Deloitte.

Together makes progress

From Fragmented Controls to Connected Risk – How Knowledge Graphs Modernise Risk Management

To build a future-proof risk control framework, banks need to move beyond fragmented controls and create stronger connections between risks, regulations, processes and accountability. This article outlines how Deloitte's Risk Control Framework, supported by knowledge graphs and AI, can help banks develop a more integrated, transparent and scalable approach to risk and control management.

The management of non-financial risk has become a strategic priority for banks, driven by past losses, operational incidents, and growing expectations from regulators, customers and other stakeholders. While non-financial risks do not typically generate direct financial upside, they cannot be assessed in isolation from the bank's strategy.

A sound understanding of non-financial risks is essential to evaluating whether strategic objectives can be achieved in a controlled, resilient and sustainable way. This requires banks to consider both risks and rewards when making strategic decisions, ensuring that growth, innovations, and transformation are supported by effective prevention, control, and governance. Regulators are also placing greater emphasis on this connection, expecting banks to embed non-financial risk consideration into strategic decision-making, risk appetite and overall business resilience.

Current State: why non-financial risk controls matter now

Non-financial risks are becoming more complex, visible and consequential. Regulatory expectations continue to increase, particularly in areas of operational resilience, digital risk, outsourcing, data quality, financial crime, ESG and customer protection. Simultaneously, banks are under pressure to demonstrate that they are able to identify, control and evidence these risks in an automated and consistent manner across the organisation.

Most banks have already built strong foundations to manage these risks. Control libraries, risk assessments, testing procedures, governance processes and reporting structures are often in place. However, these foundations have frequently expanded over time in response to regulatory change and evolving supervisory expectations, resulting in an increasingly large and complex set of controls. As a result, the control environment can become overloaded, with too many controls creating fragmentation, duplication and overlap. This can limit oversight, obscure interdependence, increase the burden of testing and reporting, and make it more difficult to demonstrate that the organisation is effectively in control.

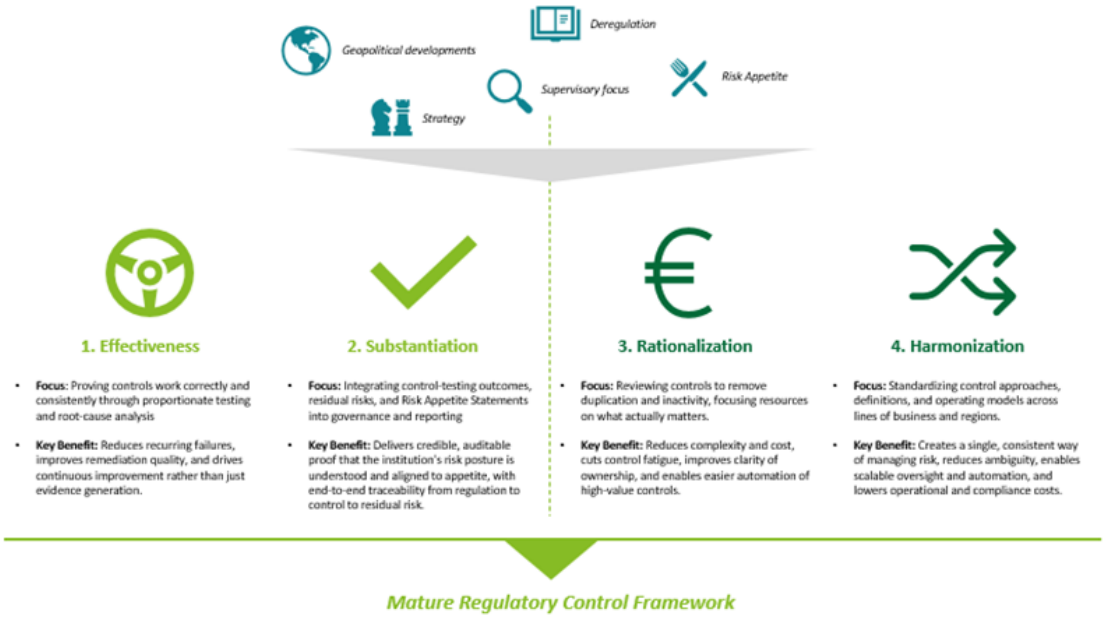
This fragmentation is significant because the impact of risk events is rarely limited to a single control area, risk type, or initial event. Cyber incidents, for example, can affect operational continuity, customer trust, increased regulatory attention and third-party dependencies, but may also create financial risk implications, such as increased credit risk if affected customers or counterparties are unable to meet their obligations. Likewise, data quality issues can affect risk models, disclosures, regulatory submissions, and downstream decision-making across both financial and non-financial risk domains. In an interdependent banking environment, a weakness in one control area can quickly cascade across the organisation, creating consequences far beyond the original risk event.

