THE SECURITY INSTITUTE

JULY 22, 2026

QUALITATIVE SECURITY RISK ASSESSMENT

For the Built Environment – Overview

- Defining the full Threat Vulnerability & Risk Assessment (TVRA) / Security Risk Assessment (SRA) for a built asset
- Distinguishing a full SRA from the BREEAM Hea 08 Security Needs Assessment requirement
- Mapping SRA obligations to each RIBA Plan of Work Stage

David Buston CSyP, FSyI, MAPM

Protective Design & Security

Romsey

45-Minute Webinar · CPD Accredited · Mapped to RIBA Security Overlay Framework

OVERVIEW

AGENDA

Six modules · 45 minutes · Q&A

01

SRA in the Built Environment

Purpose - why qualitative? The regulatory and policy landscape and security risk management frameworks

02

Anatomy of a full TVRA / SRA

What a complete TVRA / SRA should contain

03

Anatomy of a BREAM Hea 08 – SNA Security

What is an SNA, purpose, scope and credits options

04

Overlay for the RIBA Plan of Work (PoW)

Mapping SNA & SRA / TVRA to the PoW

05

Full TVRA / SRA vs SNA

Depth, scope, application to the RIBA PoW

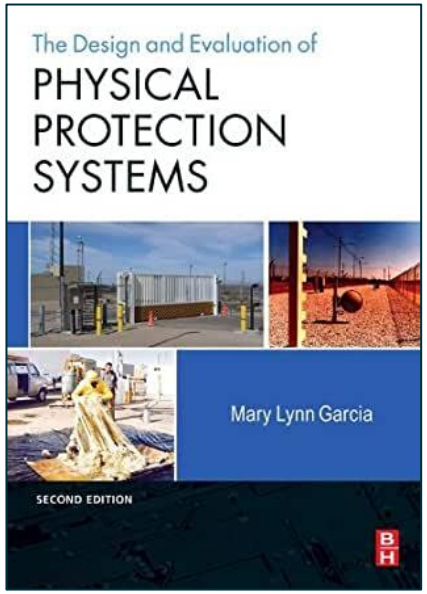
06

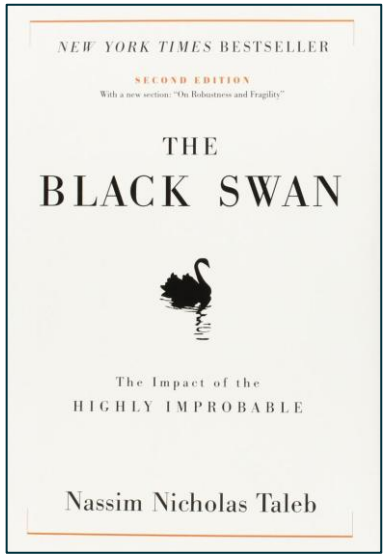
Integration in practice

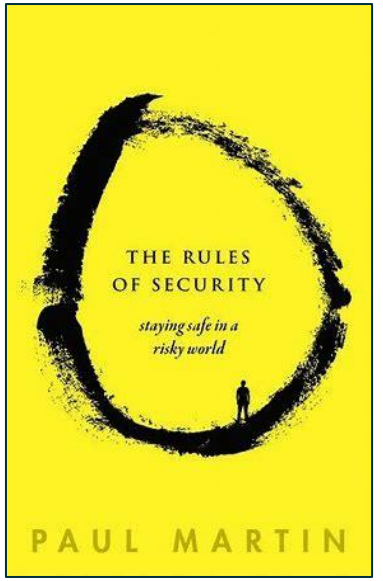
Using a full TVRA / SRA to drive design

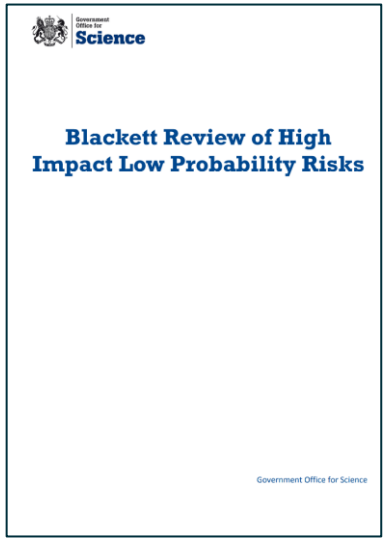
SOURCES

- **The Design and Evaluation of Physical Protection Systems** (2nd ed.). *Mary Garcia, 2008, Sandia National Laboratories, Burlington, MA: Butterworth-Heinemann.*
- **The Black Swan. The Impact of the Highly Improbably** (2nd ed.). *Taleb, Nassim Nicholas, 2010, London: Penguin.*
- **The Rules of Security** (1st ed.). *Paul Martin, 2019, CSyP Oxford: Oxford University Press*
- **Blackett Review of High Impact Low Probability Risks.** *UK Gov. Office for Science*









SECURITY RISK ASSESSMENT - GETTING IT RIGHT

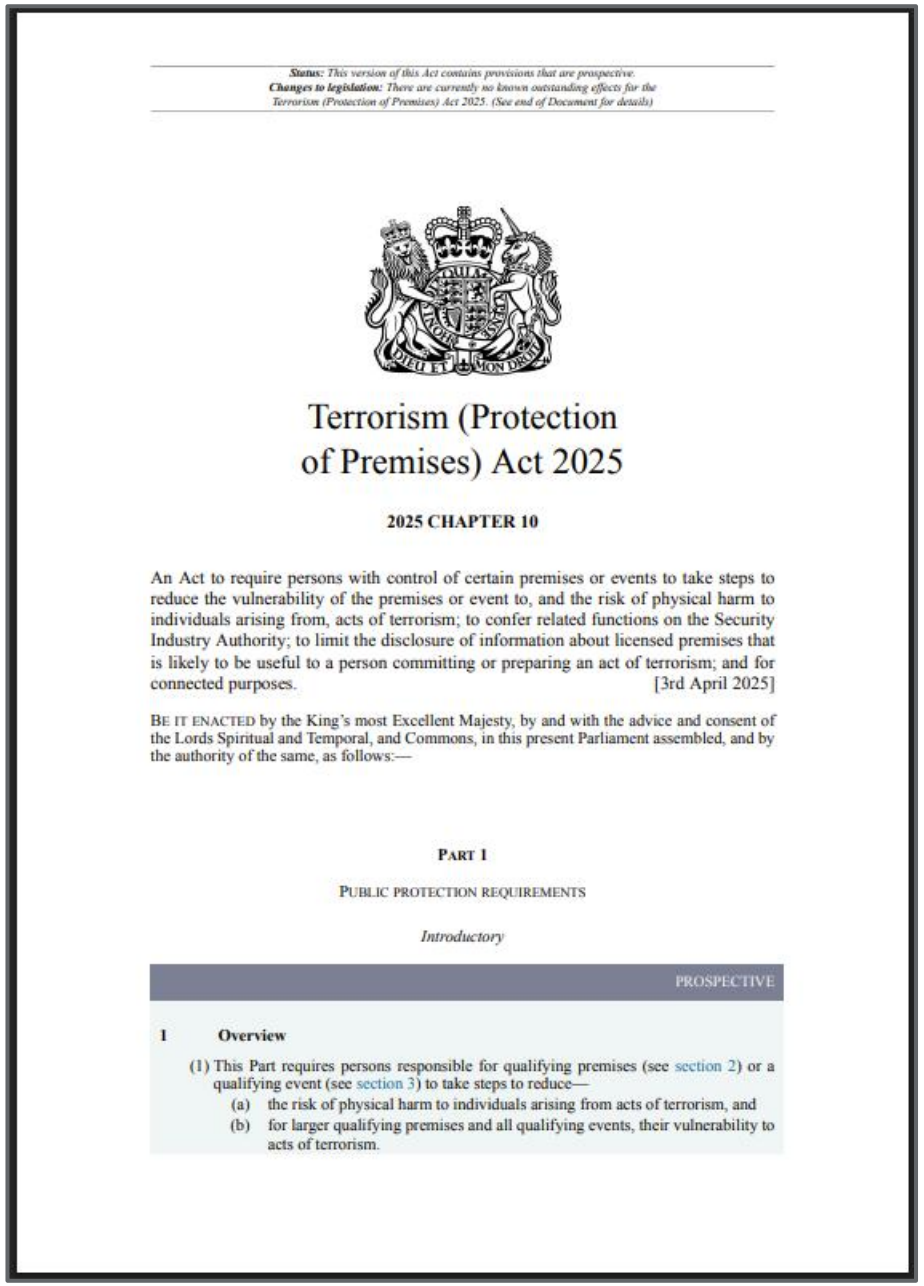
With the statistical low probability but high impact of the threat from terrorism, there was a risk of a perception that *“it won’t happen here”.*

