PREMSIGHT

A Counter-drone threat and vulnerability evaluation

Site-specific template built on the four tasks in NPSA guidance, Countering Threats from Uncrewed Aerial Systems: Assessing the Threat and Vulnerability.

Counter-Drone Site Risk Assessment Pack (UK)

Built on NPSA guidance, Countering Threats from Uncrewed Aerial Systems

Version 1.0 | Law and guidance checked 17 November 2026

SAMPLE PAGES

Sample pages. Sections 0 to 2 of the threat evaluation and its scoring matrix. The last page lists what the full pack adds.

How to use: fill the blue [PLACEHOLDERS], delete the rows marked EXAMPLE, and keep the section order. It follows NPSA Tasks 1 to 4 so a reviewer, police Counter Terrorism Security Adviser (CTSA) or insurer can trace your work to the guidance. NPSA does not prescribe a scoring method and says the results should feed the site's existing risk process; the matrix in section 4 is a default you can swap for the client's own.

0. Assessment details

Field	Entry
Client and site name	[CLIENT_NAME], [SITE_NAME]
Site address and grid reference	[ADDRESS], [GRID_REF]
Site type	[E.G. NATIONAL INFRASTRUCTURE / SENSITIVE SITE / CROWDED PLACE / COMMERCIAL]
Assessor and firm	[ASSESSOR_NAME], [FIRM_NAME], SIA ACS ref [ACS_REF]
Senior risk owner at the site	[NAME, ROLE]
Date of desk work / ground survey	[DATE] / [DATE]
Version and status	v[0.1] [DRAFT / ISSUED]
Existing site security risk assessment referenced	[DOCUMENT TITLE, DATE]
Classification / handling	[E.G. OFFICIAL-SENSITIVE OR CLIENT CONFIDENTIAL]

0.1 Existing protective security (baseline)

NPSA asks you to understand what is already in place before starting. Record it here so later sections only add what is missing.

Measure	In place?	Notes (coverage, gaps, who runs it)
Assets covered from view (tree lines, screening)	[Y/N/PART]	[NOTES]
Assets concealed or disguised (netting, roofing)	[Y/N/PART]	[NOTES]
Assets protected by design or construction	[Y/N/PART]	[NOTES]
Information security measures for sensitive information	[Y/N/PART]	[NOTES]
CCTV, lighting, patrols covering perimeter and approaches	[Y/N/PART]	[NOTES]

Measure	In place?	Notes (coverage, gaps, who runs it)
Any drone detection (DTI) system already installed	[Y/N]	[SYSTEM, COVERAGE, DATA HELD]

1. Stakeholders, roles and risk ownership (NPSA Task 1)

Name who owns the drone risk and who else adds to it or helps reduce it. Ownership can vary by scenario; record that in the last column.

Stakeholder	Name / contact	Role in this assessment	Owns which risks?
Senior risk owner	[NAME]	Accepts residual risk, signs off plan	[ALL / SCENARIO IDS]
Site security manager	[NAME]	[ROLE]	[ ]
Site operations / asset owners	[NAME]	Explain how each asset works and fails	[ ]
Health and safety lead	[NAME]	Safety-related drone risks	[ ]
Police: local force CTSA	[NAME, FORCE]	Threat information, launch site support, response	n/a
Local authority (land, transport, planning)	[NAME]	[ROLE]	n/a
Public transport operators nearby	[NAME]	[ROLE]	n/a
Neighbouring businesses / landowners	[NAME]	Access to likely launch sites	n/a
Local flying clubs	[NAME]	Legitimate flying nearby; deconfliction	n/a

Police drone use: record whether the local force flies drones near the site and how sightings will be deconflicted. [ANSWER]

2. Threat picture and critical assets (NPSA Task 2)

2.1 Threat actors

Mark each actor relevant or not and say why. Capability drives the launch ranges you use in section 3: a reckless user flies close and overtly; a hostile state actor may fly from further away and knows the security measures.

