A PROPOSED METHODOLOGY FOR THE SECURITY SECTOR

The Operational Capability Framework

Measuring Speed Through TFOI and Quality Through the Operational Capability Review

Kevin Stanley

July 2026

A conceptual framework offered for professional and academic review.
Not presented as an established industry standard or a finished body of research.

Contents

Chapter 1: Introducing Operational Intelligence **1**
1.1 Definition . . . 1
1.2 Purpose . . . 1
1.3 Scope . . . 2
1.4 Contribution . . . 2
1.5 Structure of This Publication . . . 2

Chapter 2: Operational Uncertainty **3**
2.1 The Nature of Operational Uncertainty . . . 3
2.2 Operational Uncertainty in Practice . . . 3
2.3 Why Resources Alone Do Not Resolve Uncertainty . . . 4
2.4 From Uncertainty to Operational Intelligence . . . 4

Chapter 3: Operational Information and Decision-Making **5**
3.1 Operational Context . . . 5
3.2 Operational Information and Operational Intelligence . . . 6
3.3 The General Decision-Making Pattern . . . 7
3.4 The Operational Information Network . . . 7
3.5 The Evolution of Operational Awareness . . . 8
3.6 Information Quality . . . 9
3.7 Operational Metric — Time to First Operational Intelligence (TFOI) . . . 9

Chapter 4: Operational Capability Framework (OCF) **12**
4.0 Introduction . . . 12
4.1 Why Capability Matters . . . 12
4.2 Operational Capability Review (OCR) . . . 13
4.2.1 Capability Domains . . . 13
4.2.2 Conducting the Review . . . 14
4.2.3 TFOI and OCR Together . . . 14
4.3 A Note on Future Development . . . 15
4.4 Summary . . . 15

Chapter 5: Operational Application of the Operational Capability Framework **16**
5.1 Purpose . . . 16
5.2 Operational Decision Cycle . . . 16
5.3 Time to First Operational Intelligence (TFOI) . . . 17
5.3.1 TFOI is Source-Agnostic . . . 17
5.3.2 Worked Example: Aerial Platform Deployment . . . 18
5.3.3 Observation Time and Confidence . . . 20
5.4 Comparative Operational Scenario . . . 21
5.5 Comparative Analysis . . . 23
5.6 The Relationship Between OCF and TFOI . . . 24

Chapter 6: Operational Capability Framework Assessment and Resource Allocation **25**
6.1 Purpose . . . 25
6.2 Principles of Proportionate Capability . . . 26
6.3 Operational Capability Framework Assessment Factors . . . 26
6.4 Capability Escalation Model . . . 27
6.5 Selecting Capability Enhancements . . . 28
6.6 Worked Example . . . 28
6.7 Relationship to TFOI . . . 29

Chapter 7: Implementation **30**
7.1 Purpose . . . 30
7.2 Implementation Principles . . . 30
7.3 Phased Adoption . . . 31
7.4 Training and Competency . . . 31
7.5 Documentation and Record-Keeping . . . 32
7.6 Governance and Review . . . 32
7.7 Automated Data Collection . . . 32

Chapter 1: Introducing Operational Intelligence

1.1 Definition

> Operational Intelligence (OI) is the discipline concerned with the acquisition, interpretation and exploitation of information to support timely, proportionate and effective decision-making during operational activity.

Operational Intelligence is not a technology, a piece of equipment, or a specific method of gathering information. It is a way of thinking about operational decision-making — one that treats the speed and quality of information as central to operational effectiveness, rather than as a secondary consideration behind staffing levels, equipment, or procedure.

This publication is concerned with how that discipline applies specifically within the security sector, though the underlying principle is not unique to it. The College of Policing's National Decision Model places the gathering of information ahead of assessing threat and risk; Colonel John Boyd's OODA Loop, developed for combat decision-making, rests on the premise that the party able to observe and process information faster gains a decisive advantage. Operational Intelligence applies an equivalent principle to private security operations.

1.2 Purpose

This publication proposes a structured way of thinking about operational capability within the security sector — one built around a simple premise: an organisation's effectiveness is shaped as much by the speed and quality of the information available to its decision-makers as by the resources it deploys.

From this premise, the publication introduces the Operational Capability Framework (OCF), a structured methodology for assessing and improving operational capability, together with two measurable outputs the framework produces: Time to First Operational Intelligence (TFOI), an objective timing metric, and the Operational Capability Review (OCR), a qualitative assessment of an organisation's intelligence practice over time.

This publication is presented as a proposed conceptual framework, offered for professional and academic review. It is not put forward as an established industry standard, a validated measurement system, or a finished body of research.

The ideas, models and metrics that follow are intended to encourage discussion, scrutiny and empirical testing within the security sector, and to invite contribution from practitioners, researchers and organisations willing to challenge, refine or test them against real operational practice. Where a specific claim, figure or model requires further validation, this is noted at the relevant point in the text; that qualification should be read as applying throughout the publication, not only where it is explicitly repeated.

1.3 Scope

This publication is concerned with operational decision-making within private security operations — including static guarding, keyholding, mobile patrol response, event security, and the monitoring and response functions that support them. It focuses specifically on the acquisition and use of operational intelligence, and on the framework, metrics and assessment tools proposed to measure and improve it.

This publication does not prescribe specific technology, mandate particular equipment, or argue that any single capability enhancement — aerial or otherwise — should be adopted as standard practice. Where specific technologies are discussed, including aerial platforms, they are presented as illustrative examples of capability enhancements that may be justified under the framework in particular circumstances, not as the subject of the framework itself.

1.4 Contribution

This publication contributes to the security sector in three ways. First, it proposes a distinction between operational activity and operational capability, arguing that traditional performance metrics measure the former without necessarily capturing the latter. Second, it introduces TFOI as an objective, measurable timing metric for the speed of operational intelligence acquisition — something existing sector metrics do not directly capture. Third, it introduces a structured, judgement-supporting method — the Operational Capability Framework Assessment — through which supervisors can determine when enhanced operational capability is proportionate to assessed risk, without reducing that judgement to an automated or purely numerical process.

1.5 Structure of This Publication

This publication is structured as follows:

- Chapter 2 examines why operational decision-making is inherently difficult, independent of an organisation's resources or capability — establishing operational uncertainty as the problem this publication's framework exists to address.
- Chapter 3 examines how raw operational information is transformed into operational intelligence, and introduces the general decision-making pattern that underpins effective operational response.
- Chapter 4 introduces the Operational Capability Framework in full, together with its two measurable outputs: TFOI and the Operational Capability Review.
- Chapter 5 demonstrates the framework's application through comparative operational scenarios, and introduces the confidence model used to determine when operational intelligence is sufficient to act upon.
- Chapter 6 sets out the Operational Capability Framework Assessment, the structured method by which supervisors determine when enhanced operational capability is justified.
- Chapter 7 addresses implementation: how an organisation adopts the framework in practice, including phased adoption, training, documentation and governance.

Chapter 2: Operational Uncertainty

2.1 The Nature of Operational Uncertainty

Every operational incident begins the same way: with more unknowns than knowns.

An alarm activates. A member of the public reports suspicious activity. A patrol officer notices something out of place. In each case, the individual or organisation responding does not yet know what is actually happening. They know only that something might be happening, and that a decision — however small — now has to be made in the absence of complete information.

