THE RISK MANAGEMENT FORUM

# The Integrated Architecture

## SRA-I, C-SRA-I and Fragility Intelligence as one system

Master Framework Document

**Version 2.0**

28 August 2026

Dr André Du Venage, DBA, CSMP, CCTP

Co Founder and Chief Executive Officer, The Risk Management Forum

Open Researcher and Contributor Identifier (ORCID): 0009-0003-3706-9124



**Suggested citation**

Du Venage, A. (2026) The Integrated Architecture: SRA-I, C-SRA-I and Fragility Intelligence as one system. Master Framework Document, Version 2.0. Paarl: The Risk Management Forum.

**Status**

This is the controlling document for the framework. It does not replace WP-2026-007, which remains the citable scholarly source for the definition, the scope conditions and the propositions.

The Risk Management Forum | www.trmf.org.za | andre@trmf.org.za

# Contents

## Part 1. The problem the architecture answers

Governance has become more codified, more audited and more thoroughly scored in every decade since Cadbury. Governance failure has not become correspondingly rarer.

The usual response is to conclude that the apparatus was not rigorous enough, and to add to it. That response assumes the relationship between governance quality and governance failure is one of degree, so that more governance, more precisely specified, must eventually produce less failure. The record does not support the assumption.

The alternative explanation is that codification answers a different question from the one failure poses. Codes and scores establish whether governance structures are present and adequate. That is a state description. Failure is not a state. It is a trajectory. An organisation does not fail because a structure was absent on a particular day. It fails because deterioration was observable over a period and was not interpreted as deterioration by anyone with the authority to act.

Two questions follow, and they are not the same question.

1. Where in the system is pressure building, and how does it move? This is a question about the system, and the answer is a model.
2. Can this organisation still see the pressure and correct it? This is a question about capacity, and the answer is a measurement.

The first question is answered by the Strategic Risk Architecture Integrated (SRA-I) model and its organisational application. The second is answered by Fragility Intelligence. Neither is complete without the other, and Part 2 sets out how they join.

# Part 2. The integrated architecture

This Part is the spine of the framework. Everything that follows is an elaboration of it.

## 2.1 Three instruments, one system

| Instrument | What it is | What it answers | Output |
|---|---|---|---|
| SRA-I | Strategic Risk Architecture Integrated. The general model of systemic deterioration. Reads at country, sector and institutional level | Where is pressure building, and along which pathway does it travel | A domain reading and a transmission pathway |
| C-SRA-I | Corporate Strategic Risk Architecture Integrated. The same architecture applied to a single organisation | The same question, at organisational scale, against organisational data | A domain reading and a transmission pathway for one entity |
| Fragility Intelligence | The analytical discipline that reads the systemic stabiliser | Can this organisation still detect the pressure, and can it still correct it | A stabiliser reading, expressed as transmission stage, active pathway and stabiliser availability |

The relationship between the first two is parent and application, not old and new. SRA-I is the general theory and is what makes C-SRA-I more than a consulting checklist. C-SRA-I is the commercial instrument and carries the board work, the evaluation mandate and the platform. SRA-I remains necessary because it is the only one of the two that reaches an institution sitting inside a state system, where the deterioration runs across both. That is the shape of the Public Investment Corporation (PIC) case.

## 2.2 The four domains and the systemic stabiliser

The architecture has five elements, and they are not five of the same thing. Four are domains that can be observed, each with a data source. The fifth has no data source of its own.

| Element | SRA-I form | C-SRA-I form |
|---|---|---|
| Domain 1 | Governance integrity and decision architecture | Governance architecture and decision integrity |
| Domain 2 | Economic and capital stability | Capital strength and financial stability |
| Domain 3 | Social cohesion and legitimacy | Organisational cohesion and execution alignment |
| Domain 4 | Security and organised threat landscape | Operational risk and threat landscape |
| Stabiliser | Strategic resilience and adaptive capacity | Strategic resilience and adaptive capacity |

The stabiliser is not a fifth domain and is not parallel to the other four. It is revealed only by what happens when the four come under pressure: whether the signal moved, whether a decision was taken, whether the correction held.

The transmission ring settles the point independently. The sequence runs governance weakness, economic instability, social fracture, security breakdown, systemic decline. Those are the four domains

passing pressure to one another. Resilience is not a station on that line. It determines whether the line continues, which is why the schematic already names it the intervention point.

**This also matters practically. Five parallel elements invite a score in five parts, and a score in five parts invites averaging. Averaging would allow a strong reading in one domain to offset a failed stabiliser, which is the shape of every institution that looked adequate on most measures while the thing that mattered had stopped working.**

## 2.3 Where Fragility Intelligence attaches

Adaptive capacity means the ability to see a problem and correct it. That is exactly what Fragility Intelligence measures: detection, response capacity and willingness to act.

> *Fragility Intelligence is not a sixth element of the architecture and not a layer above it. It is the instrument that reads the systemic stabiliser.*

The join runs both ways, and each side gains something it did not previously have.

### What the model gives Fragility Intelligence

- Axes for convergence. Convergence has to be convergence across something. The domains supply the axes, which is what makes a convergence finding falsifiable rather than impressionistic.
- A pathway for projection. The transmission ring supplies the route along which deterioration travels, which is what allows a warning to state where it will surface next rather than only that something is wrong.
- A derived silo taxonomy. The ten origination silos are not an arbitrary list. Each sits in a domain, and the domain determines which correlation tests apply. The map is at 5.6.
- Reach beyond the single organisation. Through SRA-I, the same instrument reads an institution embedded in a state system, where the deterioration runs across both levels.