Saunders (2021)
The Manchester arena inquiry report vol.1

UK LEGAL BASIS

Martyn's Law - Who is affected?

- Publicly Accessible Locations (PALs): hospitality, retail, entertainment, education, healthcare, sports, leisure, transport hubs.
- Qualifying Events: ticketed or controlled-access events expecting 200+ attendees.
- **Exclusions:** Certain government buildings, regulated industries (aviation, shipping, rail, civil nuclear), some transport premises, private gatherings without public access.
- **Responsible Person:** Entity controlling premises or event; must appoint Designated Senior Individual (DSI) for corporate bodies.
- **Risk Assessment & Plan:** Informs appropriate and proportionate measures - to protect the building in so far as is reasonably practicable



Status: This version of this Act contains provisions that are prospective.
Changes to legislation: There are currently no known outstanding effects for the Terrorism (Protection of Premises) Act 2025. (See end of Document for details)

Terrorism (Protection of Premises) Act 2025

2025 CHAPTER 10

An Act to require persons with control of certain premises or events to take steps to reduce the vulnerability of the premises or event to, and the risk of physical harm to individuals arising from, acts of terrorism; to confer related functions on the Security Industry Authority; to limit the disclosure of information about licensed premises that is likely to be useful to a person committing or preparing an act of terrorism; and for connected purposes. [3rd April 2025]

BE IT ENACTED by the King's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

PART 1

PUBLIC PROTECTION REQUIREMENTS

Introductory

PROSPECTIVE

1 **Overview**

(1) This Part requires persons responsible for qualifying premises (see section 2) or a qualifying event (see section 3) to take steps to reduce—
(a) the risk of physical harm to individuals arising from acts of terrorism, and
(b) for larger qualifying premises and all qualifying events, their vulnerability to acts of terrorism.

01 SECURITY RISK ASSESSMENT IN THE BUILT ENVIRONMENT

POLL

PURPOSE OF SECURITY RISK ASSESSMENT

To acquire, evaluate and present information to provide insight on potential security risks to assets. Findings inform decisions to invest in cost effective, appropriate and proportionate security measures.

In the built environment, a TVRA / SRA is conducted at defined RIBA stages. It is the primary instrument for identifying security requirements and translating these and security policy into security design, procurement specifications and operational arrangements to reasonably mitigate security risks

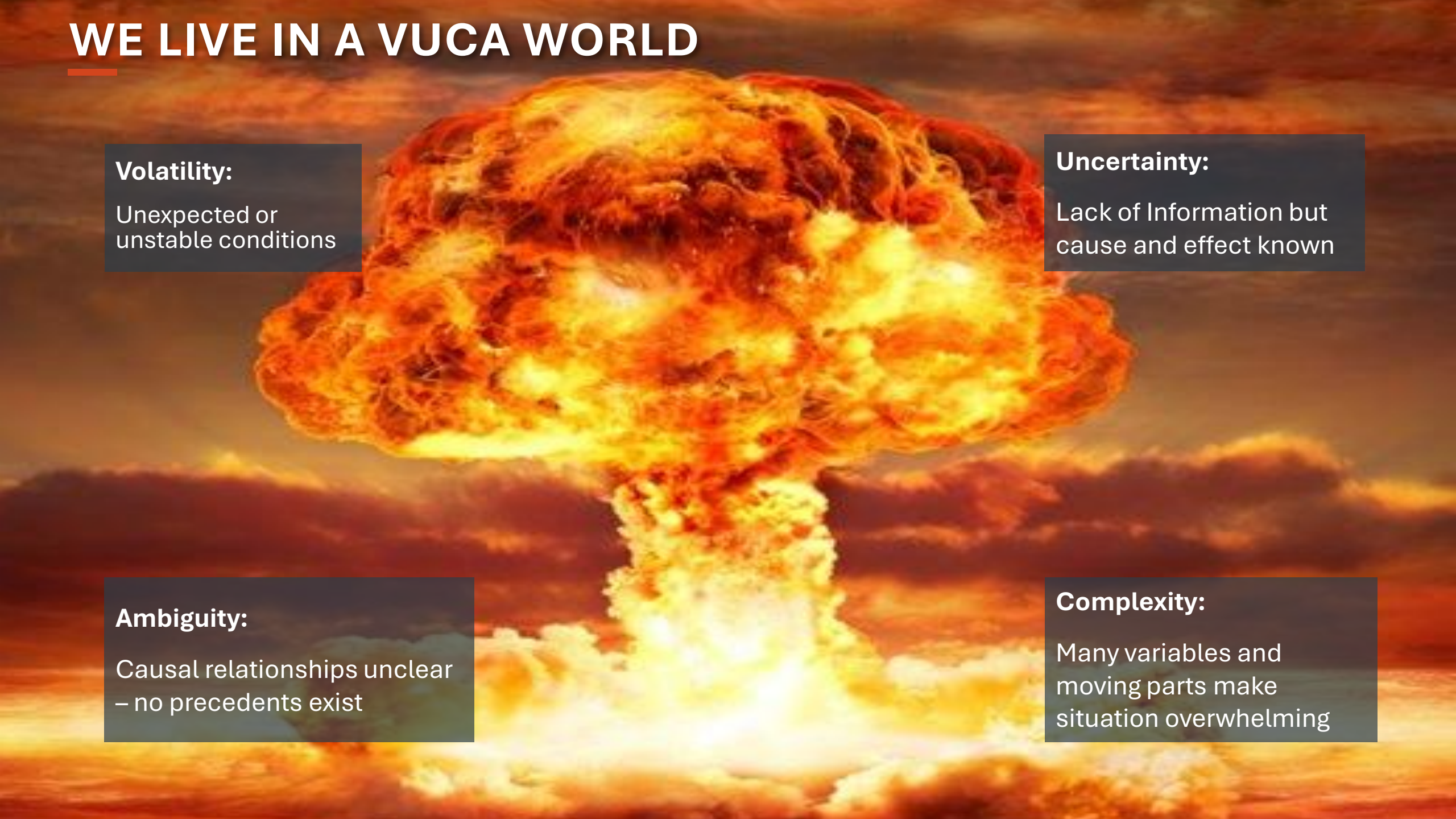
"We need the wisdom to know what we do not know"

Theaetetus of Plato

"To know what you know and what you do not know, that is true knowledge".

