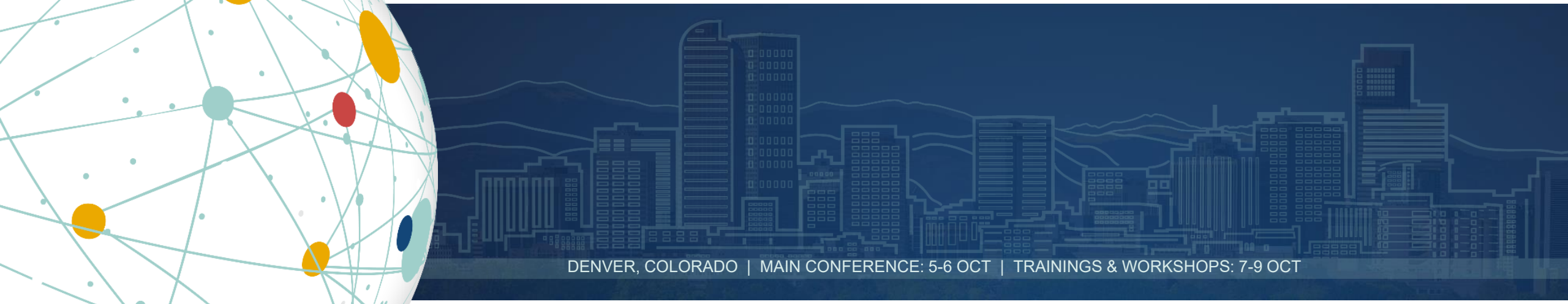


2026 US Interchange

THE FUTURE IS CONNECTED: STANDARDS AND AI POWERING DIGITAL TRANSFORMATION



Your Clinical Systems Are Connected – Your TMF Governance Isn't

Olga Radyushkina, Epista | Tiffani Nelson, Gilead

Speakers



Olga Radyushkina

Manager, TMF

Epista Life Science

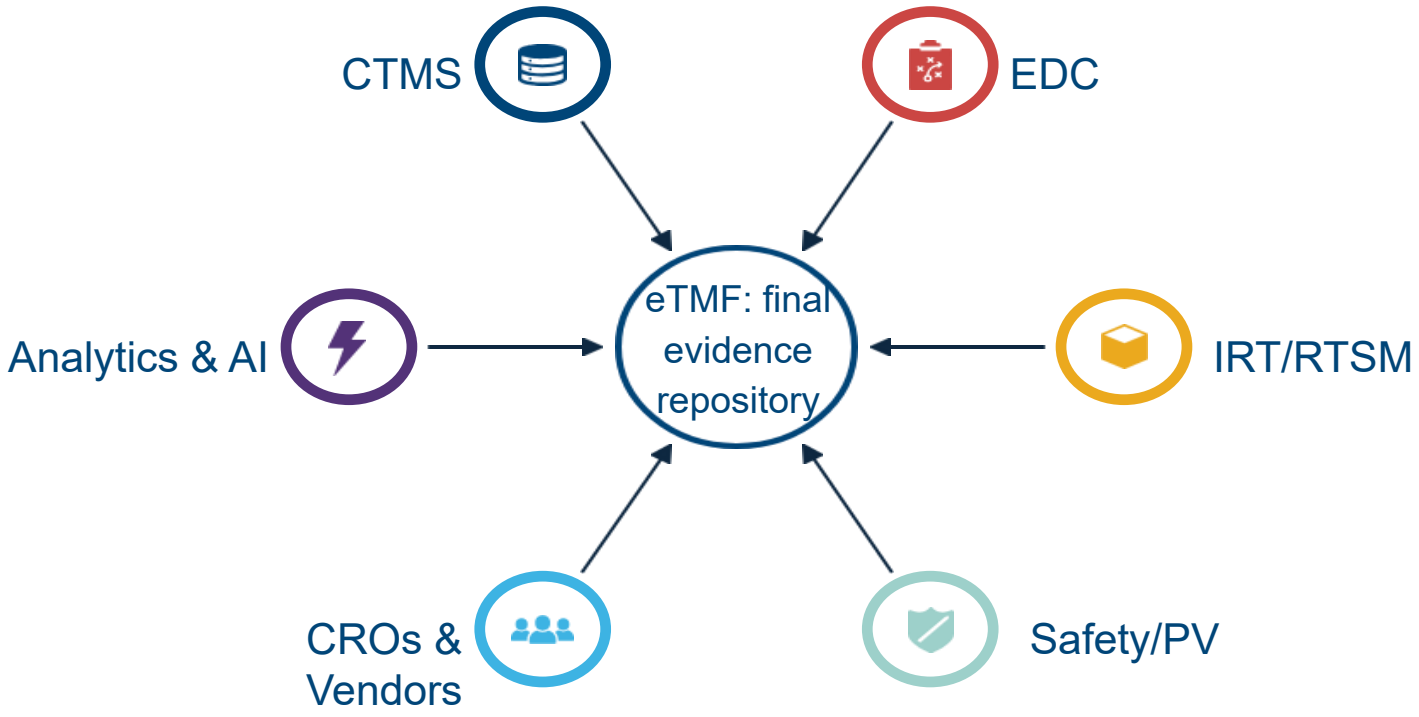


Tiffani Nelson

Sr. Manager, Clinical Records and Information Management

Gilead

The Clinical Evidence Ecosystem

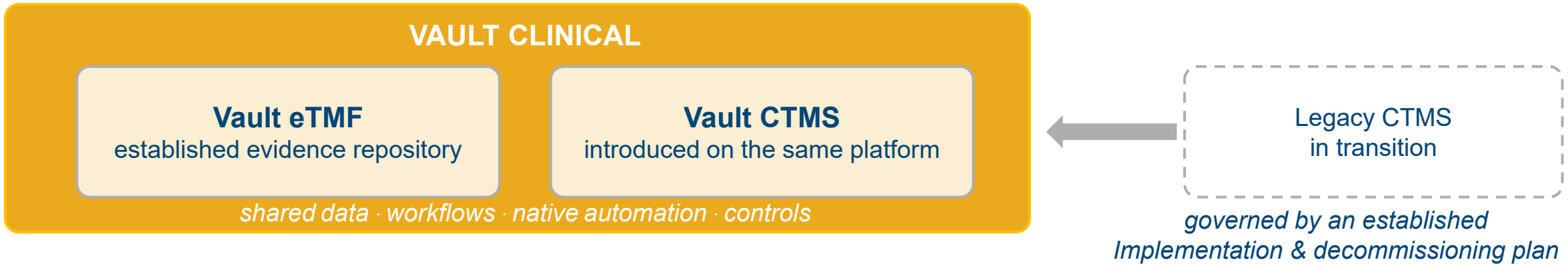


TMF evidence is shaped by data, events, and decisions across clinical operations – not only by documents filed in the eTMF.