### What Fragility Intelligence gives the model

- It makes the intervention point measurable. The schematic already names strategic resilience as the point of intervention. Until now the model asserted that point and could not test whether it was available. Fragility Intelligence supplies the reading.
- It turns the transmission loop from a description into a monitored process, because filtration events are dated, registered and attributable to a node.
- It supplies the evidence that a domain reading is trustworthy. A domain reading assembled from filtered information is a reading of the filter, not of the domain.

## 2.4 What the integration changes in practice

### Convergence splits into two findings

Convergence within a single domain is concentration. Convergence across domains is transmission. The second is materially more serious and escalates faster, because it means the feedback loop is running. This is already operative in the signal classes, where Class B is triggered by correlation across two or more domains.

### Reporting is a stage model, not a score

Fragility Intelligence reports three things and no composite figure:

1. Which transmission stage is active.
2. Which pathway is carrying it.
3. Whether the stabiliser is available.

This answers the practitioner question about how fragility is quantified without inventing a false metric, and it holds the line against the scoring failure mode set out at 3.4. What must never happen is the collapse of Fragility Intelligence into domain scoring. Integration is structural, not arithmetical.

#### Filtration acquires its structural explanation

Filtration degrades the stabiliser directly, whatever domain the underlying signal came from. That is why it escalates on its own account, as Class E at 5.4. A filtered signal reduces adaptive capacity even where the matter underneath it turns out to be nothing.

### 2.5 One signal through the whole architecture

A worked sequence, to show the parts operating together rather than side by side.

1. A supplier payment pattern shifts. The signal originates in Domain 2 and is registered at first contact under Rule Three, in the originator's own wording, with the domain recorded.
2. Senior finance staff depart under settlement agreements. This is Domain 3. Two domains are now implicated, so the signal is Class B by correlation rather than by anyone's judgement of severity.
3. The Fragility Intelligence function aggregates and identifies the transmission direction: capital pressure moving into cohesion, which is the second and third stations of the loop.
4. The Chief Financial Officer is implicated. The signal becomes Class C, and Rule One removes the finance controlled route automatically.
5. Rule Two moves custody laterally to the Chief Audit Executive and the Chair of the Audit Committee, which are tested for independence on appointment, remuneration and tenure.
6. The disposition threshold of ten working days passes with no recorded decision. The default rule escalates the signal without anyone deciding that it should.
7. A performance action is taken against the originator inside the ninety day window. That is deemed an originator attack, the burden reverses onto the acting node, and a separate Class E signal is registered.
8. The Class E event escalates the original signal by one class to Class D and adds the acting node as the subject of a second signal.
9. The stabiliser reading is now available and it is not a matter of opinion. Detection worked. Response did not. Willingness to act is contradicted by the record. The organisation cannot correct what it has seen.
10. The board receives a transmission finding, not a score: pressure is moving from Domain 2 into Domain 3, the pathway is live, and the stabiliser is unavailable at the executive node.

**Note what carried the finding. Not the seriousness of the payment pattern, which on its own would have been a routine item. The finding came from the handling.**

# Part 3. Fragility Intelligence defined

## 3.1 Formal definition

> *Fragility Intelligence is the analytical discipline concerned with interpreting the trajectory of institutional deterioration by treating the interpretive capacity of the governance tier as its unit of analysis, applying indications and warning methodology to signals about that capacity, and coupling the resulting warning judgement to an explicit model of how the deterioration transmits to consequence.*

Four elements carry the weight. It is interpretive rather than descriptive, which separates it from governance analytics. It is concerned with trajectory rather than condition, which separates it from governance scoring. Its unit of analysis is the interpretive capacity of the governance tier rather than the financial record, which separates it from the distress prediction tradition. And it is coupled to a transmission model, supplied by the architecture at Part 2, which is what allows it to state where and when rather than only whether.

## 3.2 Constructs

- Governance visibility. The proportion of material deterioration that is in principle observable to the governance tier through the existing reporting architecture. A property of the architecture, not of the deterioration.
- Visibility gap. The difference between what is observable in principle and what is interpreted in practice. Generated by attention allocation rather than by information scarcity, and widened by silence mechanisms operating below the level of conscious decision.
- Interpretive capacity. The demonstrated ability of a governance tier to convert an observed anomaly into a warning judgement. Measured by behaviour under prior anomalies, not by structure. This is the point of departure from governance scoring.
- Warning threshold. The declared level of convergence at which a warning is issued. Declared in advance, because a threshold set after the event is hindsight and not warning.
- Transmission pathway. The directional route by which deterioration in one domain generates deterioration in an adjacent domain. Supplied by Part 2.

## 3.3 Scope conditions

The discipline is asserted to apply where the following hold, and is not asserted to apply otherwise.

- A governance tier exists that is structurally separated from operational management, so that information must travel an escalation path to reach decision authority. In an owner managed firm with no such separation, the visibility gap has no referent.
- The deterioration is gradual rather than instantaneous. The discipline has nothing to say about failures with no incubation period.
- A minimum observation window exists. Trajectory cannot be estimated from a single observation, which materially limits use at first contact and in due diligence.
- The governance tier retains authority to act. Where authority is already captured, the discipline degrades from an early warning instrument into a forensic one.
- The indicator set is lawfully obtainable. Fragility Intelligence indicators are records of the conduct of identifiable people. Under the Protection of Personal Information Act 4 of 2013 (POPIA) and the General Data Protection Regulation (GDPR) these are personal information processed for a purpose the data subject did not anticipate. Processing is not unlawful in principle, but it is conditional on purpose specification, minimisation and a defensible lawful basis. A capability that

measures escalation behaviour without a lawful basis is a surveillance instrument, and a regulator will draw that distinction whether or not the discipline draws it first.

