated in response to the Architectural Concept	Architectural and engineering information Spatially Coordinated	All design information required to manufacture and construct the project completed Stage 4 will overlap with Stage 5 on most projects	Manufacturing, construction and Commissioning completed There is no design work in Stage 5 other than responding to Site Queries	Building handed over, Aftercare initiated, and Building Contract concluded	Building used, operated and maintained efficiently Stage 7 starts concurrently with Stage 6 and lasts for the life of the building
Security Related Tasks	Undertake High Level Security Risk Assessment and consider impact on Project Risks	Undertake Security Risk Assessment Prepare Security Requirements and include within Project Brief Consider Security Governance and the need for the appointment of security advisers or consultants within the project team Produce draft Security Plan or include strategic requirements in Security Requirements	Prepare Security Strategy in response to Security Requirements Ensure that Concept Design , Strategic Engineering proposals and other Project Strategies are coordinated with Security Strategy Ensure that Cost Plan allows for measures included in Security Strategy Review Security Strategy against draft Security Plan Consult with internal and external security professionals as set out in Security Governance	Update Security Strategy as required Ensure that any security measures are Spatially Coordinated with other aspects of the design Continue to consult with security professionals as required	Update Security Strategy as required Ensure designs produced by specialist subcontractors are integrated into coordinated design and reviewed against Security Requirements Continue to consult with security professionals as required	Discuss with security professionals outlined in Security Governance any security risks associated with the site and any logistics	See Stage 7	Review Security Plan on regular basis along with Security Risk Assessment to ensure that it reflects the latest threats
Security Information	High Level Security Risk Assessment	Security Risk Assessment Security Requirements Security Plan (Draft)	Security Strategy	Security Strategy (Updated)	Security Strategy (Updated)	Security Strategy (Updated) Building Manual Security Plan	Security Plan (Updated) Security Risk Assessment (Updated)	Security Plan (Updated) Security Risk Assessment (Updated)
<i>Security Risk Assessment</i>	Produced by Client Team	Updated As Required	Updated As Required	Updated As Required	Updated As Required	Updated As Required	Updated As Required	Updated As Required
<i>Security Requirements</i>	N/A	Produced by Client Team	Derogations Reviewed	Reviewed	Review Relevance for Procurement Strategy	Review	N/A	N/A
<i>Security Strategy</i>	N/A	N/A	Produced by Design Team	Updated As Required	Updated As Required	Updated As Required	N/A	N/A
<i>Security Plan</i>	N/A	Review as part of Security Requirements	N/A	N/A	N/A	Produced by Client Team	Updated As Required	Updated As Required

Appendix B: Example Risk Registers

Project	New Town Office Building		
Client	Prime Developers		
Site	Old Town Road		
Date	22-Apr-22		
Threat	Risk	Proposed Mitigation	Status / Note
Theft and Burglary	Tenants not known so risks difficult to identify.	Good quality locks installed on buildings external doors. Include infrastructure that enables tenant to install motion detectors or other measures.	Tenant may wish to install additional measures such as motion sensors.
Trespassing	Unsafe environment, facilitating theft, vandalism or terrorism.	Perimeter fence, security patrols, staff security awareness training to promote vigilance.	
Vandalism and Arson	Damage to property.	Design to incorporate SBD principles, depending on tenant Landlord installs CCTV System to building perimeter.	Design team to engage with DOCOs early in the project. MEP team to develop performance specification.
Assault, Robbery and Violent Theft	Staff being approached and assaulted in car park.	Provision of good quality lighting and CCTV and access control to car park.	Design team to make proposals during RIBA Stage 2.
Intimidation / Harassment	Unknown	Other measures should mitigate.	
Extortion and Kidnapping	Unknown	To be considered by tenant.	
Mass Protests and Demonstrations	Unknown	To be considered by tenant.	
Commercial Espionage	Unknown	To be considered by tenant.	
Internet-facilitated crime such as hacking, viruses and phishing.	Unknown	Consider how IT infrastructure responds to this risk.	To be considered by tenant.
Terrorism	Meeting with CTSA or NPSA to be arranged at start of RIBA Stage 2 to determine risk.	Some terrorist risk mitigation measure may affect the design e.g., if the risk from bomb blast is a credible threat.	Consider location of building on the site and whether specific materials to minimise fragmentation are likely to be required to be used.

Appendix B1: Example of Risk Register developed during a **Security Risk Assessment** for a medium-sized office building in a regional town

Major Threat Category	Threat Sub-category	Vulnerabilities		Initial Risk			Additional Mitigation		Mitigated Risk		
		Type or description	Subject Affected	L	I	R (LxI)	Physical	System	L	I	R (LxI)
Terrorism	VBIED	Loading Bay	People	3	2	6	Loading bay design enhanced to withstand blast.	Access control to loading bay.	2	1	2
			Asset	3	4	12			2	3	6
Terrorism	PBIED	Crowded cafe area	People	4	3	12	Access control to non public area.	Security patrols and CCTV operators to detect left bags and suspicious behaviours.	3	3	8
			Asset	4	3	12			3	3	9
Terrorism	Bladed or Blunt force weapons attack	Crowded area	People	5	3	15	Access control to office area.	Security patrol and CCTV to detect suspicious behaviours.	5	2	10
			Asset	5	2	10			5	2	10
Terrorism	Loss of sensitive data facilitated by an insider	Corporate offices	People	3	2	6	Access control to office area.	Insider risk mitigation measures with restricted access to sensitive information.	2	1	2
			Asset	3	5	15			2	4	8

Appendix B2: Extract from a Risk Register developed during a **Security Risk Assessment** for a major project

Royal Institute of British Architects
66 Portland Place,
London, W1B 1AD, UK
Tel: +44 (0)20 7580 5533
info@riba.org
www.architecture.com

Incorporated by Royal Charter No: RC000484
Registered Charity Number 210 566
VAT Registration Number 232 351 891

RIBA 
Architecture.com