

ADAPTIVE COMPLIANCE • EXECUTIVE TOOLKIT

From argument to operating discipline

Seven executive diagnostics for payments, AI, models, transformation and global compliance

DIAGNOSE Expose where evidence is weak	DECIDE Name the accountable choice	ADAPT Set the trigger to reassess
--	--	---

Micheal Sheehy

2026 edition • Vendor-neutral • Designed for executive working sessions

OPERATING GUIDE

How to use the toolkit

Use each tool to convert a broad risk discussion into an evidence-backed decision with a named owner.

THE STANDARD

A score is not the output. The output is a decision, the evidence behind it and the condition that would make the organization reconsider.

Choose the right starting point

TRIGGER	START WITH	DECISION SUPPORTED
Richer payment messages, ISO 20022 or virtual accounts	01 · Payment Transparency	Where data breaks undermine identity, purpose or traceability.
Copilot, model or agent entering a regulated workflow	02 · AI & Agent Governance	What authority is permitted and what evidence is required before release.
Model performance is changing or outcomes are disputed	03 · Model Health & Drift	Whether to continue, tune, constrain, validate or stop the model.
New platform, migration or program reset	04 · Transformation Readiness	Whether the program is ready to move through the next gate.
Global hubs, regional growth or central bottlenecks	05 · Global Operating Model	Which capabilities and decisions belong globally, regionally or locally.
Board oversight of high-impact AI	06 · Board Oversight	What the board should approve, challenge or require management to evidence.
Transformation needs traction in one quarter	07 · 30/60/90-Day Plan	What will change, who owns it and what proves improvement.

Working-session discipline

- Pre-read: circulate the relevant tool, baseline data and known issues at least two working days in advance.
- Score independently: collect individual views before the meeting so hierarchy does not manufacture agreement.
- Challenge the evidence: require a source, owner and date for every strong claim or high score.
- Close explicitly: record the decision, dissent, residual risk, owner, due date and reassessment trigger.

OPERATING GUIDE

Scoring, confidence and evidence

A common standard prevents teams from using the same score to describe very different realities.

LEVEL	ANCHOR	WHAT EXISTS	EVIDENCE EXPECTATION	LEADERSHIP IMPLICATION
1	Unclear	No shared standard; ownership or intended outcome is disputed.	Anecdote, incomplete inventory or no reliable record.	Do not scale. Establish ownership and the minimum standard.
2	Emerging	Practice exists but depends on individuals or local workarounds.	Examples exist; coverage and consistency are unknown.	Stabilize the process and expose variation.
3	Defined	Documented standard, owner and workflow; application is reasonably consistent.	Policy, process, inventory and sampled execution evidence.	Prove performance and manage exceptions.
4	Monitored	Performance, exceptions and thresholds are visible; action is governed.	Current metrics, trends, thresholds, decisions and closure evidence.	Test whether signals drive timely decisions.
5	Adaptive	The control learns from evidence and changes through accountable feedback.	Closed-loop evidence showing detection, decision, change and validation.	Protect against complacency and uncontrolled optimization.

Confidence is separate from maturity

CONFIDENCE	USE WHEN	REQUIRED RESPONSE
High	Evidence is current, representative, attributable and independently challengeable.	Use the score; retain the evidence reference.
Medium	Evidence is directionally useful but incomplete, stale or limited to selected populations.	Use provisionally; create a dated evidence gap action.
Low	The score depends on assertion, a narrow sample or an owner's judgment.	Treat as unknown; do not use the score to justify expansion.

FACILITATOR CHALLENGE

Where would an independent reviewer look to reproduce this answer—and what might they conclude differently?

Executive decision record

DECISION FIELD	WORKING RECORD
Scope assessed	_____
Facilitator	_____
Participants	_____
Decision forum	_____
Evidence cut-off date	_____

TOOL 01

Payment Transparency Readiness

Determine whether payment data can support identity, purpose and contextual decisions before risk disappears into the transaction chain.

USE WHEN	PRIMARY OUTPUT
Preparing for structured payment data, cross-border growth, virtual-account issuance or stronger transparency enforcement.	A data-break heatmap, control-placement decision and accountable remediation plan.

Follow the data, not the organizational chart

INITIATION	VALIDATION	ROUTING	SCREENING	SETTLEMENT	MONITORING
Who and why enter the message.	Required fields and format are checked.	Data is transformed and passed.	Risk is assessed before release.	Value and message reach destination.	Behavior and outcomes feed learning.