### 3.4 What Fragility Intelligence is not

- It is not a prediction of failure. A warning is a judgement issued under uncertainty, and it is not falsified by the non occurrence of the outcome where intervention followed the warning.
- It is not a governance score, and must not be allowed to become one. The moment an assessment is expressed as a single figure on which organisations are ranked, the indicators become management targets rather than observations. This is the most probable failure mode of the discipline's own commercialisation.
- It is not a replacement for financial distress prediction. The relationship is complementary and incremental.
- It is not a substitute for the governance apparatus it interprets. It sits above that apparatus, depends on it for collection, and inherits every deficiency in the underlying record.

### 3.5 The Fragility Interpretation Cycle

Eight stages. They are not sequential in operation. They run concurrently, and each has its own characteristic failure mode.

1. Signal acquisition. Indicators bearing on interpretive capacity: escalation latency, the disposition of dismissed anomalies, concentration of approval authority, exceptions granted against declared policy, the distance between an anomaly's originator and the governance tier, and what is raised informally but never recorded.
2. Signal validation. Whether an indicator reflects the condition it purports to reflect.
3. Signal interpretation. Conversion of a validated indicator into a judgement about deterioration. The literature identifies this as the binding constraint, and no methodology has ever made it reliable.
4. Convergence assessment. Whether multiple independent indicators are moving consistently, and whether the movement is concentration or transmission.
5. Warning judgement. Issue of a formal warning against a pre declared threshold, stated with its confidence and its basis.
6. Transmission projection. Application of the model at Part 2 to state where the deterioration will surface next and when the intervention window closes. Neither the general warning literature nor the distress models contain this stage.
7. Response. The action taken. This stage fails independently of the quality of everything preceding it.
8. Adaptive learning. Revision of thresholds and weights against outcome. This is where the false positive record accumulates and where the empirical credibility of the discipline ultimately rests.

The failures compound. A signal not acquired cannot be validated. An interpretation not converged into a warning is a private opinion. A warning that produces no response is indistinguishable in outcome from a warning never issued. An organisation that does not accumulate the outcome record cannot improve any earlier stage, so the chain does not merely fail, it fails permanently.

# Part 4. The capability

## 4.1 Four levels

Fragility Intelligence is an organisational capability rather than an individual role.

| Level | Node | Function |
|---|---|---|
| 1 | Every participant | Sensor. Observes and raises |
| 2 | Integrating function | Registers, cross reads across domains, classifies and routes |
| 3 | Executive management | Response ownership |
| 4 | The board | Oversight and challenge |

This answers who does the work. It does not answer the harder question, which is what happens when fragility originates at, or is concealed by, the very node the signal would ordinarily pass through. That question is not peripheral. It is the central one. Every significant governance failure in the South African record shares the same structural feature: the signal existed, the signal was raised, and the signal was absorbed by the node responsible for carrying it forward. The failure was never sensory. It was architectural.

## 4.2 Where the coordinating function sits

The function maintains the signal record, cross reads across domains, applies the classes and routing rules, keeps the evidence trail and prepares the board products.

It may be hosted inside risk, governance or the company secretariat, but the hosting decision must be conditional. The framework must state in advance where the mandate reverts to if the host function is itself the subject of a signal. Without that reversion clause the function is captured by the first serious matter it handles. Where the function sits in the office of the Chief Risk Officer, Silo 3 at 5.6 states the single exception to universal registration.

The function must have a protected line to the relevant committee chair that does not depend on the permission of any executive.

## 4.3 Three usages that are commonly confused

- Levels. The four level capability model at 4.1. Who does the work.
- Stages. The eight stage interpretation cycle at 3.5. What the analysis does.
- Layers. The five software layers at 6.3. How the instrument is built.

The escalation architecture at Part 5 answers a fourth question that none of the three answers: where the signal goes when the node that should receive it is the subject of it.

# Part 5. The Fragility Escalation Architecture

## 5.1 Why linear escalation fails

Conventional escalation is linear and upward, and assumes each node has both the capacity and the incentive to transmit. That assumption is unsafe. Filtration behaviour is observable, recurrent and patterned.

| Filtration property | What it does |
|---|---|
| Latency | Delays a signal until it is no longer actionable |
| Reclassification | Converts a systemic signal into an isolated incident |
| Originator attack | Removes the person rather than addressing the substance |
| Referral looping | Returns the signal to the node it came from |
| Substitution | Replaces the reported matter with a narrower and more manageable one |
| Silence with continuation | Permits the conduct to persist while the signal is treated as closed by absence of response |

Each describes a failure of transmission rather than of detection. A linear model cannot detect any of them, because it treats the channel as an assumption rather than as an object of measurement. The architecture corrects this by treating the channel as itself a subject of surveillance.