Yet many banks still manage related risks through different methodologies, taxonomies, templates, and systems. Related risks may be assessed repeatedly; the same business lines may be asked for overlapping evidence, and comparable controls may exist in different parts of the organisation without being clearly connected.

Simply adding more people, more assessments or more reporting does not solve this issue. In some cases, it adds bureaucracy, slows down the business, and still leaves important gaps in oversight, accountability, and evidence. The opportunity is therefore to build on what already exists, while creating a more coherent and future-proof Risk Control Framework.

Deloitte's Risk Control Framework

Deloitte's Risk Control Framework provides a practical structure for moving from fragmented control activity to integrated and automated control governance. It is built around four mutually reinforcing pillars: effectiveness, substantiation, rationalisation, and harmonisation. Where many approaches focus on strengthening individual controls, Deloitte's framework treats risk and control as an interconnected system, explicitly linking controls to regulations, processes, ownership and risk. This connected view is what makes the framework relevant now, as growing regulatory expectations



and increasingly interdependent risks make it harder to demonstrate genuine control through isolated activity. This helps organisations shift from a compliance-driven approach to a more value-adding control environment that supports resilience, transparency, and better decision-making.

1. **Effectiveness:** controls are proven to work consistently in practice through proportionate testing and root-cause analysis. This pillar moves control testing away from a routine pass-or-fail exercise and towards a risk-based, insight-driven approach.

2. **Substantiation:** the framework is integrating control-testing outcomes, residual risks, and Risk Appetite Statements into governance and reporting. This pillar delivers credible, data-driven proof that an organisation's risk posture is understood and aligned to appetite, with end-to-end traceability from regulation to control to residual risk.

3. **Rationalisation:** controls are reviewed to remove duplication and inactivity, focusing resources on what matters. This pillar reduces complexity and costs, cuts control fatigue, improves clarity of ownership, and enables easier automation of high-value controls.

4. **Harmonisation:** controls are standardised in their approach, definition and operating models across lines of business and regions. This pillar creates a single, consistent way of managing risks, reducing ambiguity, enabling scalable oversight and automation, and lowering operational and compliance costs.

Each pillar supports the others. Implementation of controls without effectiveness testing creates uncertainty. Testing without substantiation creates weak evidence and does not build trust. Rationalisation without harmonisation may reduce consistency. Harmonisation without clear accountability results in a framework becoming a paper tiger.

Knowledge graphs as an enabler

The four pillars define what a future-proof Risk Control Framework should achieve. The connected view they depend on, however, is difficult to sustain manually across thousands of controls, regulations and processes. This is where technology becomes essential. Knowledge graphs are a natural enabler of this connected view. They semantically link fragmented risk and control information, turning the framework's principle of connection into a working model of the non-financial risk environment.

This is especially relevant for non-financial risks given its interconnected nature. A knowledge graph connects the core elements of the non-financial risk control environment, linking risks and controls to regulatory obligations, business processes, ownership, evidence and outcomes. Instead of treating these elements as separate records across separate systems, the knowledge graph shows how they relate to one another and adds a semantic layer transforming data into knowledge. For knowledge graphs to be truly useful, we must ensure that the connections we map are not just structurally sound, but also semantically validated against the established business rules of the specific risk domain.