Five control outcomes

OUTCOME	EXECUTIVE TEST	FAILURE SIGNAL
Attributable identity	Can the institution identify the parties, intermediaries and responsible customer behind the payment?	Alias, free text, pooled identity or an issued account identifier cannot be resolved.
Meaningful purpose	Can the stated purpose be compared with customer profile, product and behavior?	Narrative is generic, inconsistent or unavailable to the decision point.
Preserved context	Does relevant information survive transformation, routing and settlement?	Fields are truncated, overwritten, mapped inconsistently or dropped across rails.
Timely intervention	Which risks can be addressed before execution rather than discovered downstream?	The decisive information exists but reaches monitoring only after value moves.
Traceable accountability	Can every exception be assigned to an institution, control owner and remediation path?	Missing data is tolerated without measurement, consequence or feedback.

VIRTUAL-ACCOUNT COMPLEXITY

A virtual account is not merely another account number. The control must preserve the link between the issued identifier, underlying customer, beneficial ownership, permitted purpose and institution responsible for monitoring.

Immediate red flags

- The same payment can be attributed differently by onboarding, operations, sanctions and transaction monitoring.
- Message-quality exceptions are measured as processing defects but not evaluated as control failures.
- Virtual-account ownership can be reconstructed only through manual investigation or local knowledge.
- Commercial pressure can override missing-data rules without a documented risk acceptance.

TOOL 01 • DIAGNOSTIC

Payment transparency maturity matrix

Score each dimension 1–5, record confidence and cite the evidence. The anchors below distinguish weak, defined and adaptive practice.

DIMENSION	1 • UNCLEAR	3 • DEFINED	5 • ADAPTIVE
Identity integrity	Party roles and identifiers vary by rail or system.	Common definitions and validation exist for material flows.	Identity quality is monitored end to end; breaks change controls and upstream design.
Purpose	Purpose is optional, generic or free text only.	Purpose standards exist for priority products and corridors.	Purpose is structured, tested against context and improved through investigation outcomes.
Data structure	Material fields rely on free text or local mapping.	Required fields, formats and ownership are documented.	Structured data is governed as a control asset with quality thresholds and lineage.
Continuity	Loss or transformation across the chain is unknown.	Material transformations and handoffs are mapped.	Automated reconciliation detects loss, mutation and unexpected routing changes.
Virtual accounts	Issued identifiers are not consistently linked to the underlying customer.	Ownership, purpose and issuer responsibility are documented.	Linkage is real-time, testable and available to screening, monitoring and investigations.
Control placement	Controls run where systems happen to permit them.	Pre- and post-execution controls are intentionally assigned.	Controls move upstream when evidence shows earlier action improves outcomes.
Exception governance	Missing data is handled case by case.	Thresholds, owners and remediation paths exist.	Exception trends trigger product, counterparty or rail-level decisions.
Regulatory traceability	Requirements are interpreted in disconnected projects.	Applicable obligations map to data and controls.	Changes in expectations trigger governed reassessment and evidence refresh.

Scorecard

DIMENSION	SCORE 1–5	CONFIDENCE H/M/L	EVIDENCE REFERENCE	OWNER
Identity integrity				
Purpose				
Data structure				
Continuity				
Virtual accounts				
Control placement				
Exception governance				
Regulatory traceability				

TOOL 01 • DECISION

From data breaks to accountable action

Prioritize breaks by control consequence, not by implementation convenience.

BREAK / GAP	WHERE INTRODUCED	CONTROL IMPACT	POPULATION / VALUE	CURRENT COMPENSATING CONTROL	EVIDENCE OWNER

Prioritization test

QUESTION	RESPONSE
What risk decision is weakened by this break?	
Can the information be captured or validated earlier?	
Who can change the source, mapping, rail or commercial rule?	
What compensating control exists, and how is its effectiveness proven?	
What threshold requires product restriction, counterparty escalation or risk acceptance?	

Executive decision record

DECISION FIELD	WORKING RECORD
Decision and target state	_____ _____
Residual risk accepted	_____ _____
Accountable executive / control owner	_____ _____
Review date	_____ _____
Trigger for immediate reassessment	_____ _____

TOOL 01 • ACTION

Payment transparency delivery plan

Translate the control decision into a sequenced remediation plan with measurable closure evidence.