**Under the architecture, obstruction of a signal is a signal.**

### The three failure modes the architecture must survive

- Subject capture. The node designated to receive the signal is the subject of it. Standard routing delivers the signal to the person with the strongest interest in suppressing it.
- Appointment dependency. The receiving node depends on the subject for appointment, remuneration, mandate or tenure. Formal independence exists on the organogram but not in incentive.
- Instrument capture. The subject controls the instruments through which a signal becomes a record: the agenda, the minutes, the register, the legal opinion, the settlement agreement or the confidentiality clause. The signal is heard but never recorded, and therefore never happened.

## 5.2 The four routing rules

Deliberately few, because a rule set that cannot be recalled under pressure will not be applied under pressure. Each is testable after the fact by an independent reviewer.

### Rule One. Subject exclusion

No node may receive, assess, classify, dispose of or record the closure of a signal in which that node, its direct reports, or its immediate family or associated interests are the subject. Exclusion is automatic on receipt and does not depend on voluntary recusal. The obligation to identify the conflict rests with the receiving node and, in parallel, with the Fragility Intelligence function, which maintains the exclusion map.

Exclusion covers more than receipt. The subject must not be able to see that a signal moved, must not be able to delay it, and must not be able to identify who raised it.

### Rule Two. Single step displacement

Where a node is excluded, the signal transfers laterally to the nearest structurally independent node of equal or greater authority. It does not travel upward through the excluded node, and it does not skip to

the terminal node while an intact intermediate node exists. Independence is tested on appointment, remuneration and tenure. A node dependent on the subject for any one of the three is not independent, however senior it appears.

#### Rule Three. Immutable registration at first contact

Every signal is registered at first contact with any node, before assessment and before any judgement on merit. Registration captures a sequential reference, date and time, the receiving node, the substance in the originator's own wording, and the domains implicated. The register is append only. Reclassification is permitted only as an additional dated entry preserving the original alongside it.

This counters reclassification and substitution directly. Both depend on the original wording becoming unavailable. If the original wording survives, reclassification becomes visible as an act rather than operating as a fact.

#### Rule Four. Terminal node designation

Every path terminates at a node holding authority to act and not dependent on the subject for its own appointment, remuneration or tenure. Where no internal node satisfies both conditions, the terminal node is external and is named in advance for each silo.

**Naming it in advance is what converts transmission from an act of individual defiance into a recorded step in a designed path. An organisation that has not named its terminal nodes has not designed an escalation path. It has designed a queue that ends at whoever is most senior, which in cases of executive or board fragility is the subject.**

#### The default rule. Escalation, not lapse

A signal is never closed by absence of a response. Closure requires a recorded disposition naming the deciding node, the reasoning and any corrective action. Where a threshold expires without disposition, the signal escalates automatically. The default state of an unanswered signal is movement, not expiry. This single provision defeats silence with continuation, which is otherwise the most effective and least detectable of the six properties precisely because it requires no action at all.

### 5.3 Closure standard

A matter is not closed because management says it has been dealt with. Closure requires a recorded decision and a named owner, a deadline that has been met, evidence of implementation, independent verification where the matter is material, confirmation that the transmission pathway has been interrupted rather than the symptom removed, a reassessment of residual fragility, and formal closure by the node that held the authority to decide.

### 5.4 Signal classification

Signals are classified by the authority required to dispose of them. Not by subject matter, which would reproduce the silo problem the function exists to solve. Not by apparent severity, which invites the receiving node to determine its own jurisdiction, and that is the mechanism of reclassification.

| Class | Condition | Entry point | Disposition authority |
|---|---|---|---|
| A | Single domain, no cross domain correlation | Functional head, registered to the FI function | Functional head |
| B | Correlation across two or more domains, or recurrence of a Class A signal | FI function | Executive committee, with the FI assessment tabled unaltered |
| C | An executive is the subject, or the executive layer is structurally unable to act | Chair of the Audit Committee, directly and in writing | Audit Committee sitting without the subject present |

| Class | Condition | Entry point | Disposition authority |
|---|---|---|---|
| D | The Chairman, a board member, or the board collectively is the subject | Lead Independent Director and, in parallel, Chair of the Audit Committee | Board in camera with the subject recused, then the named external terminal node |
| E | Filtration. Any of the six properties observed in the handling of a signal of any class | FI function and Chair of the Audit Committee simultaneously | Mandatory custody transfer. Original class escalates by one level and the filtration event registers as a separate signal |

Class E is the distinguishing element. In every other governance model an obstructed signal produces, at best, a repeat attempt through the same channel. Here obstruction is not a setback in the handling of the original signal. It is a second and independently registered signal, with its own reference number, its own subject and its own escalation path. The obstruction is evidence.

This produces a property no conventional assurance function possesses. The architecture generates data about its own integrity. An organisation running it for twelve months can state how many signals were registered, how many were disposed of within threshold, how many escalated by default, how many filtration events were recorded, and where in the structure those events concentrated. That last figure is a direct reading of the stabiliser, independent of any statement management chooses to make about it.

## 5.5 Thresholds

| Stage | Threshold | Consequence of breach |
|---|---|---|
| Registration after first contact | 1 working day | Class E filtration event against the receiving node |
| Written acknowledgement to originator | 5 working days | Automatic escalation to the next node in the path |
| Recorded disposition, Class A and B | 20 working days | Automatic escalation and Class E registration |
| Recorded disposition, Class C and D | 10 working days | Automatic transfer to the named external terminal node |
| Adverse action against a registered originator | 90 day window | Deemed originator attack. Custody transfers and the burden of justification reverses onto the acting node |

The ninety day provision is the operative protection for Level 1. Any adverse action against a registered originator within ninety days of registration is deemed an originator attack unless the acting node can show the action was initiated, documented and approved before the registration date. Adverse action includes suspension, disciplinary referral, performance downgrade, withdrawal of duties or delegated authority, withdrawal of clearance or system access, restructuring that eliminates or relocates the role, and non renewal of a contract. The burden sits with the organisation, not the originator.