The systems share data and consequences. Governance must align across the systems and processes that create, change, and explain the evidence.

Gilead Use Case: Vault Clinical

Introducing Vault CTMS alongside an established Vault eTMF



ESTABLISHED

Vault eTMF and the cross-functional TMF governance foundation.

FUTURE STATE

Vault Clinical – Vault CTMS and Vault eTMF – support clinical and TMF processes on one shared platform.

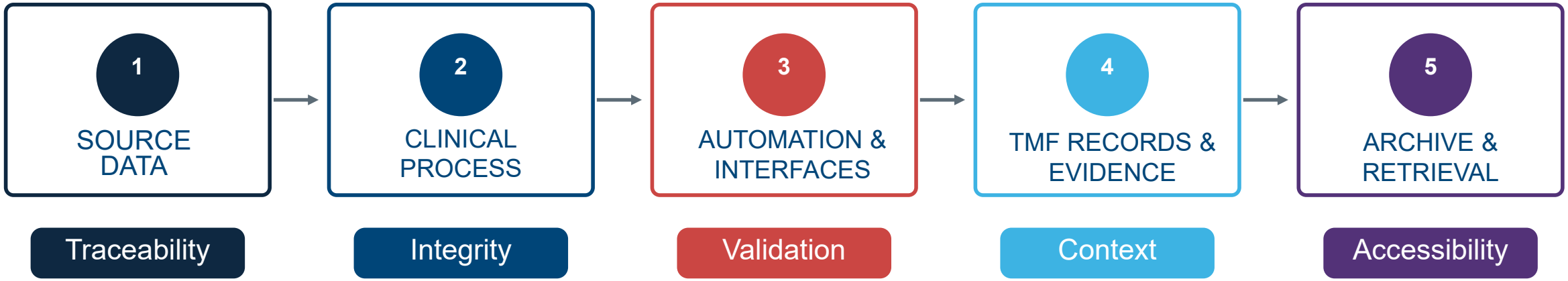
GOVERNED TRANSITION

Transition, cutover, retention, and decommissioning controls addressed in the established plan.