Confucius

WE LIVE IN A VUCA WORLD



Volatility:

Unexpected or unstable conditions

Uncertainty:

Lack of Information but cause and effect known

Ambiguity:

Causal relationships unclear – no precedents exist

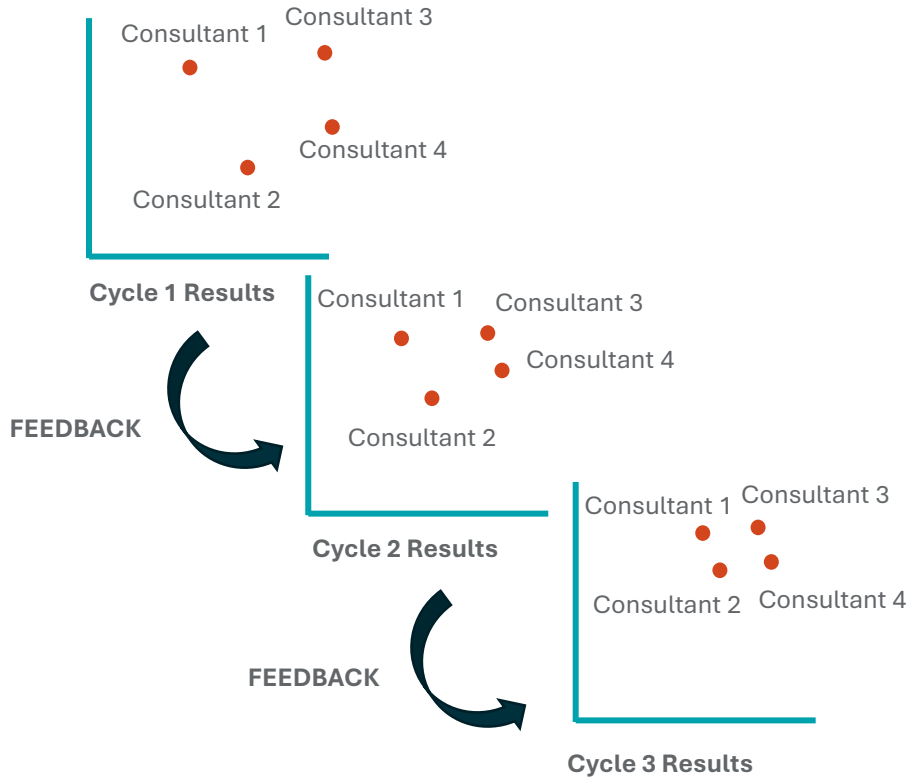
Complexity:

Many variables and moving parts make situation overwhelming

COGNITIVE BIAS

Countering Bias

- We are all prone to systematic distortion by psychological predispositions but...
- Our cognitive biases can be countered by being aware of and understanding them and by acquiring expertise through practice and experience.
- The Delphi method is a technique of structured communication, originally developed as a systematic, interactive forecasting method.
- Delphi relies on a panel of experts working through an iterative process of analysis to converge ideas over a series of cycles until consensus is reached.



QUALITATIVE vs QUANTITATIVE ASSESSMENT

Qualitative

- Subjective assessment
- Uses descriptive scales (Very Low-Very High)
- “Expert” input can add credibility
- Relatively quick and easy form of assessment
- Based on health and safety methodology, broadly recognised and accepted across multiple industry sectors in UK / International
- Can lack credibility if risk assessment process is flawed or lacks context and granularity
- Ambiguous asset, threat and vulnerability criteria will skew assessment results

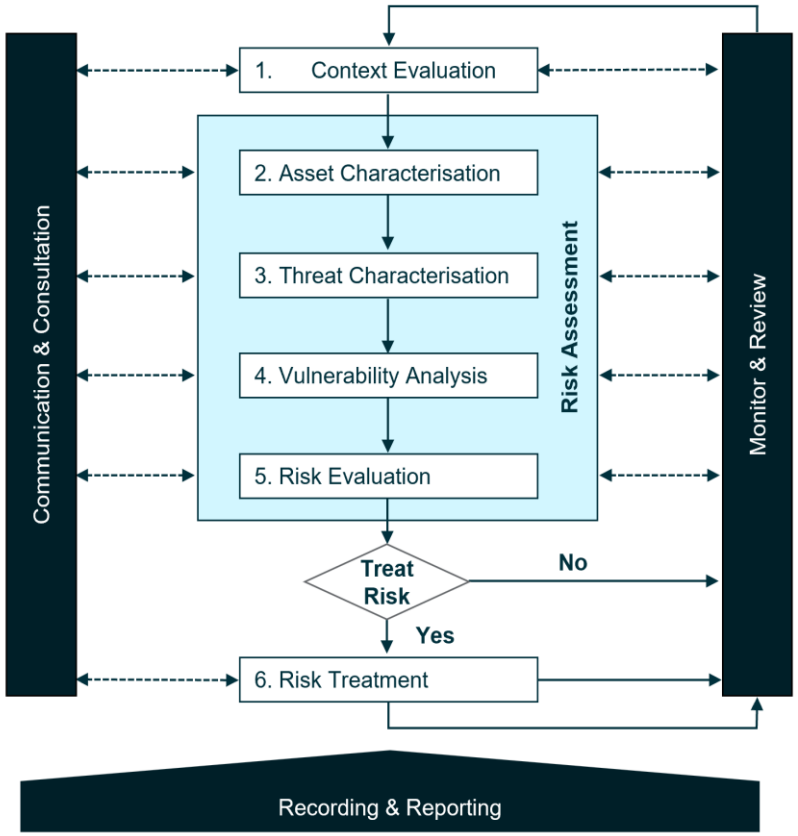
Quantitative

- Objective assessment
- Clients like finite numbers – uses numerical probabilities and frequencies
- Complex mathematical modelling, relying on accurate input data
- Resource-intensive; requires statistical expertise
- Can take a lot of time to produce results, so can be expensive to deliver
- Modelling and simulation software graphics enhance argument
- The problem with databases & AI: **Junk in = Junk out!**