**Without this reversal, every other provision in the architecture is advisory.**

## 5.6 The ten origination silos

Each silo is defined by where fragility originates or is concealed, not by where it is eventually observed. The domain column is the join to Part 2 and determines which correlation tests apply. Full silo detail, including fragility signatures, escalation paths, intervention authorities and filtration tests, remains in the companion architecture document.

**Jurisdictional note.** *The statutory terminal nodes are those of the Republic of South Africa. The routing logic is jurisdiction neutral. The terminal nodes are not.*

| Origination silo | Class | Domain | First structurally independent node | Terminal node |
|---|---|---|---|---|
| 1. Chairman of the Board | D | 1 | Lead Independent Director and Chair of the Audit Committee in parallel, subject to an independence test on the Lead Independent Director | External auditor under the section 45 reportable irregularity duty, Independent Regulatory Board for Auditors (IRBA), Johannesburg Stock Exchange (JSE) and sponsor, Auditor General and executive authority. Removal requires shareholders |
| 2. Chief Executive Officer | C | 1 | Chair of the Audit Committee, with the Chief Audit Executive providing evidential assessment through the functional line | External auditor, IRBA, JSE, and Protected Disclosures Act channels including legal adviser, Public Protector and Auditor General |
| 3. Risk function and Chief Risk Officer | C | 1 | Chief Audit Executive, since Internal Audit already holds the mandate to assess risk management effectiveness under combined assurance | Independent external quality assessment commissioned by the Audit Committee. Prudential Authority for regulated institutions |
| 4. Human Resource Management | B or C | 3 | Social and Ethics Committee, with parallel referral to Remuneration on settlement patterns and Audit on aggregate value | Commission for Conciliation, Mediation and Arbitration (CCMA) and Labour Court, Social and Ethics Committee report to shareholders, Information Regulator where data protection is invoked to obstruct assurance |
| 5. Finance and Chief Financial Officer | C | 2 | Chief Audit Executive, then the private session between the Audit Committee and the external auditor held without management present | External auditor under section 45, IRBA, JSE, Financial Sector Conduct Authority (FSCA) |
| 6. Internal Audit | C | 1 | Chair of the Audit Committee directly, with registration to the FI function in parallel rather than sequentially | External quality assessment, then shareholders at the annual general meeting, who elect Audit Committee members annually |
| 7. Company Secretary, Legal and Compliance | C or D | 1 | Chair of the Audit Committee, who instructs separate counsel where the subject instructed the original opinion | Legal Practice Council, direct filing with the applicable regulator, external auditor on completeness of the minute record |
| 8. Security, Information Technology and Cyber | B or C | 4 | Chief Risk Officer and Chief Audit Executive jointly, reporting to the Chair of the Risk Committee | Information Regulator under the section 22 notification duty, the insurer, the Transported Asset Protection Association (TAPA) certification body for cargo environments, South African Police Service |
| 9. Procurement and Supply Chain | B or C | 2 and 4 | FI function performs the aggregation, then Internal Audit assesses the aggregated pattern rather than a transaction sample | Auditor General and National Treasury for public entities, forensic review appointed by the Audit Committee, Directorate for Priority Crime Investigation, Competition Commission on collusion |
| 10. Shareholder, owner or executive | D | 1 | None. Internal escalation is exhausted. The required step is a | External auditor and Auditor General, parliamentary portfolio or standing |

| Origination silo | Class | Domain | First structurally independent node | Terminal node |
|---|---|---|---|---|
| authority | | | recorded board resolution and a minuted communication carrying a ten day threshold | committee, Public Protector, sector regulator, JSE and minority shareholders, ultimately the public record |

Silo 10 is stated honestly and must remain so in any client facing derivation. No internal authority exists where the shareholder or executive authority is the source. The objective there is documented, dated, attributable and external transmission rather than resolution. That is a lower ambition than in the other nine silos, and saying so is not a weakness of the architecture. An architecture that promised internal resolution in Silo 10 would promise what it cannot deliver.

## 5.7 The custody transfer protocol

Class E events trigger custody transfer. Responsibility moves away from the node handling the signal, and that node loses the ability to dispose of it.

1. Automatic operation. Transfer occurs on the triggering condition, not on a decision that transfer is warranted. A transfer requiring approval can be refused by the node most likely to be the subject.
2. Notification without discretion. The FI function notifies the receiving node, the originator and the register simultaneously. The transferring node is notified but does not approve.
3. Evidence preservation. The FI function takes custody of the registration record, correspondence, classification history and documents produced. Preservation notice issues immediately, and destruction or alteration after notice is itself a Class E event of the most serious kind.
4. Escalation by one class. Class B filtered becomes C. Class C filtered becomes D.

**The fourth provision is the operative one and should be stated plainly to any board considering adoption. Under conventional escalation, obstructing a signal reduces the probability that it is heard. Under this architecture, obstructing a signal increases both the probability that it is heard and the seniority of the audience that hears it, and adds the obstructing node as the subject of a second signal. The architecture does not appeal to the good faith of intermediate nodes. It removes the payoff from bad faith.**

## 5.8 The four instruments

Each is a document, each is auditable, and none requires technology, although all four benefit from it.