The immediate governance point: shared study, site, person, milestone & workflow data influence both operations and TMF evidence; ownership and impact assessment must be explicit from the start.

Regulatory Expectations Follow the Evidence Chain

The requirement follows the evidence, not the application boundary



RECONSTRUCT
Can trial conduct be reconstructed?

TRUST
Are records complete, accurate, and attributable?

PRESERVE
Are data, metadata, relationships, and audit trails preserved in context?

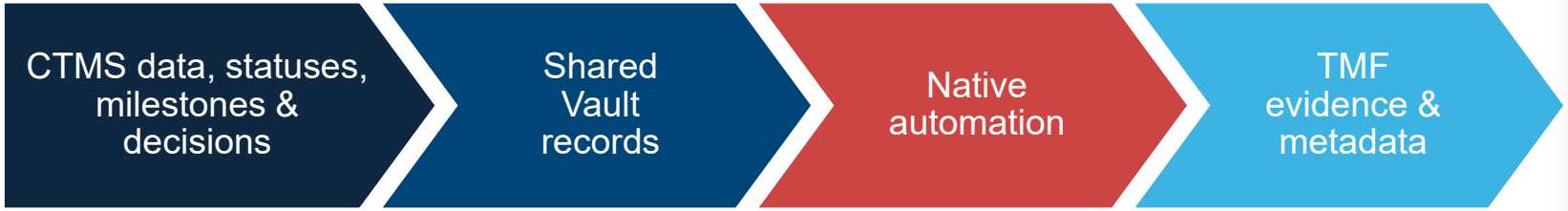
RETRIEVE
Is evidence accessible throughout retention?

The regulations do not prescribe a governance committee.
They require the organization to control and explain the complete evidence lifecycle.

- Primary sources: ICH E6(R3), Annex 1 §4.3.4(e); EMA TMF Guideline §§2, 3.4; EMA Computerised Systems Guideline §§6.10–6.12
- Supporting sources: EU CTR Articles 57–58; FDA Electronic Systems Q&A

TMF Quality Starts Upstream

- Shared records affect both operational workflows and TMF metadata – automation can create, classify, link, or update evidence.



- Consequence: data or configuration errors can become TMF quality issues before a document ever reaches the eTMF

TMF governance defines the evidence requirements;
operational data and events determine when and where those requirements apply.

Vault eTMF remains the primary repository for controlled TMF documents and records; CTMS data and workflows provide context and determine when requirements apply.

The Governance Layers

SYSTEM GOVERNANCE

Governs controlled operation of the shared Vault platform

- Architecture, configuration & access
- Validation & releases
- Native automation & incidents
- Vendors & external integrations

DATA GOVERNANCE

Governs shared data meaning, consistency, and fitness

- Authoritative values & definitions
- Identifiers & controlled terminology
- Lineage & data quality
- Correction authority

TMF GOVERNANCE

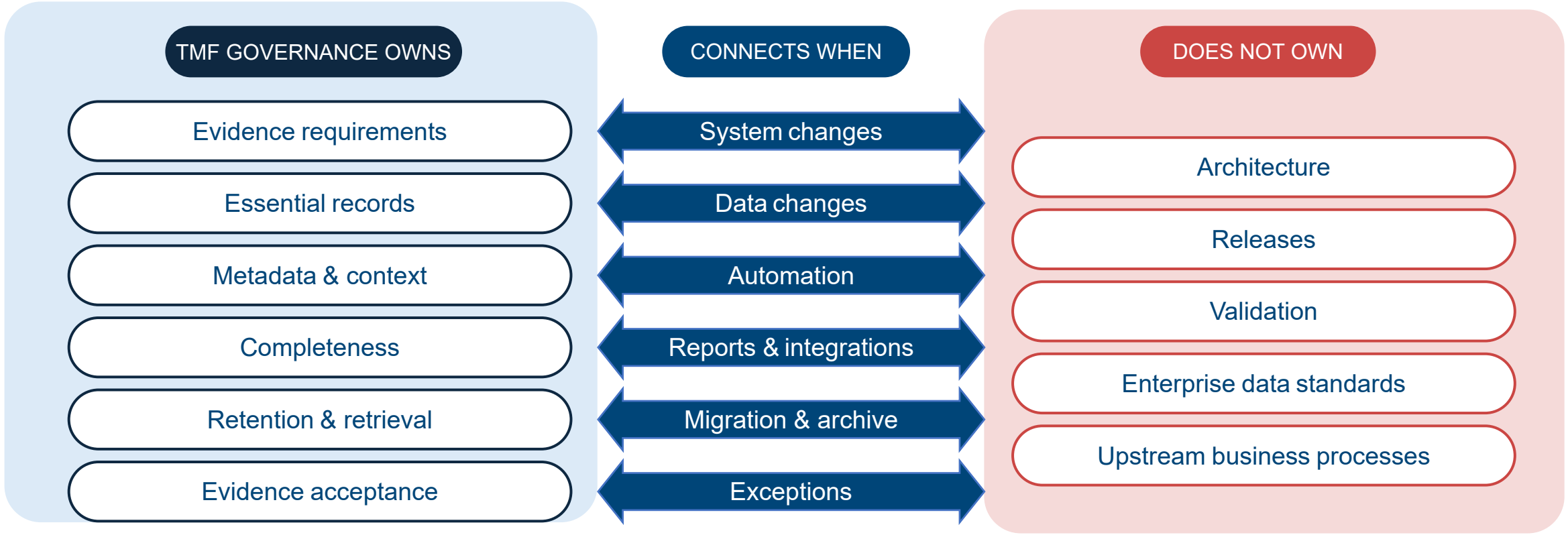
Governs TMF requirements and evidence integrity