Action register

ACTION	OWNER	DUE	SUCCESS MEASURE	REASSESSMENT TRIGGER

Progress review

REVIEW FIELD	WORKING RECORD
Review cadence and forum	
Evidence required for closure	
Dependencies requiring executive intervention	
Decision if delivery misses tolerance	

TOOL 02

AI & Agent Governance

Set authority, evidence and accountability before an AI system can influence a regulated outcome.

USE WHEN	PRIMARY OUTPUT
Approving a copilot, decision-support model or agent that can access data, call tools or affect customers.	An authority classification, control evidence pack, challenge-test record and release decision.

Start with consequence, not sophistication

AUTHORITY	SYSTEM MAY	EXAMPLE	DEFAULT GOVERNANCE
0 • Prohibited	Not operate for the proposed purpose.	Unapproved external action or sensitive-data use.	Block technically; record prohibited use.
1 • Inform	Retrieve, summarize or explain.	Policy assistant or case summary.	Data controls, accuracy testing and user disclosure.
2 • Recommend	Suggest a decision without preparing execution.	Risk prioritization or next-best action.	Outcome testing, explainability and human challenge.
3 • Prepare	Draft the action and assemble evidence.	Prepare an RFI, alert disposition or case note.	Approval workflow, traceability and override monitoring.
4 • Execute with approval	Act only after meaningful human authorization.	Submit a customer restriction after review.	Consequence-based approval, rollback and incident response.
5 • Bounded autonomy	Execute within explicit constraints and limits.	Low-risk routing or standardized remediation.	Independent validation, continuous monitoring, kill switch and board visibility where material.

Use-case profile

FIELD	WORKING DEFINITION
Purpose and intended user	
Affected customers, employees or counterparties	
Highest-consequence available action	
Data accessed, retained or transmitted	
Tools, systems and third parties connected	
Reversibility and maximum time to stop	
Proposed authority level	

EXECUTIVE QUESTION

If the system follows its instructions perfectly and still causes harm, who owns the design failure?

TOOL 02 • CONTROL DESIGN

Lifecycle control and evidence matrix

Approval should rely on an evidence pack that can survive independent challenge and future reconstruction.

LIFECYCLE	CONTROL EXPECTATION	MINIMUM EVIDENCE	OWNER
Purpose	Intended outcome, prohibited uses, affected population and success measure are explicit.	Approved use-case statement; consequence assessment.	
Data	Provenance, permission, quality, retention and sensitive-data handling are governed.	Data inventory; lineage; access record; quality results.	
Model / prompt	Version, configuration, retrieval sources and system instructions are controlled.	Version record; configuration baseline; change history.	
Tools and authority	Available actions are bounded to the approved level and environment.	Tool inventory; permissions; transaction limits; kill switch.	
Testing	Representative, edge, bias and adversarial cases test both output and action.	Test set; acceptance thresholds; failure analysis; independent challenge.	
Human oversight	Review occurs before consequence and gives the reviewer time and evidence to disagree.	Workflow design; reviewer instructions; override and disagreement data.	
Monitoring	Quality, behavior, population, tool calls, overrides and unintended outcomes are visible.	Dashboard; thresholds; trend analysis; escalation record.	
Incident and change	Containment, rollback, notification and reapproval triggers are predefined.	Incident playbook; change taxonomy; rehearsal evidence.	
Third parties	Concentration, model changes, continuity, exit and subcontractor risk are understood.	Contract rights; dependency map; contingency and exit plan.	

Release gates

GATE	PASS CONDITION	RESULT / EVIDENCE
Design	Purpose, authority and affected population approved.	
Control	Permissions, approval points, evidence retention and rollback implemented.	
Challenge	Acceptance and adversarial tests passed or residuals explicitly accepted.	
Operational	Owners, monitoring, incident response and support model are live.	
Change	Events requiring revalidation or reapproval are configured and owned.	

TOOL 02 • CHALLENGE

Adversarial test record and release decision

Test what an intelligent adversary, compromised dependency or rushed operator can make the system do.

SCENARIO	EXPECTED CONTROL	RESULT	SEVERITY	REMEDATION / OWNER
Prompt or instruction injection	System rejects or isolates untrusted instructions.			
Compromised or manipulated retrieval data	Source controls and anomaly detection prevent unsafe reliance.			
Unexpected tool behavior or unavailable dependency	System fails safely and preserves evidence.			
Confidently incorrect output	Acceptance rules or human review prevent consequence.			
Sensitive-data leakage	Data boundaries, redaction and output controls contain exposure.			
Biased or uneven segment outcomes	Segment testing and thresholds trigger remediation.			
Human rubber-stamping	Workflow, sampling and override metrics expose ineffective review.			
Unauthorized authority expansion	Permissions and change controls block new actions.			