- The Signal Register. Append only. Reference, date and time of first contact, receiving node, substance in the originator's own wording, domains implicated, class on receipt, class history, custody history, threshold dates and disposition. Amendment is impossible by design. Existence and status of every entry is visible to the FI function, the Audit Committee and the external auditor without request.
- The Filtration Log. Every Class E event, the property observed, the node concerned and the outcome. This is the primary output of the architecture as a measurement instrument. Where filtration events concentrate in one node across cycles, that concentration is a finding about the node and does not require any individual case to be proven.
- The Custody Transfer Record. Each transfer, the triggering condition, transferring and receiving nodes, the preservation notice and the class escalation. Reviewed by the external auditor as part of the control environment assessment, since a pattern of transfers bears directly on the reliability of management representations.
- The Originator Protection Schedule. Every registered originator, the registration date and the ninety day window. Any adverse action against a person on the schedule requires prior written

clearance from the Chair of the Social and Ethics Committee. Held by the FI function and not accessible to line management. Without it, the instruction that every employee is a sensor asks employees to accept a risk the organisation has not undertaken to carry.

## 5.9 The eight board approvals

The architecture cannot be implemented by the risk function acting alone. Each approval alters an existing governance instrument.

1. Approve the Fragility Intelligence charter, establishing the function, its independence, its registration mandate and its reporting line to the Audit Committee in addition to any executive line.
2. Amend the Audit Committee terms of reference to establish direct receipt of Class C, D and E signals, and to confirm authority to appoint investigators and reviewers without management concurrence.
3. Amend the Social and Ethics Committee terms of reference to establish receipt of human resource pattern signals and clearance authority over adverse action against registered originators.
4. Adopt the routing rules, classes and thresholds as a board approved standard, so that automatic escalation on breach operates by prior board authority rather than by individual initiative.
5. Name the external terminal node for each silo in advance, and record that transmission to a named terminal node in accordance with the architecture is authorised conduct and not a breach of any confidentiality obligation owed to the organisation.
6. Prohibit confidentiality clauses in settlement agreements arising from registered signals, and require Remuneration Committee approval for any settlement involving a registered originator.
7. Reserve waiver of legal professional privilege to the board or the Audit Committee, and prohibit the instruction of external counsel by any person who is the subject of the matter on which counsel is instructed.
8. Adopt the Filtration Log as a standing Audit Committee report and as a disclosed element of annual governance reporting, whether or not any filtration event occurred in the period.

**The eighth decision is the one that most reliably indicates whether an organisation has adopted the architecture or merely approved it. A board willing to disclose its own filtration record has accepted that the measurement applies to itself. A board that adopts the first seven and declines the eighth has installed a detection capability while retaining the option to suppress its output, which is the position it occupied before adoption.**

## 5.10 The relationship to King V

The architecture requires no new statutory powers. It requires the deliberate use of three provisions that already exist and are all underused.

- Election of Audit Committee members by shareholders under section 94 of the Companies Act 71 of 2008, which makes the committee the strongest structurally independent internal node available.
- The statutory Social and Ethics Committee under section 72(4) and Regulation 43, with its direct reporting line to shareholders.
- The reportable irregularity duty of the external auditor under section 45 of the Auditing Profession Act 26 of 2005.

King V governs how boards should behave. Fragility Intelligence measures whether they did. The correct position is the diagnostic layer beneath the code, not a competing code. That these three provisions are underused is a diagnostic claim, not a reform proposal.

# Part 6. Measurement and build

## 6.1 The governing design principle

The software instruments judgement. It does not replace it. If the framework is built as an algorithm that emits a fragility score, the discipline is hollowed out and becomes another dashboard, which is the symptom management the discipline was created to expose. The system captures evidence, computes what is genuinely computable, and forces an analyst to author the interpretation. A posture cannot be emitted without a named analyst and a recorded reasoning trace.

This is also the commercial moat. Anyone can build a scoring dashboard. A disciplined evidence and reasoning instrument, owned by the originator of the discipline, is far harder to copy.

## 6.2 The unit of record

The unit of record is not the risk. It is the signal and its handling trace. Every governance, risk and compliance platform in the market records risks, controls and residual ratings. None records what the organisation did when it was told something. That single shift in the data model is the whole product.

The schema is built around two joined families. Family One holds externally authored substantive signals: audit findings, regulator correspondence, whistleblower reports, litigation, ratings actions and credible reporting. Family Two holds the filtration behaviour observable in the handling of those signals. The value sits in the join.

## 6.3 Layer architecture

| Layer | Function | Build character |
|---|---|---|
| 1. Signal capture | Registers Family One signals | Structured intake, document store, provenance and confirmation status on every record |
| 2. Handling trace | Records what each governance tier did with each signal, event by event, with dates and artefacts | The core differentiator. This is the table no governance, risk and compliance platform holds |
| 3. Measurement | Computes the six filtration properties, Originator Distance and the derived indices | Deterministic engine. Every score traceable to underlying events |
| 4. Interpretation | Analyst assigns posture, records reasoning, registers a locked forward prediction | Human authored and mandatory. The system will not emit a posture without it |
| 5. Output | Transmission stage finding, trajectory view, tier filtration profile, board briefing pack | Report generation, comparative views, export |

The escalation architecture sits beneath Layers 2 and 3. It is not a sixth layer. It supplies the reference path against which Layer 2 events are compared, which is what makes several Layer 3 computations possible at all.