This is not a failure of process, training, or resourcing. It is the starting condition of almost every operational incident a security organisation will ever face. Uncertainty is not something that occasionally complicates operational decision-making; it is the environment within which operational decision-making always takes place.

2.2 Operational Uncertainty in Practice

The specific uncertainties present at the start of an incident vary, but they are rarely trivial. A single alarm activation may leave a responding officer or control room without answers to questions such as:

- Is the alarm genuine, or a false activation?
- Is anyone still present on site?
- If so, how many individuals are involved?
- Which entrance or area of the premises is affected?
- Are weapons or other hazards present?
- Are members of the public nearby or at risk?
- Is there a fire, chemical hazard, or other environmental danger?
- Has anyone already been harmed?

None of these questions can be answered by the alarm activation alone. Each represents a gap between what the organisation knows and what it needs to know before it can determine a proportionate and effective response. In many incidents, several of these uncertainties exist simultaneously, and a decision-maker must act — or decide not to act — before most or all of them are resolved.

2.3 Why Resources Alone Do Not Resolve Uncertainty

It is tempting to assume that uncertainty is primarily a resourcing problem — that an organisation with more staff, more equipment, or more advanced technology will simply have less uncertainty to contend with. This is not necessarily true.

Additional personnel deployed without additional information does not reduce uncertainty; it merely places more people into an uncertain situation. A responding officer dispatched to an alarm activation faces exactly the same unanswered questions whether they attend alone or as part of a larger team, unless something has also changed about what is known before they arrive. Uncertainty is resolved by information reaching a decision-maker in a form they can act upon — not by the presence of additional resources on their own.

This distinction matters, because it reframes the purpose of any capability an organisation might introduce. The value of a given resource — a person, a system, a piece of technology — lies not in its presence, but in whether it reduces the specific uncertainties present in a given incident, and how quickly it does so.

2.4 From Uncertainty to Operational Intelligence

Operational uncertainty cannot be eliminated. Every incident will always begin with some gap between what is known and what needs to be known. What can be influenced is how quickly, and how reliably, that gap closes.

This is the problem Operational Intelligence exists to address. Operational Intelligence exists to reduce uncertainty — not to remove it entirely, but to narrow it sufficiently, and quickly enough, that an informed, proportionate operational decision becomes possible.

The following chapter examines how this happens in practice: how raw operational information is gathered, assessed, and transformed into operational intelligence capable of supporting that decision.

Chapter 3: Operational Information and Decision-Making

"Operational information describes what is known. Operational intelligence is what allows that knowledge to be acted upon."

Chapter Objective

The purpose of this chapter is to establish why operational information represents one of the most valuable assets available within modern security operations.

It examines how information is transformed into operational intelligence, how operational intelligence supports effective decision-making, and why every significant technological advancement adopted by the security industry has ultimately served one common purpose: improving the quality, accuracy and timeliness of information available to decision-makers.

This is not a claim unique to the security industry. The College of Policing's National Decision Model (NDM) — the framework UK police forces use to structure operational decisions — places gathering information and intelligence as its first step, ahead of assessing threat and risk. Colonel John Boyd's OODA Loop, developed for combat decision-making and now applied across defence, cybersecurity and business, rests on an equivalent premise: the party that can observe and process information faster and more effectively than its counterpart gains a decisive operational advantage. By establishing these principles, this chapter provides the operational framework against which the capability enhancements discussed in later chapters — including, but not limited to, aerial platforms — will be evaluated.

3.1 Operational Context

Chapter 2 established that operational uncertainty is the starting condition of every security operation, and that this uncertainty cannot be resolved by resourcing alone. This principle applies equally to a lone security officer conducting a perimeter patrol and to a control room coordinating multiple operational resources across numerous sites.

Regardless of scale, every security operation follows the same fundamental process: information is gathered, its significance is assessed, a decision is made, and an operational response follows. Technology does not replace this process — it enhances it by improving the quality, timeliness and availability of the information upon which decisions are based.

Operational Principle
Operational effectiveness is determined not solely by the quantity of resources available, but by the quality of the information directing them. A well-resourced response guided by poor information will consistently underperform a modest response guided by accurate, timely information — a principle demonstrated directly in Section 3.5.

3.2 Operational Information and Operational Intelligence

Within operational environments, the terms information and intelligence are frequently used interchangeably. For the purposes of this publication, a distinction is drawn between the two — one that mirrors the College of Policing's National Intelligence Model (NIM), which describes a structured intelligence cycle through which raw information is assessed and converted into intelligence capable of supporting operational decisions.

Operational Information consists of individual observations, reports, recorded data or sensor outputs describing an operational environment. Examples include:

- A CCTV operator observing an individual entering a restricted area
- A patrol officer reporting an unsecured gate
- A GPS system confirming the location of a mobile response vehicle
- A member of the public reporting suspicious behaviour

Operational information describes what is known.

Operational Intelligence is created when that information has been assessed, verified where appropriate, placed into operational context, and used to support decision-making.

Operational Information	Operational Intelligence
Male wearing a red jacket observed near Gate 3.	CCTV confirms the individual has attempted to access a restricted area. The nearest patrol has been identified and deployed accordingly.

The distinction is significant. Information alone rarely determines an operational response; operational intelligence enables informed decisions.

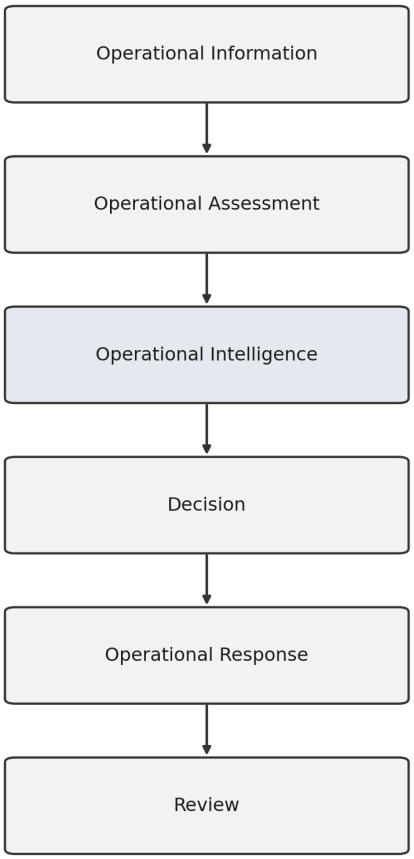


Figure 3.1 — Transformation of Operational Information

3.3 The General Decision-Making Pattern

Every security operation follows the same fundamental cycle:

Observe → Assess → Decide → Act → Review

This is a security-specific expression of a decision pattern used well beyond the industry: it mirrors both the NDM's gather-assess-respond-review structure and Boyd's Observe-Orient-Decide-Act loop. The cycle applies regardless of context — static guarding, keyholding, mobile patrols, event security, CCTV monitoring, alarm response, or critical infrastructure. Incomplete information increases uncertainty at every stage that follows it; relevant information reduces that uncertainty and enables confident decision-making.

This general pattern is formalised specifically for the Operational Capability Framework in Chapter 5, which sets out a more detailed operational decision cycle built around the acquisition and measurement of operational intelligence.