02 ANATOMY OF A FULL THREAT VULNERABILITY & RISK ASSESSMENT (TVRA) / SECURITY RISK ASSESSMENT (SRA)

QUALITATIVE RISK-BASED ASSESSMENT

ISO 31000: 2018



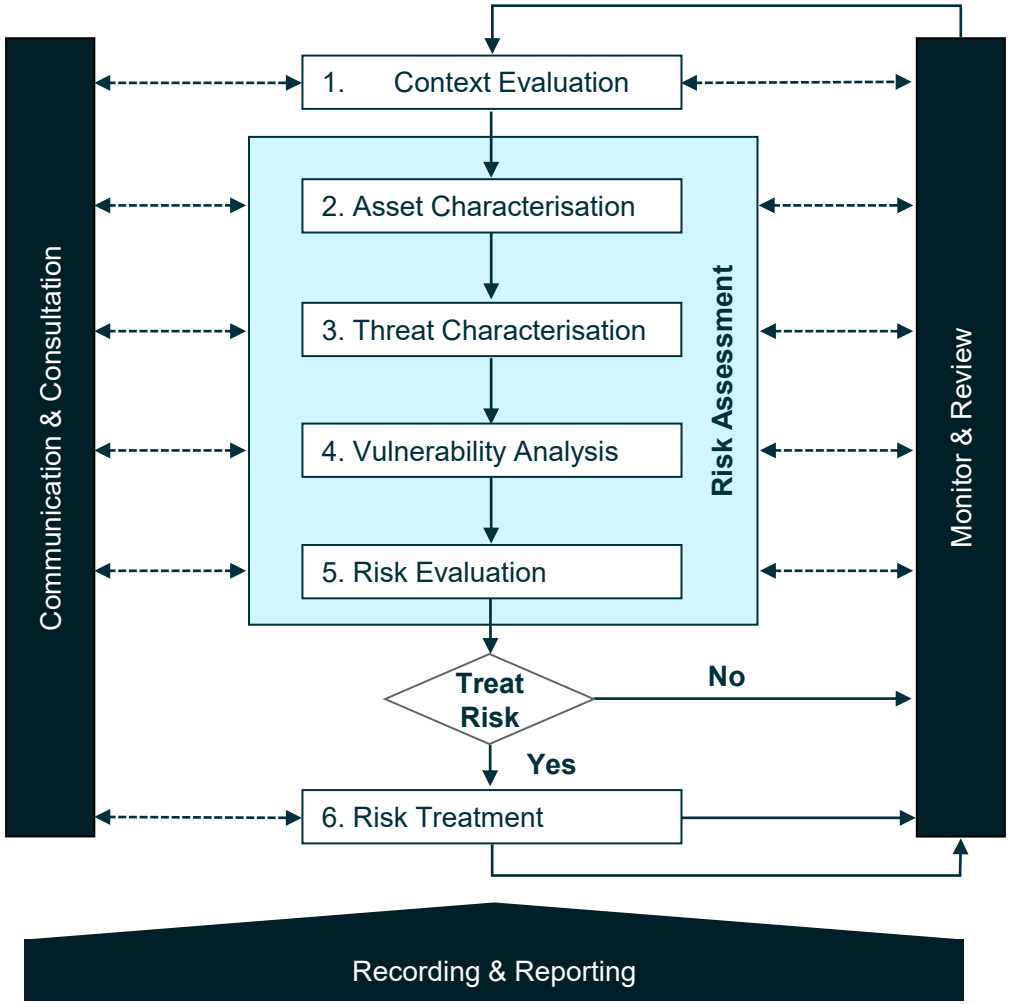
BOSTON SQUARE RISK MATRIX

Consequence	Likelihood				
	Remote	Unlikely	Credible	Likely	Highly Likely
Severe		Medium	High		Very High
Major	Low				
Moderate			Medium		High
Minor		Low			
Minimal	Very Low			Low	Medium

QUALITATIVE RISK-BASED ASSESSMENT

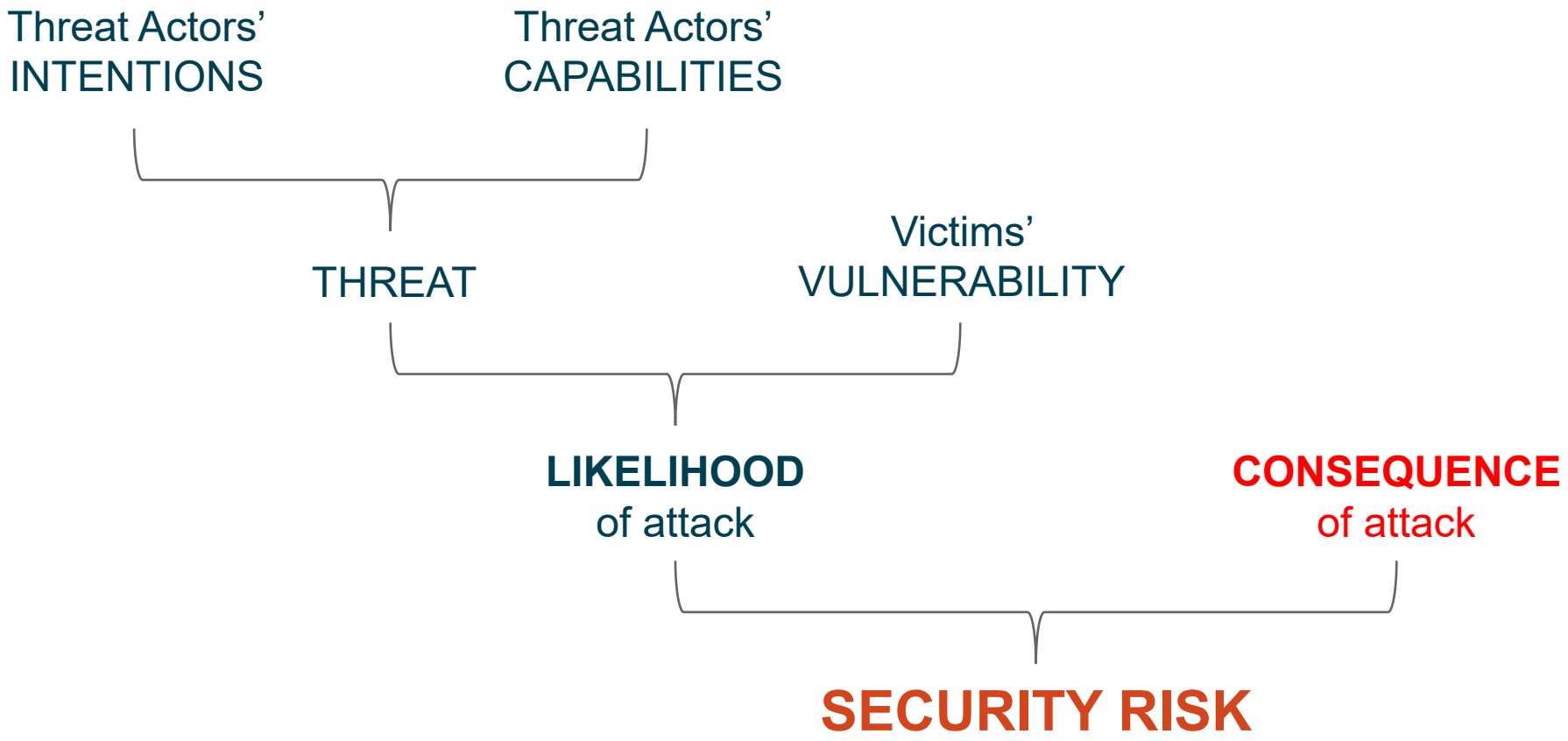
Overview

- Six-step qualitative assessment framework
- Based on ISO 31000:2018
- Understand the organisation – establish the context
- Consequence derived from asset value assessment through stakeholder engagement
- Likelihood based on best available threat information / intelligence and asset vulnerability
- Likelihood can be derived through the iterative **Delphi technique**
- Risk calculated using a schedule and mapped to a Boston Square



QUALITATIVE ASSESSMENT FORMULA

Risk = (TxV)C Threat (T) x Vulnerability (V) = LIKELIHOOD x CONSEQUENCE



MODULE 2

QUALITATIVE TVRA / SRA FORMULA

Likelihood (Threat × Vulnerability) Consequence — a universal model

THREAT

T

The likelihood that a hostile act or security event will occur. Informed by intelligence, threat landscape analysis, site attractiveness and adversary capability and intent assessment.