## 6.4 What the architecture makes computable

Three of the six filtration properties are computable from dated artefacts alone. Three required analyst coding, and two of those required it only because the schema had no reference path. The architecture supplies the reference. Six entities are added: node, silo, required action baseline, class history, custody transfer and originator protection.

The node registry is the most consequential. It records, for each governance node, who appoints it, who remunerates it and who controls its tenure. This is what makes structural independence computable rather than asserted.

Four measures then require no analyst coding at all:

1. Subject exclusion violations. Handling events in which the acting node was the subject, or a dependent of the subject, of the signal it was handling. Likely the single most damaging figure the instrument can produce about a governance structure, and it requires no assertion about anyone's intent.
2. Path deviation index. The proportion of handling events that departed from the baseline path for the class, with deviation type recorded. This is the computed form of substitution, and it distinguishes a legitimate referral from a loop through a dependent node.
3. Threshold breach rate per node. Latency expressed as a node attribute rather than a signal attribute.
4. Node independence score. Computed from the appointment, remuneration and tenure graph. It identifies, in advance of any signal, which paths in a given entity are already closed.

The fourth has a commercial property the others do not. It can be produced from public documents, before any mandate, before any privilege posture is settled, and without access to a single minute. It needs only an organogram and a set of terms of reference, which makes it the cheapest entry point to a board conversation the framework has produced.

### 6.5 Originator Distance and the paradox measure

Originator Distance is a composite of measurable attributes rather than an impression, recorded per originator and per signal: organisational distance, financial distance, appointment distance and consequence distance.

The signal filter paradox then becomes a computed diagnostic. If filtration intensity rises as Originator Distance rises, the filter is operating against independence rather than against error. That relationship is measurable across a signal population and is the strongest single output the instrument can produce, because it converts a proposition into an instrument reading.

### 6.6 Index hierarchy

- Signal Filtration Index, computed per signal from the six properties.
- Tier Filtration Profile, computed per governance tier, answering which tier is functioning as the filter. This is often the finding a board most needs and least expects. The tier set is supplied by the ten silos.
- Fragility Posture, analyst authored for a period, expressed as transmission stage, active pathway and stabiliser availability.
- Paradox Coefficient, the relationship between Originator Distance and filtration intensity across the signal population.
- Node Independence Score, computed per node, identifying closed paths in advance of any signal.

**The domains supply the correlation axes and the transmission pathway for these outputs. They do not supply a score that is combined with them. Structural integration, not arithmetical.**

### 6.7 The Prediction Register

A methodological weakness of any deterioration framework is that it explains collapses after they occur. Retrospective coding of a known failure will always look convincing. The remedy is built into the software rather than promised in a paper.

The Prediction Register allows an analyst to lock a timestamped forward posture that cannot subsequently be edited, and later scores it against observed outcomes. It makes the propositions testable in live operation, produces a defensible accuracy record over time, and is a credibility asset no competitor can retrofit, because it requires elapsed time to accumulate.

## 6.8 The market fork

The subject of measurement cannot be the operator of the instrument. A board will not honestly record its own latency, reclassification and originator attack behaviour. Any self assessment version measures the filter using the filter.

The defensible primary markets are therefore third party positions: investors and asset owners performing pre commitment or ongoing assessment, regulators and shareholder departments, assurance providers and audit committees seeking independent review, litigation and forensic support, and boards commissioning an external read on themselves. A self assessment mode may exist, but it must be labelled a preparation tool and not a posture assessment.

### Reconciliation with the architecture

An entity adopting the architecture keeps its own signal register and its own filtration log, which is on its face the filter recording its own filtration. The objection is correct and is answered in the design rather than deflected.

The architecture and the instrument measure different things. The architecture is a governance design an entity adopts and operates. The instrument measures whether that design actually operated, and does so from artefacts rather than from the entity's own log. An adopted architecture therefore does not become a self assessment. It becomes an audit surface, and a better one than currently exists, because a stated path makes departure from the path visible.

Two consequences follow, both commercial. An entity that has adopted the architecture is a materially better client for the evaluation service, not a worse one, because the baseline is its own published standard rather than an external opinion. And a filtration log with no entries after a full reporting cycle is not evidence of an absence of filtration. It is evidence the log is not in use, and should be treated with the same scepticism as a risk register on which nothing has moved.

## 6.9 Build risk register

- Interpretive hollowing. The system drifts toward a number clients quote without the reasoning. Mitigation: no posture without an authored interpretation, and reports that surface reasoning before finding.
- Legal exposure. Coding originator attack and substitution involves assertions about named individuals and bodies. Mitigation: every record carries an evidence artefact and a confirmation status, with confirmed fact and contested allegation held separately.
- Coder reliability. Two analysts coding the same signal set must reach comparable results, or the instrument is not an instrument. Mitigation: dual coding on contested classes and a recorded agreement measure.
- Retrospective bias. Mitigation: the Prediction Register, and a rule that published validation rests on locked forward postures rather than reconstructed cases.
- Scope creep into governance, risk and compliance. The moment the product holds risk registers and controls it becomes a weak competitor in a crowded market. Mitigation: hold the signal and handling trace as the only unit of record.
- Baseline capture cost. If a bespoke baseline must be built for every engagement, the method does not scale. Mitigation: a shipped South African reference matrix with a per entity override layer.

# Part 7. Falsifiability

The framework carries two proposition sets. The theory propositions test the discipline. The architecture propositions test the routing design. They are stated separately because they fail separately.