3.4 The Operational Information Network

No single information source provides complete situational awareness. Modern security operations instead depend on integrating information from multiple sources, including:

- Security Officers, Mobile Patrol Units and Supervisors
- Control Room Operators
- CCTV Systems and Access Control Systems
- GPS Vehicle Tracking and NFC Patrol Verification
- Body Worn Video and Intruder Alarm Systems
- Members of the Public and Emergency Services

Each contributes only part of the operational picture. Operational intelligence is created through the assessment, integration and communication of these sources — not through reliance on any individual technology.

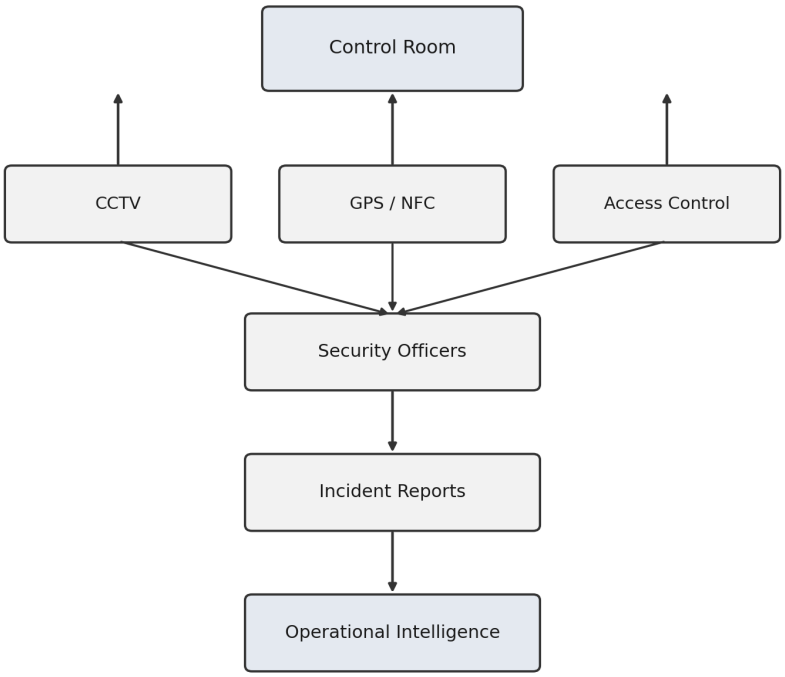


Figure 3.2 — Operational Information Network

3.5 The Evolution of Operational Awareness

The security industry has continually evolved through improving operational information:

- GPS tracking improved officer welfare and deployment awareness
- Electronic patrol verification improved accountability
- Body Worn Video improved evidential integrity and transparency
- CCTV improved continuous observation
- Access control systems improved awareness of occupancy and movement

None of these technologies replaced the security professional. They improved the information available to them.

Operational Observation 01 — The Value of Precise Operational Information
Context. During a large public event deployment, a medical response resource was positioned approximately two minutes from a casualty requiring assistance.
Observation. The initial radio transmission indicated assistance was required but lacked sufficient location accuracy for the responding crew to identify the casualty's precise location. Although physically close to the incident, the responding resource required approximately three minutes to locate the casualty. Following the transmission of precise location information, the same responding resource reached the casualty in less than one minute.
No additional personnel were deployed. No additional equipment was introduced. The responding resource did not become more capable. The only operational variable that changed was the quality and precision of the operational information communicated.
Operational Analysis. This observation demonstrates that operational effectiveness can often be improved through better information rather than additional resources. A unit stationed two minutes away is only a two-minute response if the information directing it is accurate enough to be acted upon immediately — inaccurate or vague information can turn a two-minute asset into a three-minute delay, and at scale, across a large event or critical site, that gap compounds every time it happens.

3.6 Information Quality

Effective operational information should possess five characteristics:

Accurate · Relevant · Timely · Reliable · Clearly Communicated

The objective is not to collect the greatest quantity of information. The objective is to ensure that the right information reaches the right decision-maker at the right time. Information overload may impair operational decision-making just as significantly as insufficient information.

3.7 Operational Metric --- Time to First Operational Intelligence (TFOI)

Definition. The elapsed time between the initial notification of an incident and the point at which sufficient operational intelligence has been obtained to support an informed operational decision. This definition, and the confidence model used to determine when intelligence is sufficient, are set out in full in Section 5.3.

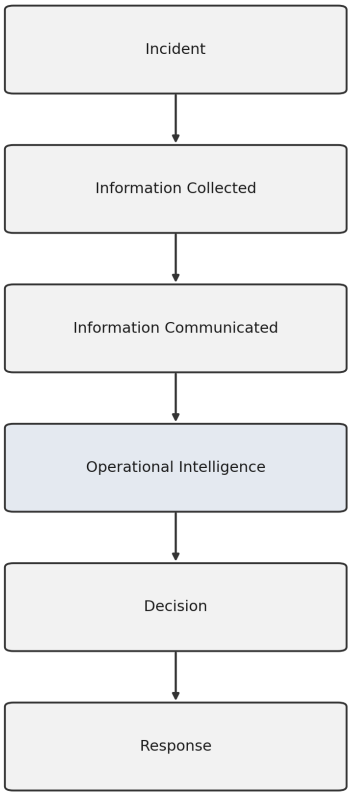


Figure 3.3 — TFOI Pathway

This metric provides an objective means of evaluating how rapidly useful operational intelligence reaches decision-makers, and forms one of the measurable outputs of the proposed capability demonstrator discussed later within this publication.

Key Chapter Findings

- Security operations are fundamentally decision-driven, following an established pattern shared with policing (NDM, NIM) and defence (OODA) doctrine
- Operational information reduces uncertainty; operational intelligence enables informed decision-making
- No single source provides complete situational awareness — integration across sources is what creates it
- Operational effectiveness depends on the quality of information directing resources, not merely the resources themselves
- Technology should be evaluated by the operational advantage it provides, measurable through metrics such as TFOI, rather than by its technical sophistication
- An aerial intelligence capability should therefore be evaluated as an additional operational information source within the organisation's wider operational framework

Transition to Chapter 4

This chapter has established that effective security depends on the quality, accuracy and timeliness of operational information available to decision-makers — and that this is a measurable property, not merely a qualitative one, through metrics such as TFOI.

The following chapter examines where an aerial intelligence capability fits within this established operational framework, and evaluates whether it can strengthen operational decision-making by providing information that is unavailable, impractical, or slower to obtain through conventional ground-based methods.

Chapter 4: Operational Capability Framework (OCF)

Measuring Speed Through TFOI and Quality Through Operational Capability Review (OCR)

4.0 Introduction

Operational performance has traditionally been evaluated using retrospective measures such as incident totals, response times, patrol frequency, arrest rates and resource deployment. Whilst these metrics provide valuable operational statistics, they predominantly assess events that have already occurred and therefore offer limited insight into an organisation's ability to prevent incidents before escalation.

This chapter introduces the Operational Capability Framework (OCF), a structured methodology for assessing operational capability. The framework produces two distinct and complementary outputs, which should not be conflated: Time to First Operational Intelligence (TFOI), an objective timing metric, and the Operational Capability Review (OCR), a structured qualitative assessment of the organisation's intelligence practice over time.

The framework presented within this chapter is intended as a conceptual model. It is not presented as an established industry standard, but rather as a structured methodology designed to encourage discussion, empirical validation and future interdisciplinary research.