VULNERABILITY

V

The degree to which the asset or environment is susceptible to a threat – site / design resilience. Assessed through site and GA plan / 3D model surveys, vehicle and pedestrian access analysis and procedural review.

CONSEQUENCE

C

The severity of impact if the threat is realised.
Considers life safety, asset damage, business continuity, revenue generation, regulatory compliance and reputational harm.

RISK = (T × V) C

Each dimension assessed independently using structured criteria before combining into a composite risk rating schedule

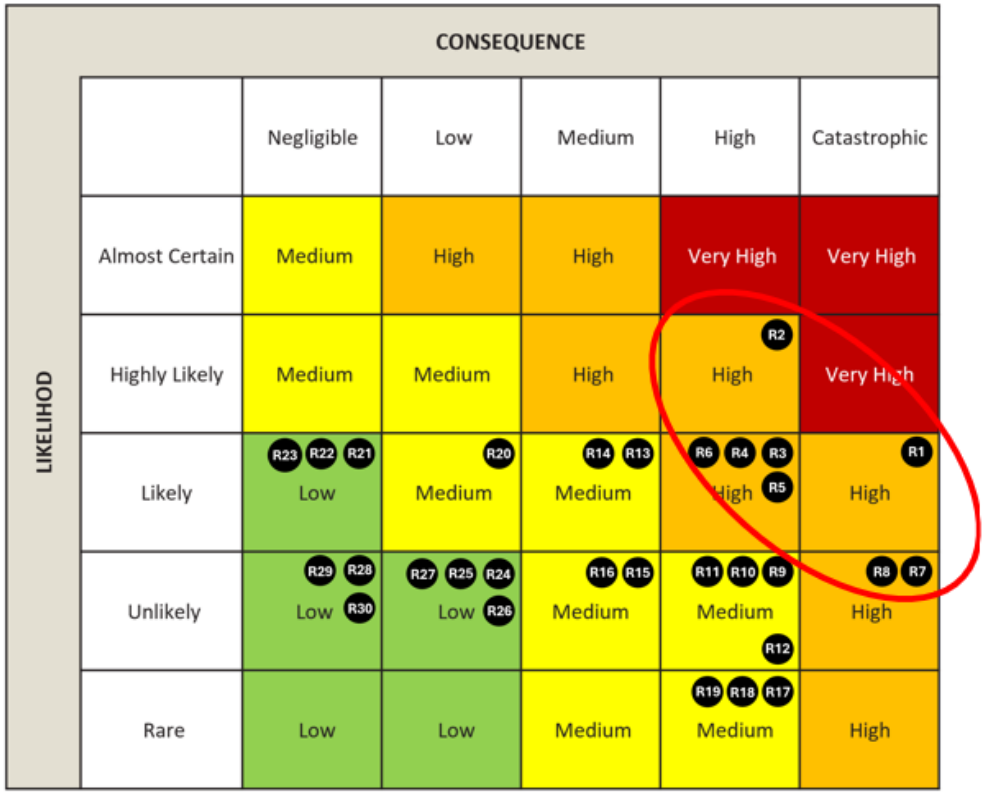
BOSTON SQUARE – PROS & CONS

PROS

- Simple method, easily understood
- Quick and easy to plot security risks
- Expert input can add credibility

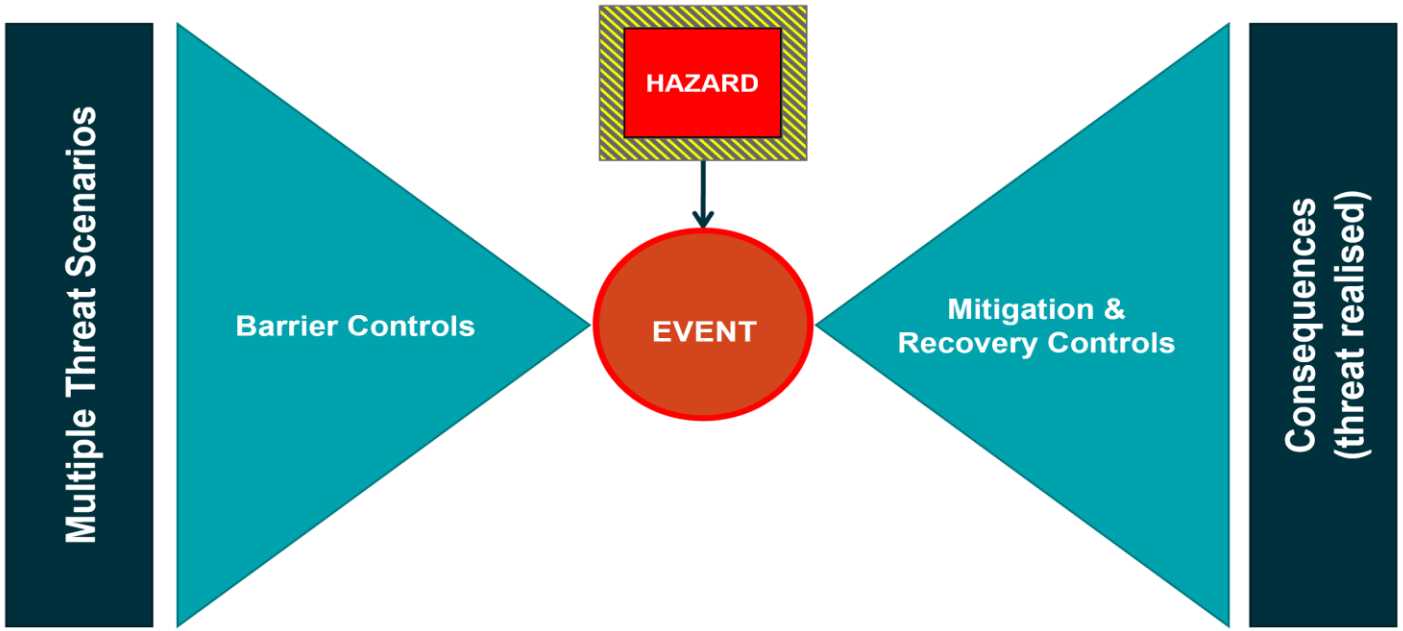
CONS

- Subjective assessment – outcomes may be flawed, or lack credibility if consultants lack knowledge and experience
- 3x3 or 5x5 matrices lack granularity and assigning numbers can be problematic
- Ambiguous outcomes if likelihood and consequence criteria poor
- Risk of excluding high consequence, low likelihood or low frequency events (Saunder's Report Findings)