Executive decision record

DECISION FIELD	WORKING RECORD
Release decision and approved authority	_____
Conditions before release	_____
Residual risk owner	_____
Monitoring / rollback threshold	_____
Reapproval trigger	_____

Action register

ACTION	OWNER	DUE	SUCCESS MEASURE	REASSESSMENT TRIGGER

TOOL 03

Model Health & Drift

Turn model monitoring into a governed decision about whether to continue, tune, constrain, validate or stop.

USE WHEN		PRIMARY OUTPUT	
Governing transaction monitoring, fraud, screening, customer-risk, prioritization or decision-support models.		A decision-linked dashboard, drift triage record and governed response.	
OPERATING PRINCIPLE			
A metric without a threshold is observation. A threshold without a decision is decoration.			
DRIFT LENS	WHAT CHANGES	PRACTICAL SIGNALS	DECISION IT MAY TRIGGER
Data	Inputs, availability, schema, latency or missingness.	Null rates; field distributions; data freshness; mapping errors.	Constrain population, repair source, reject data or pause.
Population	Customer, product, corridor, geography or channel mix.	Mix shift; new segment share; volume/value concentration.	Segment controls, recalibration or expanded testing.
Concept	Relationship between behavior and the risk outcome.	New typologies; investigation outcomes; external intelligence.	Feature or rule change; scenario redesign; risk appetite review.
Performance	Coverage, stability, precision or outcome quality.	Hit quality; known-event recall; stability; segment performance.	Tune, validate, supplement or replace.
Operational	How people and workflows use the model.	Backlog; aging; overrides; QA findings; workarounds.	Capacity, workflow or threshold change.
Adversarial	Evidence of probing, mimicry or coordinated evasion.	Boundary clustering; repeated near misses; synthetic patterns.	Threat response, control randomization or urgent redesign.

Monitoring design test

FOR EVERY SIGNAL, NAME	WORKING RESPONSE
Population and segment covered	
Data source and calculation owner	
Expected range and threshold	
Decision owner and maximum response time	
Action at amber and red	
Evidence required to close the issue	

TOOL 03 • DASHBOARD

Decision-linked model health dashboard

The executive view should explain what changed, why it matters and what management is doing—not merely show more charts.

SIGNAL	SEGMENT	CURRENT	THRESHOLD	TREND	STATUS	DECISION / ACTION	OWNER

Minimum metric set

DOMAIN	LEADING INDICATORS	OUTCOME / ASSURANCE INDICATORS
Input integrity	Missingness, freshness, schema change, source reconciliation.	Material data incidents; control populations affected.
Population	Mix shifts by product, geography, channel, risk and customer tenure.	Segment-level outcome divergence.
Model behavior	Score distribution, feature availability, stability, boundary clustering.	Known-event coverage; precision proxies; validation findings.
Operations	Alert/case volume, aging, overrides, queue concentration, investigator variance.	QA defects; SLA breaches; material missed or delayed action.
Threat response	New typologies, evasion indicators, intelligence-to-control lead time.	Detection uplift; time from signal to validated change.
EXECUTIVE CHALLENGE		
Which metric would make management stop the model today—and is that threshold actually instrumented?		

TOOL 03 • RESPONSE

Drift triage and governed change

Severity should reflect control consequence, affected population, duration and reversibility.

SEVERITY	CONDITION	INITIAL RESPONSE	DECISION FORUM
S1 • Observe	Within tolerance; no material outcome concern.	Record and continue monitoring.	Model owner.
S2 • Investigate	Threshold breach or unexplained segment change; limited consequence.	Validate data, isolate segment and set dated analysis.	Model owner + compliance operations.
S3 • Constrain	Material degradation, control gap or prolonged uncertainty.	Apply compensating control, restrict population and notify governance.	Model governance / risk committee.
S4 • Stop / incident	Potential regulatory, customer or financial harm; evidence unreliable.	Stop or rollback, preserve evidence and activate incident process.	Accountable executive + incident governance.