## 7.1 Theory propositions

| No. | Proposition | Falsified if |
|---|---|---|
| 1 | Behavioural indicators dominate structural indicators. Escalation latency and the disposition of dismissed anomalies predict failure better than board composition, committee presence and code compliance | In a matched sample of failed and surviving organisations, structural indicators achieve equal or superior discrimination to behavioural indicators |
| 2 | Governance behaviour adds incremental power and lead time to financial distress models. The claim is incremental, not competitive | The addition of behavioural indicators to a baseline distress model produces no significant improvement in discrimination, or no extension of detection lead time |
| 3 | Interpretive capacity is independent of structural adequacy. Well structured boards are not on average better interpreters of deterioration signals | A positive correlation of practical significance is observed between structural ratings and measured interpretive capacity |
| 4 | Convergence outperforms severity. Convergence of weak indicators across independent domains predicts failure better than the severity of any single strong indicator | Single indicator severity achieves equal or superior predictive accuracy to a convergence measure in the same sample |
| 5 | Originator distance predicts dismissal, independently of the anomaly's materiality | Dismissal rates show no relationship to originator distance once materiality is controlled for |
| 6 | Warning precedes response failure more often than detection failure. Failure is predominantly a response failure | A systematic review of failure inquiries finds accurate prior warnings reaching decision authority were absent in the majority of cases |

Proposition 2 is the one on which the claim to a distinct jurisdiction rests, and it is expected to be the hardest to satisfy. If it fails, the discipline is a redescription of an existing capability and should be abandoned.

Proposition 6 carries an uncomfortable implication that should be stated rather than concealed. If it is true, then improving detection, which is what the discipline primarily offers, addresses the smaller half of the problem. The commercial interest of the author lies in Proposition 6 being false. It is included because the evidence currently favours it.

## 7.2 Architecture propositions

1. In organisations that subsequently experienced governance failure, signals bearing on the failure were registered or raised in advance, and the failure of transmission is documented in the record of handling rather than in the absence of the signal.
2. The concentration of filtration events within a node predicts subsequent adverse outcomes originating in that node, with lead time exceeding that of conventional risk register movement or distress prediction.

3. Organisations in which the escalation path terminates at a node dependent on the subject exhibit higher rates of unresolved signals than organisations in which the terminal node is structurally independent, controlling for sector and size.

### 7.3 The six documentary tests

An external reviewer can test adoption without relying on management assertion.

- Does the Signal Register exist, and is it append only.
- Are Class C and D entry points published, and have they been used.
- Does the Filtration Log exist, and does it contain entries.
- Is the Originator Protection Schedule maintained, and has clearance been sought under it.
- Have terminal nodes been named in advance by board resolution.
- Were thresholds breached, and did automatic escalation occur on breach.

**An organisation returning six affirmative answers has an escalation architecture. An organisation returning six negative answers has an escalation policy. That distinction is the entire subject of Part 5.**

### 7.4 Threats to the research programme

- Intelligence failure may be structural rather than remediable. If warning failure is inherent to the relationship between analysis and decision, the discipline improves the input to a process whose constraint lies elsewhere.
- Hindsight bias and selection on the dependent variable. Retrospective coding of known failures will always look convincing. The Prediction Register is the structural answer.
- The capability becomes the ritual it diagnoses. The machinery of verification hardens into a routine that produces reports, and tabling the report becomes the proof that oversight is working. This is the most probable long term failure mode.
- The false positive problem. A warning discipline with an unmeasured false alarm rate is not a discipline. The adaptive learning stage is where that record must accumulate, and it is currently empty.

# Part 8. Document control and terminology

## 8.1 Documents governed by this master

| Document | Version | Standing |
|---|---|---|
| This master framework document | 2.0, 28 August 2026 | Controlling document. Amend here first |
| WP-2026-007, Fragility Intelligence | 2.0, July 2026 | Citable scholarly source for the definition, scope conditions and propositions. Requires a note on the domain and stabiliser distinction at next revision |
| Fragility Escalation Architecture | 1.0, 10 August 2026 | Companion document holding full silo detail. Escalation step numbers should restart within each silo |
| FI Implementation File | 0.2, 10 August 2026 | Retained as the build and commercial working file. Framework content superseded by this master |
| SRA-I schematic | Finalised 17 July 2026 | Self contained HTML file with inline scalable vector graphics. Do not redesign. Label edits only, per 8.2 |
| FI Implementation Loop, single slide | 2, corrected 10 August 2026 | Master pptx held by Dr André Du Venage. Do not rebuild. Shows the intact channel only |
| Board training module, escalation architecture | Insert drafted, not merged | Written for Board Training Plan 2.0. Requires renumbering to the host sequence |
| Board paper for approval | 0.1, 28 August 2026 | Rebuild against Parts 2 and 5 of this master |

## 8.2 Terminology now fixed

- SRA-I is Strategic Risk Architecture Integrated. C-SRA-I is Corporate Strategic Risk Architecture Integrated. No other expansion is used.
- Four domains and one systemic stabiliser. The stabiliser is not called a pillar, and the word pillar is retired from framework documents.
- Levels are the capability model, stages are the interpretation cycle, layers are the software. The three are not interchangeable.
- Fragility Intelligence and the SRA-I family are one system, not adjacent instruments. The prohibition that survives is against collapsing Fragility Intelligence into domain scoring.

---

*The risk was never where you were looking. It was in the path between the person who saw it and the person who could have stopped it.*