> Definition 4.1 — Operational Capability Framework (OCF) A structured methodology used to evaluate an organisation's ability to acquire, process, interpret and exploit operational intelligence before, during and after operational activity. The framework measures capability rather than workload, enabling organisations to assess preparedness, situational awareness and decision support across operational practice.

4.1 Why Capability Matters

Many organisations assess operational success using quantitative performance indicators — incident count, response time, patrol frequency, arrest rate, staff deployment, CCTV coverage. Whilst these indicators remain valuable, they largely measure operational workload or historical outcomes. They do not necessarily measure whether an organisation possessed sufficient intelligence to prevent an incident from occurring, or whether the intelligence it did obtain was put to good use.

Consider a simplified example: Organisation A completes 14 patrols and records 18 incidents, with a 4-minute average response time. Organisation B completes 6 patrols and records only 4 incidents, with a 6-minute average response time. Using traditional performance metrics, Organisation A appears more productive. However, if Organisation B used integrated intelligence

sources to prevent situations from escalating before they became incidents, its lower activity may reflect greater operational capability, not less.

This distinction — between activity and capability — is the reason this chapter introduces two separate measures rather than one.

> Proposed Baseline Metric — Time to First Operational Intelligence (TFOI) Time to First Operational Intelligence (TFOI) is introduced within this publication as a proposed baseline metric for measuring the speed of operational intelligence acquisition. TFOI measures the elapsed time between an operational trigger — an alarm activation, a reported incident, the start of a patrol — and the point at which actionable operational intelligence, sufficient for a decision-maker to act, becomes available. TFOI measures speed only. It does not, on its own, indicate whether the intelligence obtained was accurate, well assessed, or well used — that is the separate question addressed by the Operational Capability Review (Section 4.2). At the time of writing, TFOI should be regarded as a proposed research metric requiring further validation through operational trials, peer review and interdisciplinary collaboration.

4.2 Operational Capability Review (OCR)

TFOI answers one question well: how quickly did actionable intelligence become available? It does not answer a different, equally important question: was the organisation's handling of that intelligence actually good?

A short TFOI is not, by itself, evidence of strong capability. An organisation could achieve a fast TFOI by acting on incomplete or unverified information, generating false alarms or poor decisions in the process. The Operational Capability Review exists to address this gap.

> Definition 4.2 — Operational Capability Review (OCR) A structured, qualitative review of an organisation's operational intelligence practice, conducted at the organisational level over a defined period, assessing the strength of practice across a set of capability domains. The Review produces findings, not a numerical score.

It is important to distinguish the OCR from the Operational Capability Framework Assessment introduced in Chapter 6. The two operate at different levels and answer different questions. The Chapter 6 assessment is incident-level and forward-looking: given this specific incident, is enhanced capability justified? The OCR is organisation-level and retrospective: looking back over a period of operational practice, how strong is the organisation's intelligence capability overall? An organisation may conduct many Chapter 6 assessments in a single week; an OCR is conducted periodically, reviewing a body of practice rather than a single incident.

4.2.1 Capability Domains

The OCR assesses practice across six domains, describing the lifecycle through which operational intelligence is generated and used:

Domain	What It Assesses
Detection	The organisation's ability to identify that an operationally significant event is occurring or may occur.

Domain	What It Assesses
Observation	The organisation's ability to gather direct information about an event once detected.
Intelligence Assessment	The organisation's ability to interpret and verify information, converting it into actionable intelligence.
Prediction	The organisation's ability to anticipate operationally significant events before they occur, based on patterns and available intelligence.
Operational Influence	The organisation's ability to deploy resources and make decisions in response to intelligence.
Operational Recovery	The organisation's ability to resolve an incident and return to normal operational posture.

4.2.2 Conducting the Review

Each domain is assessed qualitatively, using a structured rating — for example, Limited / Developing / Strong — supported by a written rationale explaining the finding. This is a deliberate departure from a numerically scored or averaged model. Reducing capability to a single composite figure implies a degree of measurement precision — specific weightings between domains, validated scoring scales, established inter-rater reliability — that has not yet been established for this framework. A structured qualitative finding, of the kind used in incident investigation and audit practice more broadly, allows the framework to describe capability rigorously without overstating what can currently be measured.

An illustrative OCR finding might read as follows:

Domain	Finding
Detection	Strong
Observation	Strong
Intelligence Assessment	Developing
Prediction	Limited
Operational Influence	Strong
Operational Recovery	Strong

Read this way, the review has genuine diagnostic value without needing to average anything into a single number: it tells the organisation that its ability to detect, observe, act on and recover from incidents is strong, but that Prediction — anticipating events before they occur — is an area requiring investment. This is more actionable than a single composite figure would be on its own, since it tells the organisation where to focus, not just how it is doing overall.

4.2.3 TFOI and OCR Together

TFOI and the Operational Capability Review answer different questions and are captured on different timescales. TFOI is measured incident-by-incident, and is available within minutes of

a trigger. The OCR is conducted periodically — for example, quarterly or annually — reviewing a body of operational practice rather than a single event.

Used together, they allow an organisation to answer the question a single metric cannot: not only "are we getting intelligence faster?" (TFOI, tracked over time) but "is our overall intelligence practice actually improving?" (OCR, tracked over successive reviews).

4.3 A Note on Future Development

This chapter has deliberately avoided reducing the Operational Capability Review to a numerical index. This is a considered decision rather than an oversight. A composite score — combining six domains into a single figure — would require a validated weighting between domains, a validated scoring scale, and evidence of consistent application across raters (inter-rater reliability). None of this currently exists for this framework.

Developing such an index remains a legitimate direction for future research, and is noted here as part of the paper's future development roadmap rather than presented prematurely as part of the current framework. Until that validation work has been done, the OCR is presented as a structured qualitative tool — rigorous and repeatable, but not arithmetic.

4.4 Summary

This chapter has introduced the Operational Capability Framework and its two distinct outputs: Time to First Operational Intelligence (TFOI), an objective timing metric measuring the speed of intelligence acquisition, and the Operational Capability Review (OCR), a structured qualitative assessment of the organisation's intelligence practice over time. TFOI answers how quickly actionable intelligence became available; OCR answers how strong the organisation's underlying practice is across the intelligence lifecycle. Neither substitutes for the other, and neither substitutes for the incident-level Operational Capability Framework Assessment introduced in Chapter 6, which serves a distinct, forward-looking purpose.

Chapter 5: Operational Application of the Operational Capability Framework

5.1 Purpose

The Operational Capability Framework (OCF) provides organisations with a structured methodology for assessing operational capability throughout the lifecycle of an incident. Whilst traditional security operations often measure performance through response times or incident outcomes, the OCF expands this approach by considering the relationship between operational intelligence, available capability and informed decision-making.

This chapter demonstrates how the framework is applied during live operational incidents and introduces Time to First Operational Intelligence (TFOI) as a measurable operational metric.

The purpose of the OCF is not to replace existing procedures, but to complement them by providing a structured method for determining whether available operational capability remains proportionate to the evolving circumstances of an incident.

5.2 Operational Decision Cycle

Operational incidents are dynamic and rarely remain static. Every new piece of information has the potential to alter the most appropriate operational response.

Within the OCF, every incident progresses through a continuous decision cycle.