- Essential records & expectedness
- Metadata relationships
- Completeness & inspection reconstruction
- Retention & retrieval

Each layer maintains distinct responsibilities while aligning wherever shared data, workflows, automation, or platform changes affect TMF evidence.

cdisc®

Where TMF Governance Fits



Own the TMF evidence requirements:
engage on any change that can affect the evidence outcome.

WHO OWNS THE OUTCOME?

Raise your hand for ONE answer.

Scenario: a monitoring report is approved through the Vault CTMS workflow.
Native automation files it in Vault eTMF but the report is linked to the wrong site.

1. Who is most likely to detect the issue?
2. Who determines whether the source site relationship is correct?
3. Who owns the system configuration or automation correction?
4. Who confirms the TMF evidence outcome is restored?

A Clinical Operations

B TMF / Records Management

C Clinical Systems / IT

D Quality

E Vendor

F Business Process Owner

G All of the above

Where Governance Must Connect

1 Shared data or definitions change

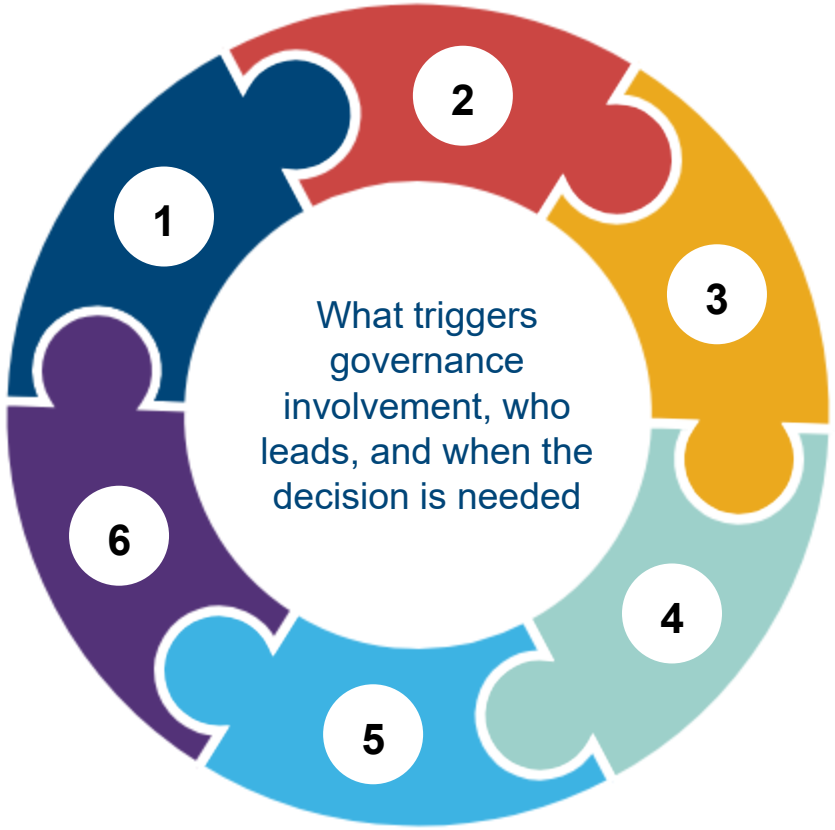
- Led by Process owner + Data owner. Engagement required before design / configuration approval.