This transforms non-financial risk management from a static inventory exercise into a connected risk model. It allows banks to see which controls support multiple non-financial risks, which processes are most exposed, where control gaps exist, and how failure in one area could affect other parts of the organisation.

Take the cyber incident described earlier. In a knowledge graph, the compromised system is linked in advance to the processes it supports, the controls meant to mitigate the risk, and the counterparties that depend on it – including their credit exposures. When the incident occurs, the chain becomes visible immediately. A control weakness in one domain can be traced through to a potential increase in credit risk in another. Control gaps surface the same way: a critical process with no effective control appears as a missing connection, rather than staying hidden until a manual audit or incident exposes it.

Having seen how this works for a single incident, it provides the platform to look at the bigger picture: how the same connective capability supports each of the four pillars. Rather than visiting each pillar in turn, Table 1 links every pillar to knowledge graph capability that enables it and the outcome it produces.

Table 1: ***How knowledge graphs bring each pillar to life***

Pillar	How the knowledge graph enables it	Outcome
Effectiveness	Links testing outcomes to the wider non-financial risk landscape	Critical controls, recurring failures, and root causes are easier to identify
Substantiation	Creates traceability from regulation to risk category, control, evidence, and residual risk	Credible, end-to-end proof that risk posture is understood and within appetite
Rationalisation	Makes duplicate and overlapping controls visible across risk domains and business lines	Reduced complexity, lower cost, and clearer focus on high-value controls
Harmonisation	Provides a single, consistent source of control definitions across the organisation	One shared way of managing risk, enabling scalable oversight and automation

Read together, these rows show that the value of a knowledge graph is not any single capability, but the way it reinforces all four pillars at once, the same connection that traces one incident across domains also underpins effectiveness, substantiation, rationalisation and harmonisation across the organisation. This is what turns a set of principles into a working, scalable framework.

These graphs provide the necessary modernisation layer, acting as the definitive map for AI to connect fragmented risk foundations. This integration turns disparate data into an integrated, auditable, and future-proof control ecosystem, unlocking advanced use cases like regulatory impact assessment, automated gap identification, and real-time risk management reporting.

Final thoughts

The biggest challenge for many banks is that their largest control weakness is not a missing control, but rather the absence of connection between the controls they already have. Years of responding to each new regulation with another control, another template and another assessment have produced multiple environments that are simultaneously overloaded and full of blind spots.

This reframes the central question. The goal is not a *bigger* control environment but a *connected* one. Where in which every control is traceable to the risk it addresses, the regulatory expectation it satisfies, and its interdependent controls. This is precisely what Deloitte's Risk Control Framework, enabled by knowledge graphs and AI, is designed to deliver. Once those connections exist, the payoff becomes visible – gaps become visible, duplication becomes removable, and evidence becomes something the system produces rather than something teams assemble under deadline.

Our approach is therefore intentionally counterintuitive. Before adding a single new control, map what you already have and how it connects. Most banks will find they need fewer controls, not more. The controls that remain will finally work as a system rather than a collection.

The banks that make this shift will not just satisfy supervisors more easily. Instead, risk transforms from a cost of doing business into a source of insight into where the organisation is actually exposed, and that is a strategic asset, not a compliance obstacle.

Let’s Talk

If the challenge of a control environment that keeps growing without becoming clearer is familiar within your organisation, the most useful first step is often the easiest: seeing how your existing controls, risks and regulations actually connect.

Deloitte can help you build that picture, using knowledge graphs to map your current control environment, surface the gaps and duplication hidden within it, and identify where connection would deliver the most value.

Let's start with a conversation about where your control environment is most fragmented, and what a connected view could reveal.

Contacts

Eric de Weerdt

Partner – Regulatory, Data & Reporting

edeweerdt@deloitte.nl

Lotte Aelvoet

Partner – Regulatory, Data & Reporting

laelvoet@deloitte.nl

Ali Khalili

Senior Manager (Specialist) – Regulatory, Data & Reporting

alkhalili@deloitte.nl

Deloitte.