Operational Stage	Primary Objective
Incident Notification	Receive initial information.
Initial Risk Assessment	Determine the initial level of uncertainty and operational risk.
Intelligence Gathering	Acquire actionable operational intelligence.
Measure TFOI	Determine when sufficient intelligence exists to support informed decision-making.
Capability Assessment	Assess whether current resources are proportionate to the incident.
Operational Response	Deploy or adjust resources based upon assessed capability requirements.

Operational Stage	Primary Objective
Continuous Reassessment	Update operational decisions as intelligence evolves.
Incident Resolution	Secure the incident and conclude operational activity.
Organisational Learning	Capture lessons to improve future operational capability.

The cycle continues throughout the incident rather than ending once resources have been deployed.

5.3 Time to First Operational Intelligence (TFOI)

One of the key operational measurements introduced within the Operational Capability Framework is Time to First Operational Intelligence (TFOI).

TFOI measures the elapsed time between the initial notification of an incident and the point at which sufficient operational intelligence has been obtained to support an informed operational decision.

Importantly, TFOI does not represent the time taken to gather all available information. Rather, it identifies the earliest point at which intelligence becomes sufficiently reliable to reduce operational uncertainty and influence decision-making.

Examples of operational intelligence include:

- Confirmation of offender presence.
- Estimated number of assailants.
- Vehicle identification.
- CCTV verification.
- Reports from responding personnel.
- Information provided by witnesses.
- Confirmation of forced entry.
- Identification of hazards.
- Live aerial observation.

Reducing TFOI enables organisations to transition from assumption-based decision-making to intelligence-led operational management.

5.3.1 TFOI is Source-Agnostic

TFOI is not tied to any single method of intelligence gathering. It is measured against whichever source first delivers intelligence of sufficient confidence to inform a decision — not against a predetermined or preferred method.

In practice, this may be an aerial platform, but it may equally be an already-monitored CCTV system, a witness already in contact with the control room, a responding officer's initial observations on arrival, or corroborated third-party reporting. The framework does not assume that any one source is superior; it recognises that the fastest and most reliable route to sufficient intelligence will vary from incident to incident, and in many cases will not involve an aerial platform at all.

Because each intelligence source has a different operational profile, the components contributing to TFOI differ by source. Aerial deployment, for example, involves a defined pre-launch and travel sequence; CCTV involves accessing and reviewing existing footage; a responding officer's contribution depends on travel time to scene. Section 5.3.2 sets out a worked example for aerial platforms, given their structured and highly measurable deployment sequence — but this is illustrative of the model, not a universal formula for TFOI.

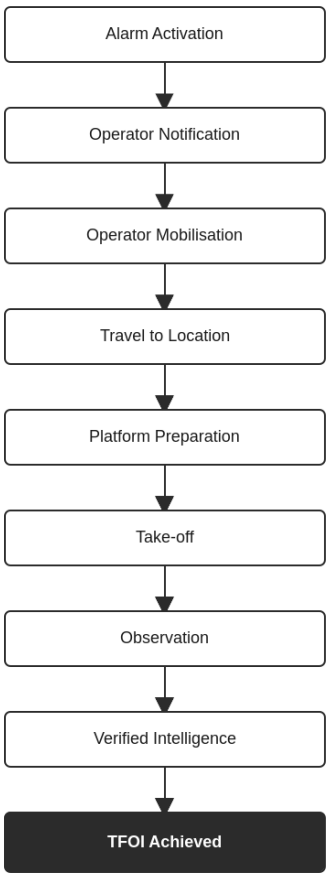
5.3.2 Worked Example: Aerial Platform Deployment

Where an aerial platform is used, TFOI can be broken into three sequential components:

- Deployment Latency — the time required to prepare and launch the platform, from initial notification to becoming airborne.
- Transit Time — the time required to reach the operational area, where applicable.
- Observation Time — the time required, once on-scene, to acquire intelligence of sufficient confidence to inform an operational decision.

Deployment model: for the purposes of this worked example, the proposed deployment model assumes that the aerial platform operator and keyholder attend the security provider's operational base to collect the necessary access equipment before travelling together to the site, with the platform stored with its operator. This illustrates one plausible operational structure rather than asserting any specific organisation's current or confirmed operating procedure; the keyholder, having travelled with the operator, would act as ground spotter once the platform is deployed.

The stages contributing to TFOI for an aerial deployment are set out below.



Component	Time
Notification to operator/keyholder attendance at operational base	Representative Operational Range (to be confirmed) — example reference: 30 minutes (based on a representative operator commute)
Access equipment collection	Representative Operational Range (to be confirmed)
Travel from operational base to premises	Representative Operational Range (to be confirmed)
On-site platform preparation (unfold, pre-flight check, power on, GPS acquisition)	5:30

Representative Operational Range (to be confirmed): notification-to-attendance and travel times will vary according to the operator's location, time of day, and distance between the operational base and the premises. The figures above should be replaced with confirmed values once validated against representative operational deployment patterns.

On-site platform preparation reflects outdoor platforms (e.g. Mini 4/5 Pro, Air 3S, M4T/M4E), which are never deployed within enclosed spaces, for operator and public safety. GPS signal acquisition (up to 2:00 of the total) is required for outdoor deployment.

For large enclosed environments — warehouses, shopping centres such as the Trafford Centre — and for night patrols, the Avata 2 is used instead. These conditions are GPS-denied or unreliable, and the Avata 2 flies in ATTI mode (Attitude mode), maintaining flight via barometer and IMU stabilisation without GPS positioning. GPS signal acquisition is therefore removed from the deployment sequence, reducing Deployment Latency relative to outdoor platforms — though ATTI mode's lack of GPS-assisted position hold demands greater operator skill, which may in turn extend Observation Time in confined or obstacle-dense environments.

The operator conducts all flights within Visual Line of Sight (VLOS). The aerial platform is not flown Beyond Visual Line of Sight (BVLOS) unless the operator holds the appropriate additional qualification and authorisation to do so.

5.3.3 Observation Time and Confidence

Regardless of source, Observation Time is the most variable component of TFOI, shaped by environmental conditions, visibility and incident complexity. Observation Time may also be influenced by the clarity required to achieve Verified confidence, meaning more complex incidents may require longer observation before TFOI is reached.

Not all intelligence carries equal reliability. A single unconfirmed report and a clearly observed, corroborated fact should not be treated as equivalent when determining whether TFOI has been achieved. The Operational Capability Framework therefore applies a three-tier confidence model to intelligence as it is received:

Tier	Description	Example
Unconfirmed	Intelligence has been reported but not independently observed or corroborated.	A witness states offenders are present, but this has not yet been visually confirmed.
Partially Verified	Intelligence has been partially observed, but conditions limit certainty (e.g. obstructed view, poor lighting, distance, motion blur).	Aerial footage shows movement on site, but individuals cannot be clearly counted or identified.
Verified	Intelligence has been directly and clearly observed or corroborated by an independent source, sufficient to inform a confident operational decision.	Aerial or CCTV footage clearly shows offender presence, number, and activity.

TFOI is achieved at the point where intelligence reaches Verified status against at least one operationally significant category (as listed in Section 5.3).

Intelligence that remains at Unconfirmed or Partially Verified may still inform an initial operational response — for example, a cautious approach or the deployment of additional resources — but it does not, in itself, satisfy TFOI. This distinction matters operationally: treating Partially Verified intelligence as sufficient risks a return to assumption-based decision-making, which the framework is specifically designed to move away from.