2 Workflow or native automation updates TMF

- Led by Process owner + System owner. Engagement required before release.

3 New reports, metrics, or logic introduced

- Led by System owner + Data owner. Engagement required before governance / inspection use.



4 External integrations or vendor services

- Led by System owner. Engagement required for implementation, release & oversight.

5 Migration, cutover, archive, or decommissioning

- Led by System owner. Engagement required at defined decision & acceptance points.

6 Reconciliation identifies an exception

- Led by Process owner. Engagement required from assignment through outcome restoration.

The goal is not another committee:
it is clear triggers, leads, and decision points with evidence-impact acceptance.

cdisc®

Change Control Across the Evidence Chain

- Formal change and release control is administered through Vault platform governance — material changes require three impact lenses.

PLATFORM IMPACT

- Validated state & configuration
- Access & automation
- External interfaces, release & rollback

DATA IMPACT

- Authoritative source & definitions
- Controlled terms, identifiers & mappings
- Lineage & data quality

TMF EVIDENCE IMPACT

- Essential records & expectedness
- Classification & relationships
- Completeness, inspection use & retention

- The accountable business process owner assesses operational-process impact (i.e. roles, workflows, procedures, training) of a change across all three lenses before release.

Deployment is not closure.
Material changes close only after post-release confirmation of the data and evidence outcome.

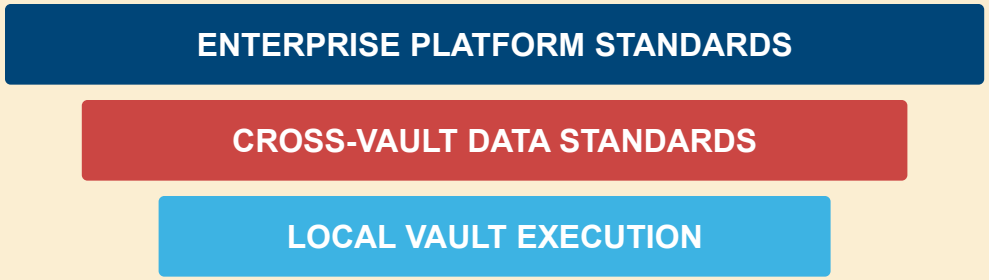
How the Operating Model Works

DISTRIBUTED CONTROL OWNERS

- Clinical Operations
- IT / Clinical Systems / QA
- Data Governance
- TMF Governance
- Records Management
- Vendors / CROs

Explicit escalation & acceptance when platform, data, and TMF requirements conflict.

MULTI-VAULT ALIGNMENT



TMF governance is the evidence partner, not the owner of every upstream system or process control.

One accountable owner is assigned to the defined end-to-end business process; control responsibilities remain distributed.

What Changes in Practice

Connected governance changes how issues, changes, and outcomes are assessed, not simply which committee discusses them.

APPLICATION-FOCUSED GOVERNANCE	CONNECTED GOVERNANCE
Clinical system changes are reviewed mainly for technical impact	**Technical, data, process, and TMF evidence impacts are assessed together**
TMF impact is identified only after release	**TMF requirements and acceptance criteria are defined before release**
Automation success = the workflow or job completed	**Automation is successful only when the intended data, process, and TMF evidence outcomes are confirmed**
Data conflicts are corrected where they appear	**Data are corrected at the authoritative source, and downstream impacts are assessed**
Each team resolves its assigned issue, but no one verifies the complete outcome	**Named owners resolve each issue, and one accountable business process owner confirms that the end-to-end evidence outcome is correct**

Confirm the Evidence Outcome



Did it execute correctly?

Are identities, values, definitions, relationships, and lineage correct and traceable?

Did the correct TMF record, metadata, relationship, and expectedness result; and is the evidence inspection-ready?

PREVENTIVE

- Ownership & common definitions
- Mapping rules & automation design
- Impact assessment and validation

DETECTIVE

- Technical / data / evidence reconciliation
- Metadata and relationship checks
- Exception aging & trend monitoring

CORRECTIVE

- Source correction & controlled reprocessing
- downstream Impact assessment & escalation
- Deviation / CAPA where needed

A technical success is not an evidence success
until the correct record, relationship, metadata, lineage, traceability, and retrieval are confirmed..

cdisc®

Building AI Readiness

1

Governance Foundation

Trusted authoritative data, common definitions, clear decision rights, and reconciliation controls.

2

What It Enables

Cross-system anomaly detection, duplicate analysis, quality monitoring, and risk prioritization.