OTHER QUALITATIVE RISK ASSESSMENT METHODS

BOW-TIE ANALYSIS



03 ANATOMY OF A BREEAM HEA08 SECURITY NEEDS ASSESSMENT

POLL

Module 3

BREEAM Hea 08 – SECURITY NEEDS ASSESSMENT

What the BREEAM credit requires and what it does not

BREEAM New Construction V.7 Context

Hea 08 (Security) is a credit within the Health & Wellbeing category of BREEAM New Construction. It is not a mandatory credit but is frequently targeted for BREEAM Very Good or Excellent ratings. It awards 1 credit for demonstrating that security measures for the building have been considered through a structured assessment process. An exemplary credit is available if the report and design perform against an independent security verification and rating scheme approved by BREEAM (i.e., SABRE, Proctor)

What Hea 08 Requires

- A Security Needs Assessment (SNA) carried out by a suitably qualified security specialist (SQSS) before or at RIBA Stage 2
- Assessment considers likely threats to the building and its users
- Assessment informs the design of security requirements and measures appropriate to context and proportionate to the threat
- Assessor evidences competence (e.g. RSES, CSyP, SBD Accredited Professional or equivalent)
- Assessment report reviewed and considered by the design team
- BREEAM Assessor to independently confirm SNA informs design — evidence of integration
- Any deviation must be supported by a Technical Justification

What Hea 08 Does NOT Specify

- No prescribed methodology — assessor determines the approach
- No requirement for detailed intelligence-led threat assessment
- No requirement for physical site survey evidence or photographs, remote assessment of plans and imagery allowed
- No prescribed rating scales or risk matrix format
- No requirement for typology-by-typology risk register
- No minimum report structure or section requirements
- No mandated review frequency or trigger conditions. However, if design changes, SNA should be updated to remain relevant

Module 3

BREEAM Hea 08 – CREDIT CRITERIA IN DETAIL

BREEAM — the assessor evidence requirements

Hea 08 Criterion	BREEAM Requirement	Evidence Required by BREEAM Assessor
Competent Assessor	Security assessment carried out by or under the direction of a suitably qualified security specialist. BREEAM accepts SABRE SQSS, RSES, CSyP, SBD LC, ASIS CPP/PSP, or demonstrated equivalent competence. The assessor's qualifications must be evidenced.	CV / professional registration evidence submitted to BREEAM Assessor
Security Needs Assessment	A formal assessment identifying the likely threats to the building, its occupants and assets. The assessment must consider the use case for the building, its location, operational context, intended use and occupancy profile.	Signed SNA report provided to design team and BREEAM Assessor
Design Integration	The SNA must demonstrably inform security design measures. The design team must confirm that the SNA recommendations have been reviewed and that design responds to them.	Clear link between threats identified and the mitigation incorporated within eh design. Design team sign-off; specification or drawing reference to SNA; BREEAM Assessor confirmation
Report Review	The SNA report must be reviewed by the design team — not merely received. Evidence of review meeting, action tracker, minutes of meetings, or design team response is expected.	Meeting notes; design team response letter; schedule of SNA recommendations and design response

Key point: BREEAM Hea 08 credits the process and integration, not the depth of the assessment. A lightweight SNA that meets the four criteria above will earn the credit. A full NPSA-standard SRA will also earn it — but earns considerably more besides.

04 SECURITY OVERLAY FOR THE RIBA PLAN OF WORK

POLL

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	**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**	Architectural and engineering information **Spatially Coordinated**	All design information required to manufacture and construct the project completed	Manufacturing, construction and Commissioning completed	Building handed over, **Aftercare** initiated, and **Building Contract** concluded	Building used, operated and maintained efficiently
	If the outcome determines that a building is the best means of achieving the **Client Requirements**, the client proceeds to Stage 1		The brief remains "live" during Stage 2 and is derogated in response to the **Architectural Concept**		Stage 4 will overlap with Stage 5 on most projects	There is no design work in Stage 5 other than responding to **Site Queries**		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 consultant 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 consultant 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)
Security Risk Assessment	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
Security Requirements	N/A	Produced by Client Team	Derogations Reviewed	Reviewed	Review Relevance for Procurement Strategy	Review	N/A	N/A
Security Strategy	N/A	N/A	Produced by Design Team	Updated As Required	Updated As Required	Updated As Required	N/A	N/A
Security Plan	N/A	Review as part of Security Requirements	N/A	N/A	N/A	Produced by Client Team	Updated As Required	Updated As Required

SECURITY DESIGN ACTIVITIES & CORE PROJECT DOCUMENTS

What? (Concerns)

What? & Why? (Needs)

How & Where? (Design)

How? (Operations)

Security Risk Assessment

- Identify threat scenarios
- Set Design Basis Threats (DBTs)
- Risk evaluation
- Security Considerations Assessment (SCA)

Security Requirements

- Basis of Design
- Security Needs
- Operational risk management
- Informs **Project Brief**

Including **Security Plan** considerations

Security Strategy

- Follows full Security Risk Assessment
- How the design will mitigate security risk
- Where - placement of proportionate security treatments
- Value Engineering & Cost-Benefit Analysis

Security Plan

- Governance & accountability policy
- Protective Security Management System
- Security Roles & Responsibilities
- Security Standard Operating Procedures