Where conditions prevent intelligence from reaching Verified status — for example, degraded visibility during night operations, or an obstructed sightline — this should be recorded as part of incident documentation. A failure to reach TFOI is itself an operationally significant finding,

and highlights a limitation of the intelligence-gathering method used rather than a failure of the framework.

5.4 Comparative Operational Scenario

The following scenario demonstrates how the Operational Capability Framework influences operational outcomes by reducing Time to First Operational Intelligence (TFOI) and improving operational capability.

Scenario A --- Conventional Operational Response

An intruder alarm activates at a commercial premises during the early hours of the morning.

A lone responding officer is dispatched with only the information provided by the alarm activation.

Time to officer arrival on site — Representative Operational Range (to be confirmed): dependent on officer's location at time of notification; comparable to the notification-to-attendance leg in Scenario B.

Believing the incident may be a routine false alarm, the officer commences an external inspection of the premises.

Time from arrival to external inspection commencing — Representative Operational Range (to be confirmed): likely near-immediate.

Unknown to the officer, three assailants remain on site loading stolen property into a waiting vehicle.

The officer unexpectedly encounters the offenders and is assaulted before being able to provide an operational update to the control room.

Elapsed time from arrival to confrontation — Representative Operational Range (to be confirmed): this is the point at which, in Scenario B, Verified-tier intelligence would already have been obtained via aerial observation before any officer approached the premises.

The control room, expecting a routine welfare communication or operational update, receives no contact from the responding officer.

Initially, there is no indication whether the delay is the result of routine activity, communication failure or an officer welfare emergency.

Standard lone-worker check-in interval — Representative Operational Range (to be confirmed): for scheduled on-site security deployments (e.g. media production sets), an hourly welfare check is a commonly used interval. It has not yet been confirmed whether the same interval applies to keyholder attendance at alarm activations, which is a distinct, unscheduled response scenario.

As the expected communication period expires, the organisation is required to manage two concurrent incidents:

- A burglary in progress.
- A potential lone-worker welfare incident.

Additional personnel are now required to locate and assist the responding officer while simultaneously managing the original incident.

Time from missed check-in to escalation and dispatch of additional personnel — Representative Operational Range (to be confirmed).

Time from escalation to verified intelligence (i.e. confirmation of the officer's condition and situation on site) — Representative Operational Range (to be confirmed): this represents Scenario A's actual TFOI equivalent: the first point at which the control room has Verified-tier operational intelligence.

Operational capability is reduced as resources are diverted towards officer welfare, and valuable operational intelligence is only obtained after the confrontation has already occurred.

Scenario B --- OCF Enhanced Operational Response

The same alarm activation is received.

Following an initial OCF assessment, the incident is identified as presenting elevated operational risk due to factors such as site profile, location, previous incident history or available intelligence.

For the purposes of this illustrative scenario, the aerial platform operator and keyholder are notified and attend the security provider's operational base to collect the necessary access equipment before travelling together to the premises, with the platform stored with its operator and travelling with them to site.

Component	Time
Notification to operator/keyholder attendance at operational base	Representative Operational Range (to be confirmed) — example reference: 30 minutes
Access equipment collection	Representative Operational Range (to be confirmed)
Travel from operational base to premises	Representative Operational Range (to be confirmed)
On-site platform preparation	5:30

Upon arrival, the platform is deployed on-site. The operator conducts all flights within Visual Line of Sight (VLOS); the platform is not flown Beyond Visual Line of Sight (BVLOS) unless the operator holds the appropriate additional qualification and authorisation. The keyholder, having travelled with the operator, acts as ground spotter during deployment.

The aerial platform conducts external reconnaissance using thermal imaging. Within approximately 2:00, it provides:

- Confirmation of offender presence or absence.
- Estimated number of assailants.
- Live situational awareness.
- Vehicle descriptions and registration details where visible.
- Observation of potential escape routes.
- Timestamped evidential video of the incident.

Intelligence reaches Verified status against offender presence and estimated numbers.

Total TFOI — Representative Operational Range (to be confirmed): sum of confirmed components above once travel-to-site and access equipment collection figures are finalised.

Using verified intelligence, the control room can now determine the most proportionate operational response.

If offenders are confirmed to be present, the responding officer remains in a place of safety while police are updated using live operational intelligence.

If no evidence of criminal activity is identified, the responding officer may proceed with a routine internal inspection of the premises whilst the aerial platform records a timestamped visual record of the external condition of the site.

Once the internal inspection confirms there has been no unauthorised entry or ongoing threat, the aerial platform lands, the operator's task is complete, and they stand down. The responding officer completes any remaining security duties before securing the premises and closing the incident.

Scenario Comparison

Operational Measure	Conventional Response	OCF Enhanced Response
Initial Operational Intelligence	Alarm only	Alarm + aerial reconnaissance
TFOI	Achieved after confrontation	Achieved before confrontation
Officer Welfare	Reactive	Proactive
Evidence Collection	Limited	Continuous
Situational Awareness	Limited	Continuous
Decision Basis	Predominantly assumption-based	Intelligence-led

5.5 Comparative Analysis

Both scenarios began with the same alarm activation.

The difference was not the speed of response, but the speed at which reliable operational intelligence became available.

In the conventional response, decisions were based primarily upon assumption until direct contact with the incident occurred.

Within the Operational Capability Framework, the acquisition of timely operational intelligence reduced uncertainty before personnel were exposed to unnecessary risk.

The aerial platform did not replace operational judgement.

It enabled better operational judgement.

By reducing Time to First Operational Intelligence (TFOI), the organisation improved officer welfare, enhanced evidential continuity, increased situational awareness and ensured that operational capability remained proportionate to the assessed risk.

The timely acquisition of operational intelligence improves decision-making but does not, in isolation, resolve an incident. Operational capability remains dependent upon the availability of appropriate personnel, equipment and supporting resources. TFOI measures the speed of the intelligence-gathering process; it does not, in itself, measure the organisation's capacity to respond.

Nor does the framework argue that an aerial platform should always be deployed. Rather, it argues that an aerial platform may be justified where it provides a proportionate increase in operational capability relative to the assessed risk. This is a position grounded in structured decision-making, not technology advocacy — the circumstances under which enhanced capability is justified are addressed directly in Chapter 6.

5.6 The Relationship Between OCF and TFOI

It is important to distinguish between the Operational Capability Framework and Time to First Operational Intelligence, as the two serve different but complementary functions.

The Operational Capability Framework is the structure. It defines the stages through which every incident progresses, from initial notification through to organisational learning, and provides organisations with a consistent method for assessing whether operational capability remains proportionate to an evolving incident.

Time to First Operational Intelligence is the metric. It measures a single, specific point within that structure — the moment at which sufficient operational intelligence exists to support informed decision-making. TFOI does not describe the framework itself; it describes how effectively the framework is being applied in practice.

In this sense, OCF answers the question “what should happen during an incident?” while TFOI answers the question “how quickly is it happening?” An organisation may adopt the OCF structure without measuring TFOI, but doing so removes the ability to demonstrate, in measurable terms, whether the framework is delivering the intended reduction in operational uncertainty. Conversely, TFOI has no meaning outside the context the framework provides — it is only a useful measurement because OCF defines what “sufficient operational intelligence” is being measured against.