3

What AI Governance Adds

Approved context of use, fit-for-purpose data, human accountability, and lifecycle control.

AI readiness is a consequence of governance readiness — not a separate workstream.

cdisc®

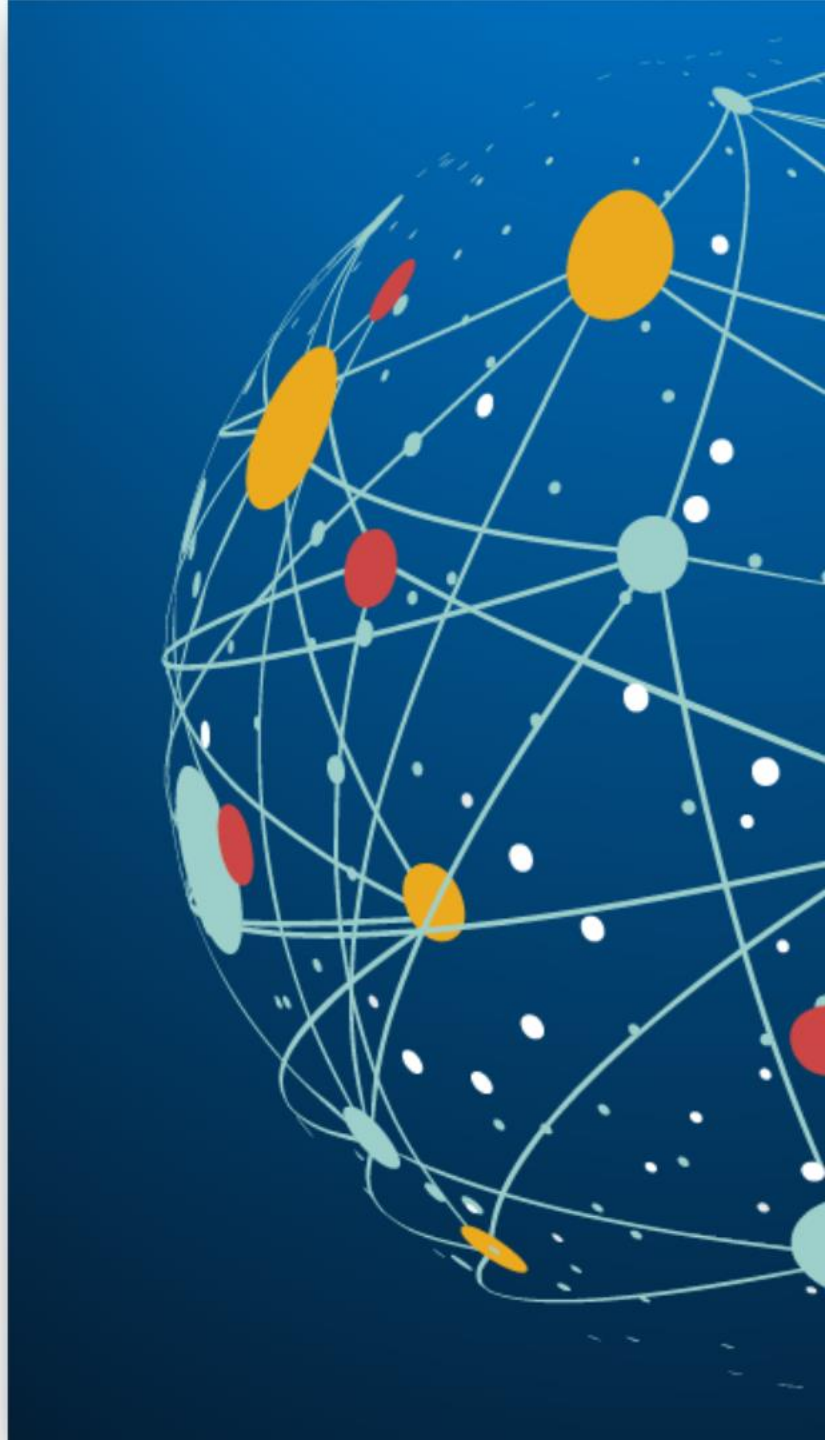
Key Takeaways

1. **One platform does not eliminate**
   distinct platform, data, process, and TMF evidence responsibilities

2. **TMF governance must engage**
   but does not need to own – when upstream changes can affect the TMF evidence outcome

3. **Material changes and exceptions**
   close only after technical, data, and evidence outcomes are confirmed

4. **Use the same foundation**
   for multi-Vault consistency and responsible AI



Thank You!