Triage record

FIELD	WORKING RECORD
Signal and detection time	
Affected model, version, population and period	
Known / suspected control consequence	
Severity and rationale	
Immediate containment or compensating control	
Evidence required to decide	
Validation / reapproval requirement	
Closure criteria	

Executive decision record

DECISION FIELD	WORKING RECORD
Decision	_____
Decision owner	_____
Dissent / challenge	_____
Effective date	_____
Review date	_____
Reassessment trigger	_____

TOOL 04

Transformation Readiness

Separate technology delivery from a demonstrable change in risk outcomes, customer experience and operating ownership.

USE WHEN		PRIMARY OUTPUT	
Selecting a platform, planning a migration, assessing a troubled program or deciding whether to scale.		A readiness heatmap, stage-gate decision, coexistence plan and benefits record.	
DIMENSION	EXECUTIVE QUESTION	EVIDENCE THAT SHOULD EXIST	COMMON FAILURE
Problem definition	What outcome must change, for whom and by how much?	Baseline, target, scope and explicit non-goals.	Technology becomes the strategy.
Data readiness	Can the required decision be made from available data?	Quality, lineage, ownership, access and representative test data.	Poor data is discovered during migration.
Process redesign	Which legacy steps, handoffs and controls will disappear?	End-to-end target process and exception design.	Old process is recreated in a new interface.
Control / model governance	How will logic, models and changes be independently challenged?	Inventory, validation, testing, change and monitoring plan.	Governance begins after launch.
Adoption	How will behavior change be observed, not merely trained?	Role design, workflow testing, usage, override and quality measures.	Training completion is treated as adoption.
Operating ownership	Who owns outcomes after the project team leaves?	Named service owner, decision rights, capacity and support model.	Permanent ownership is deferred.
Coexistence and cutover	How will old and new evidence reconcile, and how can the firm roll back?	Dual-run, reconciliation, cutover thresholds and rollback plan.	Two systems create two versions of truth.
Benefits and unintended effects	What proves better risk and customer outcomes?	Outcome measures, control coverage, friction and cost baselines.	Delivery milestones substitute for benefits.

Readiness scorecard

DIMENSION	SCORE 1-5	CONFIDENCE	EVIDENCE GAP	DECISION OWNER
Problem definition				
Data readiness				
Process redesign				
Control/model governance				
Adoption				
Operating ownership				
Coexistence/cutover				
Benefits				

TOOL 04 • STAGE GATES

Transformation stage-gate standard

A gate is a decision backed by exit evidence—not a meeting scheduled at the end of a project phase.

GATE	QUESTION	MINIMUM EXIT EVIDENCE	DECISION
0 • Frame	Is the problem worth solving and defined in outcome terms?	Baseline; affected population; target; sponsor; risk of inaction.	Fund discovery / stop.
1 • Design	Will the target process and control model solve the problem?	Process, data, control, operating and architecture designs; key risks.	Approve build / redesign.
2 • Build	Is the capability complete enough for representative testing?	Configured solution; lineage; controls; test environment; ownership.	Enter proving / remediate.
3 • Prove	Does it work for risk, operations and customers under realistic conditions?	Acceptance, control, adversarial, volume, segment and user evidence.	Approve limited release / fail.
4 • Cut over	Can the organization move safely and retain evidence?	Reconciliation; coexistence; rollback; support; incident readiness.	Cut over / extend dual run.
5 • Scale	Are outcomes sustained and unintended effects controlled?	Outcome trend; defects; adoption; capacity; validation; residual risk.	Scale / constrain / stop.

Gate decision record

FIELD	WORKING RECORD
Gate and date	
Evidence reviewed	
Acceptance criteria met / missed	
Material dissent	
Decision: proceed / conditional / hold / stop	
Conditions and accountable owners	
Next gate and reassessment trigger	
HARD TRUTH A project can be green while the transformation is red. Delivery health and outcome readiness must be reported separately.	

TOOL 04 • CUTOVER

Coexistence, cutover and benefits

The uncomfortable period when old and new systems coexist is a control state in its own right.

CONTROL AREA	QUESTION	PASS CRITERION / EVIDENCE	OWNER
Population	Do both systems process the same in-scope population?		
Decision	How are different outcomes compared and resolved?		
Evidence	Can historical and new decisions be reproduced?		
Data	Are transformations, timing and missingness reconciled?		
Operations	Are dual queues, backlogs and handoffs controlled?		
Customer	Are duplicate requests, restrictions or inconsistent messages prevented?		
Rollback	What can be reversed, how quickly and with what data?		
Retirement	What evidence permits the legacy control to be decommissioned?		