0 Strategic Definition

1 Preparation and Briefing

2 Concept Design

3 Spatial Coordination

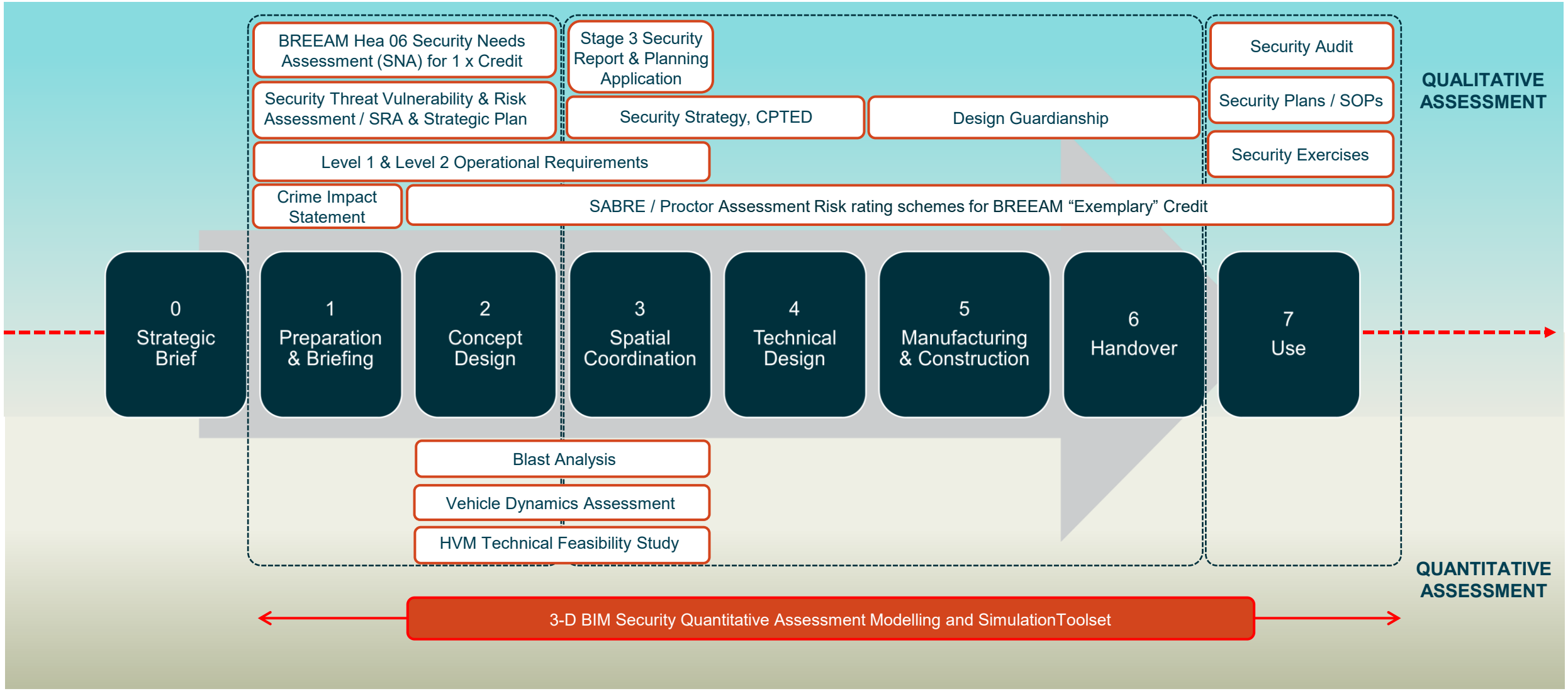
4 Technical Design

5 Manufacturing and Construction

6 Handover

7 Use

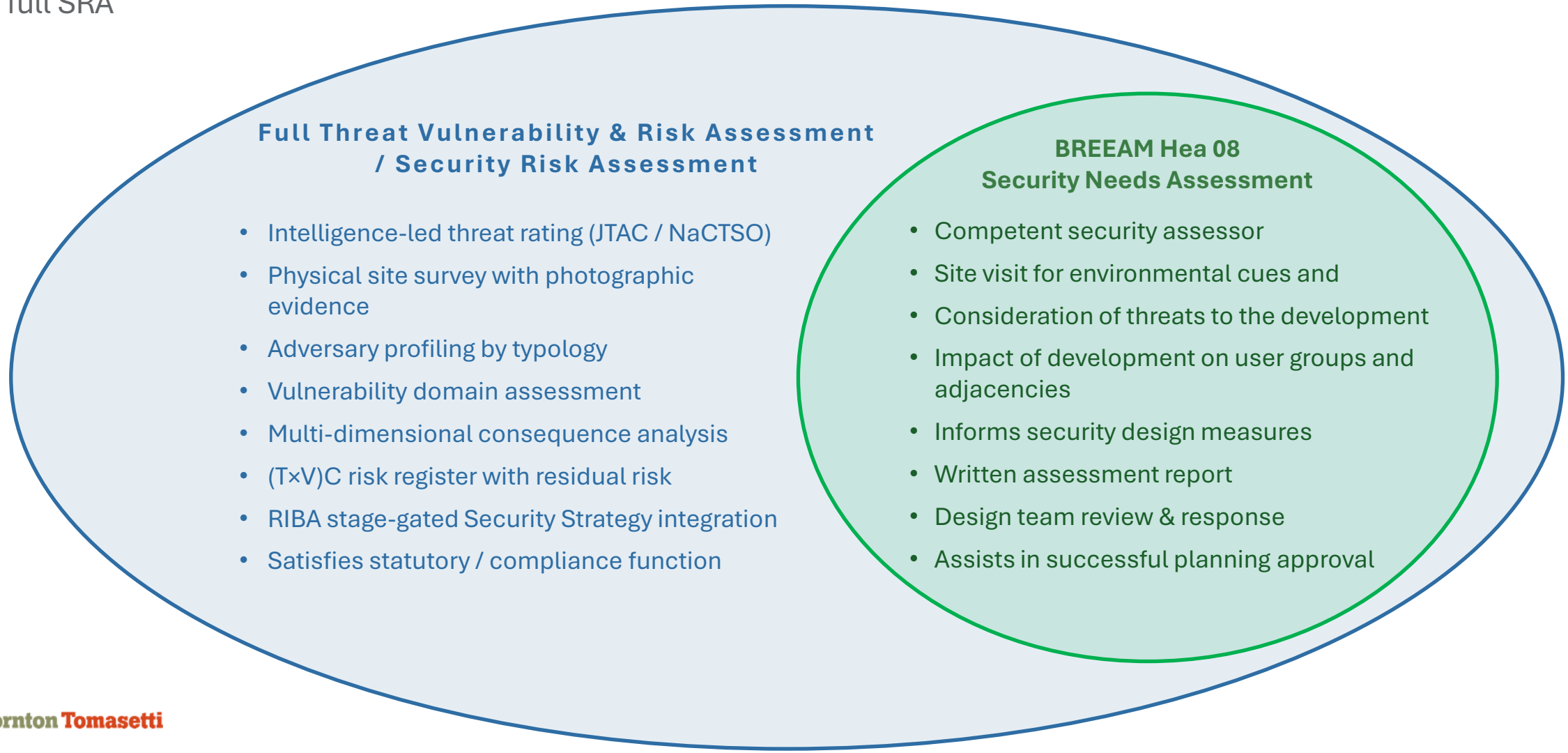
APPLICATION OF TVRA / SRA & SNA IN DESIGN



05 FULL TVRA / SRA vs SNA

SCOPE RELATIONSHIP – TVRA / SRA CONTAINS SNA

The Security Needs Assessment is a subset of the full SRA



FULL TVRA / SRA vs BREAM Hea 08 - COMPARISON

Scope, depth, methodology, outputs and regulatory weight

Dimension	Full SRA (NPSA / RIBA Overlay Standard)	BREEAM Hea 08 Security Needs Assessment
Purpose	Drive all security design and management decisions across project lifecycle	Earn BREEAM Hea 08 credit; evidence that security has been considered in design
Methodology	Structured qualitative security risk assessment with risk rating scales	No prescribed methodology — assessor discretion, so a dependency on security consultant judgement and competency
Threat Assessment	Intelligence-led; adversary profiling – Design Basis Threat	General consideration of likely threats; no intelligence mandate
Vulnerability	Physical site survey; CPTED appraisal; adversary path analysis appreciation;	Not specifically required; nature of building / location considered
Consequence	Multi-dimensional: life safety, asset, BCM, reputational; formal severity scale	Not required; implied within 'likely threats to building and users'
Risk Register	Formal (T×V)C register; composite ratings; residual risk following design treatments; owner; review date	Not required; only needs to 'identify threats' and inform design
Report Structure	Structured report; evidence appendices; assessor credentials section	No prescribed structure; signed report confirming assessment done
RIBA Integration	Required at every RIBA stage gateway; informs Security Strategy and Security System Operational Requirements	Required before RIBA Stage 4 completion for BREEAM credit evidence
Regulatory Weight	Mandated by Martyn's Law – quality of report likely to be assessed post incident	BREEAM credit only — no regulatory or legal compliance function
Review/Currency	Defined review trigger; annual review typical; post-incident mandatory, changes in technology, use case, threat	No review requirement specified post-credit award

06 TVRA / SRA / SNA INTEGRATION IN PRACTICE

INTEGRATION IN PRACTICE

Using a full SRA to discharge BREEAM Hea 08 and drive RIBA-stage design

1. Single Assessment, Dual Function

A full SRA structured to the RIBA Overlay standard will simultaneously satisfy BREEAM Hea 08. Structure the report so that a clearly labelled section constitutes the BREEAM Security Needs Assessment — the BREEAM Assessor can then extract precisely what they need.