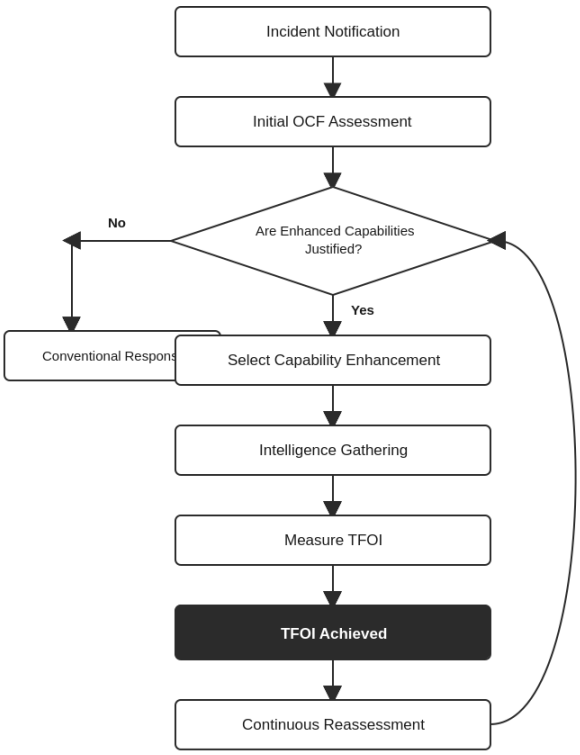
Together, the Operational Capability Framework and Time to First Operational Intelligence provide organisations with both a structured decision-making methodology and a measurable indicator of how efficiently actionable operational intelligence is acquired.

Chapter 6: Operational Capability Framework Assessment and Resource Allocation

6.1 Purpose

Definition — Operational Capability

Operational capability is the organisation's ability to respond safely, effectively and proportionately to an operational incident through the coordinated application of personnel, information, technology and supporting resources.



The Operational Capability Framework provides organisations with a structured methodology for understanding incidents and measuring Time to First Operational Intelligence (TFOI). However, obtaining operational intelligence is only one part of effective incident management.

Supervisors must also determine whether available operational capability remains proportionate to the assessed level of operational risk. Section 5.4 referred to an "initial OCF assessment" as the trigger for an enhanced response; this chapter defines what that assessment consists of and how it is conducted in practice.

This chapter introduces the Operational Capability Framework Assessment — a structured method for determining when enhanced operational capability may be justified.

The purpose of the Operational Capability Framework Assessment is not to eliminate operational judgement, but to ensure that judgement is exercised consistently, transparently and with reference to identifiable operational factors.

It is worth being precise about what the assessment actually evaluates. The incident itself is the catalyst for the assessment, not its subject. What is being assessed is whether the organisation currently possesses sufficient capability to manage that incident safely and proportionately — a question about organisational readiness, informed by the circumstances of the incident.

6.2 Principles of Proportionate Capability

The Operational Capability Framework Assessment is guided by four principles:

Principle 1 — Proportionality.

Operational capability should be proportionate to operational risk. Enhanced resources are neither automatically deployed nor automatically withheld; their use is determined by the assessed circumstances of the incident.

Principle 2 — Intelligence-led decision-making.

Operational decisions should be driven by verified operational intelligence wherever reasonably practicable, in line with the confidence model set out in Section 5.3.3.

Principle 3 — Need over availability.

Enhanced capability should be justified by operational need rather than by the availability of a particular technology or resource.

Principle 4 — Welfare as capability.

Officer and public welfare form part of operational capability, not a separate consideration weighed afterward. A response that reduces risk to personnel is, by definition, a more capable response.

6.3 Operational Capability Framework Assessment Factors

The following factors inform the Operational Capability Framework Assessment. They are considerations to be weighed by a supervisor using professional judgement — not inputs to a score or formula.

Assessment Factor	Operational Consideration
Asset Value	Financial impact if compromised.
Crime Profile	Local history of burglary or organised criminal activity.
Previous Incidents	Historical events associated with the premises.
Site Complexity	Size, layout and number of potential hiding places.
Existing Intelligence	Information available before deployment.
Lone Worker Exposure	Degree of officer vulnerability.
Environmental Conditions	Lighting, weather and visibility.
Existing Surveillance	CCTV coverage and monitoring capability.
Critical Infrastructure	Operational consequences beyond financial loss.
Public Safety	Risk to members of the public.

Two factors — Lone Worker Exposure and Public Safety — warrant particular attention, as they concern risk to people rather than risk to property or process. A significant risk to an individual's welfare or to public safety may, on its own, be sufficient to justify an enhanced response, irrespective of the remaining factors. The other factors should be considered collectively, in the context of the specific incident, rather than assessed in isolation.

6.4 Capability Escalation Model

Based on the Operational Capability Framework Assessment Factors identified in Section 6.3, a supervisor assigns the incident one of four indicative assessment outcomes:

Assessment Outcome	Description	Response
Low	Operational risk is limited and well-understood.	Conventional response.
Moderate	Some risk indicators are present, warranting increased attentiveness.	Conventional response with enhanced monitoring.
High	Multiple risk indicators are present, or a significant welfare or public safety concern exists.	Enhanced operational capability considered.
Critical	Substantial risk indicators are present in combination, or a severe welfare or public safety concern exists.	Full enhanced operational response.

This model provides a shared vocabulary for describing operational risk and a consistent structure for reasoning about it. It is a judgement aid, not a calculation: the assessment outcome reflects the supervisor's informed evaluation of the factors in Section 6.3, not a count or sum of them. Supervisors should be able to explain, in their own words, why a given outcome was reached with reference to the specific factors present.

6.5 Selecting Capability Enhancements

Where the Operational Capability Framework Assessment indicates that enhanced capability is warranted, a range of options may be considered. The following are examples of possible capability enhancements, not a prescribed or exhaustive list:

- Additional responding personnel.
- Aerial platforms.
- Existing CCTV monitoring.
- Thermal imaging.
- Body Worn Video.
- Police liaison.
- Additional supervisory support.
- Temporary scene containment.

The selection of an appropriate enhancement depends on the specific factors identified during assessment, the resources available to the organisation, and the environmental conditions present at the site (see Section 5.3.2 for platform selection considerations relevant to enclosed or low-light environments). No single enhancement is treated as a default response; the assessment identifies the level of capability required, and the specific method by which that capability is delivered is a separate, subsequent decision.

6.6 Worked Example

The following example applies the Operational Capability Framework Assessment to the scenario introduced in Section 5.4.

Assessment factors present:

- High-value warehouse.
- Previous burglary.
- High-crime area.
- Lone response (Lone Worker Exposure).
- Poor external CCTV.
- Night-time / reduced visibility.

Assessment outcome:

Lone Worker Exposure is present, and on its own would be sufficient to justify an enhanced response. This is reinforced by several further indicators — the site's asset value, its history of burglary, its location in a high-crime area, and the limitations of its existing surveillance — all of which point toward substantial operational risk. Taken together, the supervisor assesses this incident as Critical.

Enhanced capability selected:

- Aerial platform (thermal-equipped, given night-time conditions).
- Additional responding officer.
- Police notified in advance of attendance.

The outcome reached in Section 5.4's Scenario B is therefore not presented as a default or automatic response to an alarm activation. It is the outcome of a structured assessment: the lone-worker risk alone would have been sufficient to justify escalation, and was reinforced by the wider circumstances of the incident. A different premises — lower value, well-lit, strong existing CCTV coverage, no adverse history — could generate the same alarm activation and reasonably receive a conventional response instead.