Benefits realization

OUTCOME	BASELINE	TARGET	CURRENT	EVIDENCE	OWNER
Risk coverage					
Decision quality					
Customer friction					
Time to adapt					
Operational capacity					
Control cost					

Executive decision record

DECISION FIELD	WORKING RECORD
Cutover decision	_____
Residual risk and accountable executive	_____
Legacy retirement / benefits review date	_____
Stop / rollback trigger	_____

TOOL 05

Global Compliance Operating Model

Place standards, capabilities and judgment where they produce consistency without creating a global queue.

USE WHEN	PRIMARY OUTPUT
Designing global hubs, follow-the-sun operations, regional growth or correcting excessive centralization.	A capability placement map, decision-right matrix, handoff standard and concentration response.
DESIGN PRINCIPLE Centralize the standard. Distribute informed judgment. Connect the system through evidence.	

Capability placement test

CAPABILITY	GLOBAL	REGIONAL	LOCAL	HYBRID	RATIONALE / EVIDENCE
Policy and minimum standards					
Regulatory interpretation					
Customer / product risk decisions					
Investigations and intelligence					
Screening / monitoring operations					
Quality assurance and calibration					
Data, models and control technology					
Regulatory engagement and reporting					

Placement criteria

CENTRALIZE WHEN	DISTRIBUTE WHEN
Consistency, scarce expertise, control integrity or scale materially improve.	Language, market context, regulatory proximity or response speed materially improve.
Fragmentation would create incompatible data, models or evidence.	Local judgment can operate within a clear global standard and escalation rule.
Independent challenge or enterprise visibility requires separation.	Customer or regulator outcomes suffer when decisions wait for a remote queue.

TOOL 05 • DECISION RIGHTS

Decision rights and follow-the-sun handoffs

A distributed model works only when authority and evidence travel together.

DECISION	GLOBAL OWNER	REGIONAL AUTHORITY	LOCAL EVIDENCE	MUST ESCALATE WHEN
Policy interpretation				
Customer onboarding / restriction				
Suspicious activity / investigation				
Sanctions or high-risk nexus				
Model / threshold change				
Regulatory communication				
Incident or material control failure				

Minimum handoff packet

HANDOFF ELEMENT	STANDARD	OWNER / SYSTEM OF RECORD
Decision state	What has been decided, what remains open and the deadline.	
Evidence	Relevant customer, transaction, intelligence and prior-decision sources.	
Risk hypothesis	What concern is being tested and what would disprove it.	
Authority	What the receiving team may decide and what must escalate.	
Priority	Consequence and time sensitivity—not merely queue age.	
Closure	Required rationale, evidence retention and feedback to upstream teams.	

FAILURE SIGNAL

If the receiving team must reconstruct the case, the organization has not transferred work—it has transferred confusion.

TOOL 05 • RESILIENCE

Concentration and operating resilience stress test

Test the model against the loss of a location, leader, vendor, dataset or regulatory assumption.

SCENARIO	CURRENT EXPOSURE	TOLERANCE	IMMEDIATE RESPONSE	RECOVERY EVIDENCE	OWNER
Primary hub unavailable					
Key leader / specialist unavailable					
Critical vendor or model unavailable					
Material data feed degraded					
Regulatory interpretation conflicts across markets					
Volume surge exceeds regional capacity					
Cyber or geopolitical event isolates a location					

Leadership-depth test

QUESTION	EVIDENCE / RESPONSE
Can each hub make and defend decisions, or does it only execute?	
Which material decisions still depend on one person, time zone or language?	
Are performance differences visible and converted into shared learning?	
Can regions challenge the global standard without creating local exceptions by default?	
What work could move within 24 hours without losing control evidence?	

Executive decision record

DECISION FIELD	WORKING RECORD
Operating-model decision	_____ _____
Risk accepted / accountable executive	_____ _____
Capability to relocate or duplicate	_____ _____
Target / stress-test date	_____ _____

TOOL 05 • ACTION

Operating-model implementation plan

Turn the placement and resilience decisions into specific authority, capability and evidence changes.

Action register

ACTION	OWNER	DUE	SUCCESS MEASURE	REASSESSMENT TRIGGER

Progress review

REVIEW FIELD	WORKING RECORD
Review cadence and forum	
Calibration / consistency evidence	
Regional or local feedback requiring a standard change	
Decision if concentration remains outside tolerance	

TOOL 06

Board Oversight of AI Agents

Help directors govern consequence, authority and accountability without turning the board into a technical design committee.

