Subsurface

Trust Signal Scan

A 10-Minute Diagnostic for System Trust Integrity

Modern systems make thousands of automated decisions every day. Yet very few organisations can clearly explain the **evidence behind those decisions**.

The Subsurface Trust Signal Scan is designed to help leaders quickly evaluate the strength of trust signals within operational systems.

Rather than asking whether a system simply *works*, this diagnostic explores whether systems can:

• Justify their decisions with credible evidence
• Detect anomalies and manipulation attempts
• Maintain operational visibility as processes scale
• Operate with layered and resilient control architecture

Estimated completion time: **10 minutes**

Four Trust Signal Domains

1. Evidence Integrity

How clearly can decisions be traced back to credible supporting evidence?

2. Identity Credibility

How resilient is the system against identity manipulation or synthetic identities?

3. Operational Visibility

Can inefficiencies, delays and signal gaps be detected before they create operational impact?

4. Control Architecture

Are decisions protected by layered verification and resilient control structures?

Trust Signal Diagnostic Questions

1. Are critical automated decisions supported by multiple independent signals?

Strong	Moderate	Weak

2. Can system outputs be traced clearly back to underlying evidence?

Strong	Moderate	Weak

3. Does identity verification include behavioural or contextual signals beyond document checks?

Strong	Moderate	Weak

4. Can the system detect anomalies such as device mismatch or location inconsistencies?

Strong	Moderate	Weak

5. Could a synthetic identity realistically pass onboarding without detection?

Strong	Moderate	Weak

6. Can operational delays be detected in real time rather than after the fact?

Strong	Moderate	Weak

7. Are workflow bottlenecks measured and monitored systematically?

Strong	Moderate	Weak

8. Do controls rely on layered verification rather than a single checkpoint?

Strong	Moderate	Weak

9. If one control layer failed, would the system detect the failure automatically?

Strong	Moderate	Weak

10. Are automated decisions periodically reviewed for false approvals or false rejections?

Strong	Moderate	Weak

11. Is decision evidence retained long enough to support audits or investigations?

Strong	Moderate	Weak

12. Is there a defined process for investigating unexpected system behaviour?

Strong	Moderate	Weak

Interpreting Your Trust Signal Profile

Strong Signal Architecture
Systems operate with layered evidence and resilient verification signals. Decisions can be justified and traced with confidence.

Moderate Exposure
Systems function effectively but may rely on narrower evidence sources or limited signal diversity. Risk exposure may increase as systems scale.

Trust Fragility
Key decisions rely on limited signals or assumptions. As systems automate and scale, vulnerabilities may emerge in verification or operational visibility.

Systems rarely fail because they stop working. They fail because the signals supporting decisions weaken over time.

The Subsurface Trust Signal Scan is designed to highlight those signals early.

Garry Cameron
Founder — Subsurface | Trust & Risk Architecture

Website: subsurfaceconsulting.co
Email: garry@subsurfaceconsulting.co