6.7 Relationship to TFOI

Time to First Operational Intelligence and the Operational Capability Framework Assessment serve distinct but connected functions within the framework.

TFOI measures how quickly sufficient operational intelligence becomes available. The Operational Capability Framework Assessment determines how that intelligence — and the wider circumstances of the incident — should influence operational decision-making, including whether enhanced capability is justified.

Together, these processes allow organisations to move from assumption-based responses towards proportionate, intelligence-led operational management: TFOI provides the measurable indicator of how quickly the organisation reaches a position of sufficient knowledge, while the Operational Capability Framework Assessment provides the structured method for acting on that knowledge in a manner appropriate to the assessed risk.

Chapter 7: Implementation

7.1 Purpose

Chapters 3 to 6 have defined the Operational Capability Framework (OCF), introduced Time to First Operational Intelligence (TFOI) as its measurable metric, demonstrated the framework's application through comparative scenarios, and set out the Operational Capability Framework Assessment as the structured method by which supervisors determine when enhanced capability is justified.

This chapter addresses a different question: how does an organisation actually begin using the framework in practice?

Implementation is treated separately from the conceptual chapters that precede it because adopting a framework is a distinct undertaking from understanding one. An organisation may accept every principle set out in this paper and still fail to apply it consistently without a deliberate approach to rollout, training, documentation and review. This chapter sets out that approach.

7.2 Implementation Principles

Adoption of the Operational Capability Framework is guided by the following principles:

Principle 1 — No prerequisite technology.

The framework does not require an organisation to acquire new equipment before it can be adopted. The OCF Assessment, the escalation model, and the principles of proportionate capability can be applied using an organisation's existing resources. Capability enhancements, including aerial platforms, are considered only where the assessment indicates they are justified.

Principle 2 — Phased adoption.

The framework is intended to be introduced in stages rather than all at once, allowing an organisation to build familiarity and confidence before extending its use.

Principle 3 — Documentation from the outset.

Assessment outcomes and TFOI figures should be recorded from the point of adoption, even where enhanced capability is not deployed. Early documentation, including of conventional responses, provides the organisational baseline against which future review depends.

Principle 4 — Review is part of implementation, not an afterthought.

An organisation adopting the framework should plan, from the outset, how it will periodically review whether the framework is being applied consistently and whether it is achieving its intended purpose.

7.3 Phased Adoption

A phased approach allows an organisation to adopt the framework without requiring simultaneous changes to procedure, technology and training. Three indicative phases are set out below; organisations may adapt this structure to their own circumstances.

Phase 1 — Assessment and Terminology.

The organisation adopts the Operational Capability Framework Assessment and the shared vocabulary of assessment outcomes (Low, Moderate, High, Critical) set out in Section 6.4. Supervisors begin applying the assessment factors from Section 6.3 to incidents as they occur, using existing resources. No new technology or capability is introduced during this phase; its purpose is to establish consistent operational reasoning.

Phase 2 — TFOI Measurement.

The organisation begins measuring and recording Time to First Operational Intelligence for incidents, using the confidence model set out in Section 5.3.3. This phase establishes a factual baseline for how quickly the organisation typically reaches sufficient operational intelligence using its existing methods, before any capability enhancement is introduced.

Phase 3 — Capability Enhancement.

Where the organisation's own review of Phase 1 and Phase 2 data indicates a case for doing so, specific capability enhancements (Section 6.5) are introduced and evaluated against their effect on TFOI and assessment outcomes over time.

This staged approach ensures that any decision to invest in enhanced capability, including aerial platforms, is supported by the organisation's own operational data rather than made in advance of it.

7.4 Training and Competency

Consistent application of the framework depends on personnel understanding their role within it. This paper does not prescribe a specific training course or syllabus, but identifies the areas of competency implementation requires:

- Supervisors require a working understanding of the Operational Capability Framework Assessment (Chapter 6), including the assessment factors, the escalation model, and the principle that the model supports rather than replaces professional judgement.
- Control room and monitoring personnel require an understanding of the confidence model (Section 5.3.3) in order to record intelligence accurately as Unconfirmed, Partially Verified, or Verified, since this directly determines when TFOI is achieved.
- Operators of any deployed capability enhancement (aerial or otherwise) require competency specific to that resource, in addition to an understanding of how their role fits within the wider framework — for example, an aerial platform operator should understand that their role is to help achieve Verified-tier intelligence, not simply to fly a platform.
- All personnel benefit from understanding Principle 4 of Section 6.2 — that welfare is part of capability, not a separate concern — so that the framework is applied with that principle in mind rather than as an administrative afterthought.

7.5 Documentation and Record-Keeping

The credibility of the framework, both internally and to external stakeholders, depends on consistent record-keeping. At minimum, an organisation implementing the framework should record, for each relevant incident:

- The assessment outcome reached (Low, Moderate, High, Critical) and the factors that informed it.
- Where TFOI is measured, the time elapsed and the intelligence source(s) involved.
- Where a capability enhancement is deployed, which enhancement was selected and why.
- Where an assessment outcome is later found to have been inaccurate (for example, a Low-assessed incident that escalated significantly), this should be documented as part of organisational learning, consistent with the final stage of the decision cycle set out in Section 5.2.

This record-keeping serves two purposes: it provides the evidential basis for the organisational review described in Section 7.6, and it ensures that the "transparent and consistent" quality of the assessment, described in Section 6.1, is demonstrable rather than assumed.

7.6 Governance and Review

Implementation does not end once the framework is in use. An organisation should establish a periodic review process, examining:

- Whether assessment outcomes have been applied consistently across similar incidents.
- Whether TFOI figures are trending as expected, and whether any patterns (for example, consistently poor Observation Time in particular conditions) indicate a need for procedural or capability changes.
- Whether capability enhancements introduced in Phase 3 are producing a measurable effect on TFOI or operational outcomes proportionate to their cost.
- Whether the assessment factors and thresholds in Sections 6.3 and 6.4 remain appropriate to the organisation's operating environment, or require adjustment.

This governance activity mirrors, at an organisational level, the Continuous Reassessment stage of the incident-level decision cycle set out in Section 5.2 and illustrated in the decision-flow diagram in Section 6.1. Just as an individual incident is continuously reassessed as new intelligence arrives, the framework itself should be continuously reviewed as the organisation accumulates operational experience in using it.

7.7 Automated Data Collection

Where an organisation's operational technology permits, TFOI measurement and the documentation described in Section 7.5 may be supported by automated data collection — for example, a system that timestamps the notification of an incident, logs each piece of reported intelligence as it arrives, and records the point at which a supervisor or control room operator confirms that intelligence has reached Verified status.

Such a system improves the accuracy and consistency of TFOI measurement relative to manual recording, and reduces the administrative burden on personnel during live incidents. It does not, however, alter where responsibility for judgement sits within the framework. The classification of intelligence against the confidence model in Section 5.3.3 — and the decision as to whether an assessment outcome or operational response is warranted — remains a matter of professional judgement, consistent with Principle 3 of Section 6.2. An automated system may record that a judgement was made and when; it does not make the judgement itself.

Organisations considering automated data collection as part of implementation should ensure that any such system is positioned as a recording and timing tool within the framework, rather than as a decision-making system in its own right.