USE WHEN	PRIMARY OUTPUT
Board or risk-committee approval, oversight of a material AI use case or expansion of agent authority.	A board challenge record, concise dashboard and explicit approval conditions.

Questions the board should ask

DOMAIN	BOARD QUESTION	EVIDENCE MANAGEMENT SHOULD PROVIDE
Purpose	What outcome is the system designed to improve, and for whom?	Approved purpose, affected population, baseline and success measure.
Authority	What can it do—not merely recommend—and what is the highest-consequence action?	Authority level, permissions, limits and prohibited actions.
Human oversight	Where can a person meaningfully disagree before consequence?	Workflow, reviewer evidence, override and disagreement data.
Evidence	Can an independent reviewer reconstruct the system's reasoning and actions?	Version, inputs, outputs, tool calls, approvals and retained rationale.
Testing	How was the system tested against realistic failure and adversarial behavior?	Acceptance, segment, bias, security and adversarial test results.
Resilience	How quickly can it be stopped, rolled back or isolated?	Kill switch, rollback time, incident rehearsal and contingency.
Change	Which changes require revalidation or reapproval?	Change taxonomy covering model, data, tool, purpose, authority and market.
Third parties	Where are concentration, continuity and exit risks?	Dependency map, contract rights, alternative service and exit plan.
Outcomes	How will management distinguish productivity from risk moved elsewhere?	Risk, customer, control, workforce and quality measures.
Accountability	Who owns harm when the system follows its instructions?	Named accountable executive, control owners and incident governance.

BOARD BOUNDARY

The board does not need to approve prompts. It should approve the consequence envelope, evidence standard, accountability and conditions for management to expand authority.

TOOL 06 • OVERSIGHT

Board dashboard and decision record

Keep the board view concise enough to govern, but specific enough to expose false confidence.

DOMAIN	STATUS	KEY EVIDENCE	CHANGE SINCE LAST REVIEW	MANAGEMENT ACTION	BOARD CHALLENGE
Purpose / population					
Authority / permissions					
Performance / outcomes					
Human oversight					
Incidents / near misses					
Drift / material change					
Third-party / resilience					
Residual risk					

Board decision

FIELD	BOARD RECORD
Decision: approve / conditional / decline / require redesign	
Approved purpose, population and authority ceiling	
Conditions management must satisfy	
Risk accepted and accountable executive	
Metrics / incidents requiring notification	
Changes requiring return to the board	
Next review date	

THE ONE QUESTION

What would have to be true for management to recommend stopping this system—and would the board hear about it in time?

TOOL 07

30/60/90-Day Transformation Plan

Create visible progress in one quarter without confusing urgency with ungoverned activity.

USE WHEN	PRIMARY OUTPUT
Starting, resetting or rescuing a compliance transformation.	A one-quarter charter, sequenced evidence plan, ownership model and scale / stop decision.

Define the 90-day outcome

CHARTER FIELD	WORKING DEFINITION
Outcome to improve	
Affected risk, customer and operating population	
Baseline and evidence date	
90-day target and acceptable tolerance	
Accountable executive	
Permanent operating owner	
Decision forum and cadence	
What is explicitly out of scope	
Stop condition	

Workstream architecture

WORKSTREAM	90-DAY QUESTION	LEAD
Risk and control	What control outcome changes, and how will coverage be proven?	
Data and technology	What data, model, platform or integration must become reliable?	
Process and customer	What friction, handoff, exception or delay will be redesigned?	
People and ownership	Who will operate, challenge and improve the capability?	
Governance and evidence	What decisions, thresholds and records make change accountable?	

TOOL 07 • DAYS 1–30

Establish the truth

The first month should reduce ambiguity: one outcome, one baseline, named ownership and the real constraints.

DELIVERABLE	EXECUTIVE STANDARD	OWNER	DUE	EVIDENCE / DECISION
Outcome charter	Problem, affected population, baseline, target and non-goals approved.			
Current-state control map	Material decisions, controls, handoffs, exceptions and workarounds visible.			
Data reality	Quality, lineage, access, ownership and representative-data gaps documented.			
Risk and dependency map	People, vendors, models, systems and regulatory dependencies named.			
Operating baseline	Coverage, quality, aging, customer friction, capacity and cost measured.			
Governance	Sponsor, permanent owner, decision forum, cadence and escalation rule active.			
90-day proof point	One narrow outcome can be changed and evidenced within the quarter.			

