Behavioural Security QuickScan (Executive)

Control reliability triage for a security-critical workflow (5-7 minutes)

What this is

A short self-assessment designed to surface **likely behavioural exposure** in a selected security-critical workflow - where security outcomes are shaped by how work is actually done under constraints (pressure, exceptions, workarounds).

What this is not: a diagnostic, a risk score, an audit, or proof of safety. Use it to decide whether a workflow warrants deeper review.

How to use it

1) Select a **control area**, **asset**, and likely **impact** for one workflow (last 90 days).

2) Tick statements that are true **often enough to matter** for that workflow.

3) Use the results guide (Page 3) to decide whether to commission a deeper review.

ERA self-awareness (input quality)

Before answering, notice what your answers are based on:

- **E - Evidence:** direct workflow contact (walkthrough, sampling, incident pack review).
- **R - Reporting:** dashboards, metrics decks, summaries, second-hand updates.
- **A - Assumption:** inference or belief without a source.

Rule of thumb: if your view is mainly dashboards/summaries, treat it as **Reporting**, not Evidence.

Tip: Keep the scope tight. One workflow, one asset, one control area. Broad scopes produce broad (and less useful) answers.

QuickScan - Inputs (scope to one workflow, last 90 days)

Control area (circle one)	IAM / Privileged access • Data handling • Change / Release • Incident handling • Third-party access
Asset at stake (circle one)	Credentials/keys • PII • IP/source code • Production service • Financial/regulatory records
Primary impact if it fails (circle up to two)	Unauthorised action/fraud • Data exposure • Outage • Regulatory breach • Material loss/rework
Workflow choke point (one line)	____ ______________
Control step most often bypassed / negotiated (one line)	____ ______________
When is this control hardest to follow? (one line)	____ ______________
Evidence contact (circle one)	E (Evidence) • R (Reporting) • A (Assumption)

Tick what's true for this workflow (last 90 days)

Answer for the selected **control area** and **asset**, not general organisational issues. Tick statements that are true **often enough to matter**. If unsure, leave unticked.

□ **1.** No single person is clearly accountable for this workflow's security outcome.

□ **2.** Workarounds and exceptions are normal, not rare.

□ **3.** Assurance relies mainly on artefacts (sign-offs/screenshots) rather than checking workflow reality.

□ **4.** When security steps slow delivery, the workflow adapts informally to keep moving.

□ **5.** Security exceptions are not consistently logged with a reason and approver.

□ **6.** Security-relevant near-misses are often fixed locally and not recorded.

□ **7.** Issues tend to be escalated only when urgent or externally visible.

□ **8.** Records (tickets/logs/reports) often lack key context for learning (what changed/why/decision trail).

□ **9.** Reporting looks stable while recurring friction/exceptions persist.

□ **10.** The documented security process differs from how work is actually done.

□ **11.** Under time pressure, security steps are shortened, skipped, or bundled.

□ **12.** Exceptions are approved case-by-case without consistent criteria/process.

□ **13.** The workflow depends on a small number of individuals to prevent failure.

□ **14.** During peaks, work is improvised rather than using agreed 'what can be relaxed' rules.

□ **15.** After fixes are introduced, the workflow tends to drift back toward prior behaviour.

Quick cross-check (3 clicks)

□ Controls shape the work / Work shapes the controls

□ Problems surface early / Problems surface when they hurt

□ Controls hold under pressure / Controls fail under pressure

Results guide (rough, not a score)

This page helps you interpret the QuickScan without turning it into a diagnostic method.

Your context	
This QuickScan relates to (circle/write)	Control area / Asset / Impact: __________________ / ________________ / ____________________
Tick total (0-15)	__________
Reality basis (ERA)	E **|** R **|** A (circle one)

Rough guide (heuristic):

- **Few ticks (0-3):** Low signal - either the workflow is stable *or* you have limited visibility.
- **Several ticks (4-6):** Medium exposure - control reliability likely varies with pressure and exceptions.
- **Many ticks (7-15):** High exposure - controls are unlikely to be reliable in real operating conditions.

ERA rule: If your reality basis is mainly **R** or **A**, treat a 'low signal' result as **unknown**, not safe.

What this means (plain terms)

If you ticked many statements, it suggests security outcomes in the selected workflow are being shaped by exceptions, workarounds, and pressure responses - meaning formal controls may not hold consistently when it matters.

Next step (optional)

Executive Briefing Call (Behavioural Security)
£195 • 60-minute call + 1-page written brief
A structured briefing that ends with a clear next step (Diagnostic vs Review), with suggested scope.
£195 is credited against the Diagnostic or Review if you proceed within 30 days.

Best for: board questions, stalled delivery, repeat surprises, assurance vs speed tension, exceptions becoming normal.

Limitations

This QuickScan is self-report and does not constitute a security assessment, audit, or risk score. It does not measure control effectiveness; it flags likely exposure patterns worth reviewing.