Actor (NPSA list)	Relevant?	Why / evidence and source	Assumed capability
Reckless or negligent users	[Y/N]	[EVIDENCE, SOURCE]	[LOW/MED/HIGH]
Journalists and others conducting unauthorised surveillance	[Y/N]	[ ]	[ ]
Unlawful protesters	[Y/N]	[ ]	[ ]
Serious and organised criminals / criminals	[Y/N]	[ ]	[ ]
Terrorists	[Y/N]	[ ]	[ ]
Hostile state actors	[Y/N]	[ ]	[ ]

Threat information gathered (NPSA list): local, national and international reporting from police contacts, NPSA adviser and partners; the site's all-threat picture and how a drone could deliver it; historic drone activity in and around the site (hostile, reckless and legitimate); output from any installed detection system. Record each source and date: [SOURCES]

2.2 Threat methodology

For each method, answer the two NPSA questions: why would an attacker prefer a drone here, and how is the site more exposed to a drone than to another method?

Method	Applies?	Why a drone here? Why more exposed?
Disruption (over or near the site, stopping normal operations)	[Y/N]	[ANSWER]
Surveillance (images, data, perch and stare)	[Y/N]	[ANSWER]
Delivery of a payload (delivering or removing items)	[Y/N]	[ANSWER]
Drone as a kinetic weapon (modified or unmodified)	[Y/N]	[ANSWER]
Cyber attack delivered by drone	[Y/N]	[ANSWER]

2.3 Likely drone capability

Factor	Assessment for this site
Type: rotary wing (hovers, small launch area, shorter endurance) or fixed wing (longer range and speed, larger launch area, cannot hover)	[RW / FW / BOTH]
Payload needed for the methods above	[ ]
Speed and endurance needed	[ ]
Range from likely launch areas	[ ]

Factor	Assessment for this site
Operating environment (open rural, where performance is closer to maker claims, or complex urban, where it is often lower)	[ ]

2.4 Critical assets

List the assets whose compromise would significantly harm the site's operation. Assets can sit inside or outside the perimeter. Plot each on the site map and give it a reference.

Ref	Asset	Type (physical, information, people, service, crowded place)	Inside / outside perimeter	Map ref
EXAMPLE	Loading yard during deliveries	Service / people	Inside	M-02
AS-01	[ASSET]	[TYPE]	[ ]	[ ]
AS-02	[ASSET]	[TYPE]	[ ]	[ ]
AS-03	[ASSET]	[TYPE]	[ ]	[ ]

2.5 Threat scenarios

Combine who, how, with what and where into scenarios. These are the units you score in section 4 and plan against in the mitigation roadmap.

ID	Actor	Method	Drone type	Target asset	Likely launch area
EXAMPLE	Reckless user	Disruption	Small RW, off the shelf	Loading yard (AS-01)	Public footpath, LS-03, 500 m zone
S1	[ ]	[ ]	[ ]	[ ]	[ ]
S2	[ ]	[ ]	[ ]	[ ]	[ ]
S3	[ ]	[ ]	[ ]	[ ]	[ ]

4. Scoring (extract)

Each scenario gets a likelihood and an impact. The risk level is read from this matrix, never estimated.

Likelihood / Impact	Low impact	Medium impact	High impact
High likelihood	**MEDIUM**	**HIGH**	**CRITICAL**
Medium likelihood	**LOW**	**MEDIUM**	**HIGH**
Low likelihood	**LOW**	**LOW**	**MEDIUM**

What the full pack adds

The full evaluation continues with Task 3 launch site analysis (500 m, 1,000 m and 1,500 m launch range zones, desk exercise, ground survey with landowner permissions), the scored scenario register, consolidation into a C-UAS plan, review triggers and sign-off. Around it sit seven more working files.

File	Format	What it does
A. Threat and vulnerability evaluation	DOCX	The core assessment: NPSA Tasks 1 to 4, scored
B. Site survey checklist	XLSX	41 desk and ground checks, launch site log, risk level looked up from the matrix automatically
C. Site confirmation register	XLSX	27 points the client must confirm in writing, with days-open tracking
D. Mitigation roadmap	DOCX	Measures in NPSA order, linked to scenarios, owners and dates
E. Roles and legal limits note	DOCX	What a private firm may and may not do about drones in UK law, with sources
F. Client report template	DOCX	The deliverable your client receives
Start here and Sources	DOCX	Order of work, licence, every source with the date checked

> Licensed per firm, including use on paid client work. £149 + VAT.

Built on NPSA guidance (page last updated 22 September 2026) and ProtectUK C-UAS guidance, both checked 17 November 2026. This template is not NPSA or police endorsed and is not legal advice.