Day-30 decision

QUESTION	WORKING RESPONSE
Is the original problem statement still valid?	
What assumption failed first?	
Which dependency or evidence gap threatens the 90-day outcome?	
What will be stopped, narrowed or deferred?	
Decision: proceed / reframe / stop	

Action register

ACTION	OWNER	DUE	SUCCESS MEASURE	REASSESSMENT TRIGGER

TOOL 07 • DAYS 31–60

Prove the change

The second month should test the target process and control with representative users, data and failure conditions.

DELIVERABLE	EXECUTIVE STANDARD	OWNER	DUE	EVIDENCE / DECISION
Target process	Legacy steps removed; decisions, handoffs and exceptions designed end to end.			
Control design	Control purpose, owner, evidence, threshold and escalation are explicit.			
Representative test	Realistic populations, edge cases and material segments are included.			
Failure / adversarial test	The program tests how data, models, users and dependencies fail.			
Coexistence and rollback	Old/new reconciliation, cutover criteria and recovery are rehearsed.			
Operating ownership	Permanent team can operate, challenge and improve the capability.			
Outcome evidence	Early results compare with baseline and expose unintended effects.			

Day-60 decision

QUESTION	WORKING RESPONSE
What has been proven with representative evidence?	
What remains assertion or demonstration?	
What control, customer or operational effect was unintended?	
What must be true before limited release or cutover?	
Decision: release narrowly / continue proving / redesign / stop	

Action register

ACTION	OWNER	DUE	SUCCESS MEASURE	REASSESSMENT TRIGGER

TOOL 07 • DAYS 61–90

Govern the scale

The final month should transfer ownership, prove sustained outcomes and make the next scale decision explicit.

DELIVERABLE	EXECUTIVE STANDARD	OWNER	DUE	EVIDENCE / DECISION
Outcome comparison	Current results compared with baseline, target and segment tolerances.			
Control assurance	Quality, validation and independent challenge support continued use.			
Permanent ownership	Service, model, process and policy owners accept accountability.			
Monitoring and triggers	Dashboard, thresholds, escalation and reassessment events are live.			
Residual risk	Known gaps, compensating controls, acceptance and expiry dates recorded.			
Scale economics	Capacity, cost, customer and risk impacts support the next investment.			
Learning record	What changed, what failed and what should not be repeated are published.			

Executive decision record

DECISION FIELD	WORKING RECORD
90-day outcome achieved / missed	_____
Scale decision	_____
Evidence supporting the decision	_____
Residual risk	_____
Permanent accountable owner	_____
Next review date	_____
Stop / reassessment trigger	_____

CLOSE THE QUARTER

Publish the learning—not only the success. An adaptive organization becomes faster because it retains evidence from what did not work.

CONSOLIDATED OUTPUTS

Executive action and evidence register

Use this page to bring decisions from multiple tools into one accountable view.

TOOL / DECISION	ACTION	OWNER	DUE	SUCCESS MEASURE	STATUS	TRIGGER

Evidence inventory

EVIDENCE ITEM	SOURCE / SYSTEM	OWNER	AS-OF DATE	CONF.	GAP / ACTION

CLOSURE STANDARD

An action is not closed because work was performed. It is closed when the agreed evidence demonstrates the intended outcome and the residual risk is understood.

FACILITATOR CLOSE

The tool is the conversation it makes possible

Adaptive compliance is the organizational capability to see change, interpret evidence, decide accountably and improve while risk is still moving.

BEFORE THE SESSION	IN THE ROOM	AFTER THE DECISION
Define scope and decision. Select participants who own evidence and consequence. Circulate baseline material. Collect independent scores.	Separate maturity from confidence. Ask what evidence would change the answer. Record dissent and uncertainty. Name the decision—not merely the discussion.	Assign owner and due date. Retain the evidence reviewed. Set success measure and trigger. Return when the trigger occurs, not only on the calendar.
FINAL PRINCIPLE		
Better compliance begins when the organization can change its mind for the right reason—and show its work.		

About the author

Micheal Sheehy is a global payments and compliance executive and the author of the eight-volume Adaptive Compliance series. His work focuses on financial crime, payment transparency, artificial intelligence, model governance, global operating models and the leadership systems required to scale safely.

READ	CONTACT
michealsheehy.com/adaptive-compliance.html	micheal@michealsheehy.com • +1 (818) 397-8890
michealsheehy.com/tools.html	linkedin.com/in/micheal-s-88479045

Vendor-neutral working material • Not legal advice • Confirm applicable regulatory requirements