2. BREEAM Evidence Pack

Prepare a standalone BREEAM Hea 08 evidence document that draws from the full SRA: (a) assessor credentials, (b) executive summary of threat considerations, (c) design team review confirmation, (d) schedule of SRA recommendations and design responses. This is submitted to the BREEAM Assessor separately from the full SRA (which may be commercially confidential).

3. Design Team Integration Protocol

Hold a design team briefing at Stage 2 to present SRA findings. Minute the meeting. Record design decisions that respond to specific risk register references. This meeting minutes document is the most powerful piece of BREEAM Hea 08 evidence — and the most commonly missing.

4. RIBA Gateway Discipline

Do not allow the Stage 2 or Stage 3 design sign-off to proceed without an updated SRA. Insert SRA sign-off as a project gateway condition in the project programme from Stage 0. This prevents the SRA becoming a retrospective exercise.

Module 6

STRUCTURING A DUAL PURPOSE SRA / SNA REPORT

How to write a full SRA that simultaneously discharges BREEAM Hea 08

1 **Executive Summary**

Overall risk rating; top risks; critical design recommendations. ← Hea 08: extract for BREEAM Assessor as standalone summary

2 **Introduction, Scope, Methodology & Assessor Credentials**

Assessment boundary; risk assessment methodology; rating scales. ← Hea 08: SQSS professional / assessor qualifications evidence lives here

3 **Asset Characterisation - Context / Building Profile**

Site description; occupancy – user groups; use class; regulatory context; BREEAM project reference

4 **Threat Assessment**

Intelligence-led; Adversary profiling; Design Basis Threats; source hierarchy.

5 **Vulnerability Analysis**

Site survey / visit; CPTED; physical, procedural, technological, processes, operational, governance.

6 **Consequence Assessment**

Multi-dimensional; life safety, asset, revenue generation, regulatory, reputational, environmental, Business Continuity Management.

7 **Risk Register & Matrix**

(T×V)C ratings; composite risk; heat map; residual risk. [Full SRA only — distilled into design recommendations for Hea 08]

8 **BREEAM Hea 08 — Design Integration Summary**

Dedicated Hea 08 section: key threats considered; design measures arising; design team review confirmation. To be submitted to BREEAM Assessor

9 **Treatment Plan & Design Recommendations**

Risk-referenced recommendations with design response cross-reference. ← Hea 08: schedule of recommendations and design responses

App **Appendices, Evidence & Source Log**

Survey photographs; drawings; checklist evidence; intelligence source log, Minutes of Meeting (i.e., with CTSA).

Green = section typically included in BREEAM Hea 08 evidence submission

Blue = Full SRA content; typically, confidential / not submitted to BREEAM

COMMON PITFALLS – HOW TO AVOID THEM

Conflating SNA with SRA

Commissioning only a BREEAM Hea 08 SNA for an Enhanced Tier venue, believing it satisfies the security risk management obligation – results in an insufficient level of detail

No Design Team Briefing

Delivering the SRA report without a structured design team briefing and recorded design response. BREEAM Hea 08 requires evidence of review — and the SRA has no value if design teams don't act on it, or the design changes.

Late Security Appointment

Appointing the security consultant at Stage 3 or later means the SRA is retrospective — it justifies design rather than informing it and influencing it. The Security Overlay for the RIBA PoW advocates security input from Stage 0.

Stale SRA at Gateway

Issuing the Stage 3 Security Strategy against a Stage 2 SRA that has not been updated to reflect design development. The risk register must reflect the current design, not the concept stage geometry – new vulnerabilities may have evolved.

Two Separate Documents

Producing a full SRA and then a separate, inconsistent SNA for BREEAM. Creates evidential conflicts and doubles the effort. Structure the SRA with an integrated Hea 08 section from the start.

Scope Mismatch

SRA scope limited to CT threats for a venue that also requires protection from protest, theft, fraud, and insider risk. The full SRA must cover all material threat typologies for the asset type, unless a specific bound scope necessary and agreed.

SESSION SUMMARY

SUMMARY – KEY TAKEAWAYS

Six critical points for built environment security practice

01 The RIBA Security Overlay requires a stage-appropriate SRA at every Plan of Work gateway — not once at Stage 2 alone. The SRA evolves with the design.

02 A full SRA is an intelligence-led, site-surveyed, multi-dimensional risk assessment with a formal risk register. It is substantially more than the Hea 08 Security Needs Assessment content.

03 BREEAM Hea 08 credits process and integration — SQSS competent assessor, written report, design team review and design response. It does not validate the depth of the threat analysis – consultant judgement & competency dependent.

04 A full SRA will always satisfy BREEAM Hea 08. Hea 08 SNA report alone will not satisfy Martyn's Law, or the RIBA Overlay for a complex asset.

05 Structure the full SRA with a dedicated Hea 08 integration section from the outset. One document, dual purpose — no inconsistency, no duplication of effort.

06 Appoint the security consultant at Stage 0 or Stage 1. Late appointment makes the SRA retrospective — it cannot then perform its primary function of informing design decisions.

THE SECURITY INSTITUTE

JULY 22, 2026

QUALITATIVE SECURITY RISK ASSESSMENT

For the Built Environment – Overview

Q & A

David Buston CSyP, FSyI, MAPM

Protective Design & Security

Romsey

- dbuston@ThorntonTomasetti.com
- +44 (0) 1794 528441

SESSION SUMMARY

REFERENCES: STANDARDS & METHODOLOGIES

Standards, industry guidance & 3rd party audit

- ISO 31000:2018 – Risk management – Guidelines
- ISO 31010:2019 – Risk assessment techniques
- ISO 31073:2022 – Risk management – Vocabulary
- BS 16000:2015 Security Management. Strategic and operational guidelines
- **NPSA** Protective Security Risk Management – 8-Step process, Role-based Protective Security Risk Assessment Guidance (Insider) & 7-Step Risk assessment process (Cyber)
- **NaCTSO** 5-Step Risk assessment process – ProtectUK
- **BREEAM Hea 08 New Construction V.7 Credits:**
  - Security Needs Assessment (SNA) – 1 Credit
  - Risk rating schemes for BREEAM Exemplary Credit:
    - **SABRE** – Security Assessment by the Building Research Establishment. An audit process that evidences security resilience and governance
    - **Proctor** – Built Environment Security Rating Scheme

Security risk methodologies

- **American Petroleum Institute (API) 780** Security Risk Assessment (SRA) – Oil & Gas (O&G)
- **Bow-Tie Analysis** – Civil Aviation / O&G
- **CARVER +Shock** – Target Attractiveness (USA)
- **International Ship & Port Facility Security (ISPS) Code**. Ship Security Assessment / Port Facility Security Assessment
- **PRISM** – proprietary for the energy sector
- **UK Government Probability Yardstick**
- **Vital Area Assessment** – Civil Nuclear
- **Vulnerability Self-Assessment Tool** (VSAT) – Poole RE

THANK YOU