VEIL GOVERNANCE RESEARCH · VGR-001

The Missing First *Line of Defence*

Compliance by Design: Formal Verification of Regulated Business Processes

Why banks spend billions on compliance technology and still pay billions in fines — and what formal process verification changes

Leonid Burlakov

DataCraft LLC · Tashkent, Uzbekistan

leonid.burlakov@datacraft.uz

PUBLISHED	SERIES	WEB
March 2026	VGR-001	veilgovernance.com

$5.15B+

Combined AML fines — TD Bank & Danske Bank (2022–2024)

79%

Share of compliance budgets spent on personnel, not technology

Zero

Mainstream commercial tools offering pre-deployment formal process verification

CONTENTS

EXECUTIVE SUMMARY

The industry built detection. It never built prevention.

Despite a decade of rising compliance investment, banking regulators continue to impose record fines. The pattern is consistent: failures are systemic, structural, and detectable in process architecture long before the first transaction is processed.

> *The banking industry has built substantial surveillance infrastructure to detect compliance violations after they occur. This paper argues that very little has been invested in tools that identify structural violations at the design stage — and that this gap is not accidental but follows from the historical trajectory of available technology and regulatory metrics.*

The root cause is a category blind spot. No mainstream BPM platform integrates regulatory reachability verification — ensuring mandatory controls cannot be bypassed on any execution path — into the standard process design workflow. The closest commercial precedent, DCR Solutions, operates in the Danish public sector on a different notation and regulatory context. In banking compliance, the category does not exist as a standard workflow step.

This paper introduces **pre-deployment formal process verification** — a discipline with 30+ years of academic history that has not been commercialised at scale for banking compliance — and argues that DORA Article 8 and the global AML enforcement environment create the first viable commercial window for it.

- **No mainstream BPM tool** currently integrates regulatory reachability verification — the systematic check that mandatory controls cannot be bypassed on any execution path — as part of the standard process design workflow.
- The **79% personnel / 9% technology split** in compliance budgets reflects a fundamentally reactive posture — not an economically optimal one.
- **DORA Article 8** creates a new evidentiary question — how to demonstrate that controls cannot be bypassed — that no existing toolchain answers systematically.
- The **SR 11-7 precedent** shows regulators are willing to mandate formal validation for model classes when the risk is material. Process models are next.

MARKET CONTEXT

The size of the problem

Understanding the commercial opportunity requires sizing three adjacent markets: compliance spending, RegTech, and process management tooling.

$270B

Global financial crime compliance spend per year — LexisNexis / ACAMS True Cost of Financial Crime study [4]

$19B→$60B

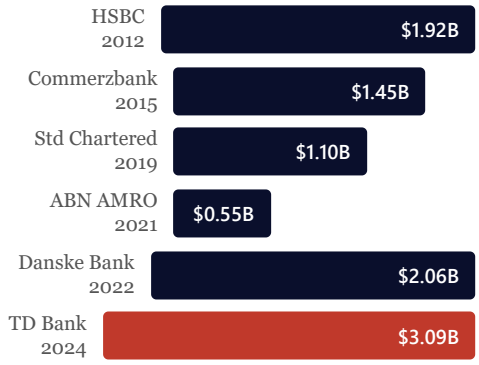
RegTech market 2024→2030, CAGR 18%+ — Gartner Magic Quadrant for Process Mining, 2024 [13]

$15B

BPM / process management platform market (IDC, 2024) — of which pre-deployment formal verification is, in this paper's assessment, near zero

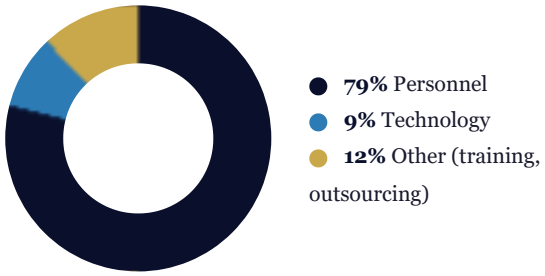
Major AML Enforcement Actions 2012–2024

Selected fines, USD billions — primary source: DOJ, FinCEN, SEC official releases



Compliance Budget Allocation

US & Canada financial institutions (LexisNexis Risk Solutions)



SECTION 1

The Compliance Paradox

Over the past decade, global banks have spent hundreds of billions of dollars building compliance infrastructure. They hired armies of analysts, deployed sophisticated transaction monitoring platforms, and commissioned Big Four audits. Regulatory penalties have not declined. They have accelerated.

1.1 The Enforcement Landscape

In 2024, US regulators assessed **$4.3 billion in financial penalties** against financial institutions — a 522% increase from prior-year levels, with transaction monitoring violations accounting for more than $3.3 billion of that figure, according to Fenergo's annual enforcement analysis [6]. The pattern is not a one-year anomaly: penalties have risen in aggregate across the decade.

The two most instructive recent cases are not outliers. They are archetypes:

TD BANK · OCTOBER 2024

$3.09 Billion

According to the DOJ guilty plea and FinCEN assessment [1][9]: AML monitoring system not updated for 8 consecutive years (2014–2022) despite documented deficiencies. 92% of $18.3 trillion in transaction volume went unmonitored. The DOJ plea agreement documented that certain transaction categories were excluded from monitoring by design decision.

Formal verification cannot prevent intentional misconduct — but makes structural monitoring gaps explicit and auditable before deployment.

DANSKE BANK · DECEMBER 2022

$2.06 Billion

According to the DOJ and SEC resolutions [2][10]: approximately €200B in suspicious transactions through the Estonian branch between 2007–2015. The branch operated on a separate IT system with no automated AML screening — a structural gap in the operating model documented from the time of acquisition. SEC findings noted that the bank made misleading disclosures about AML compliance to investors.

The regulators' findings document that the operating model topology made the violations difficult to detect through standard monitoring.

> *DOJ and SEC findings in both cases identified the same structural signature: the compliance failures were encoded into the process design, not detectable through post-deployment monitoring alone. According to the DOJ plea in the TD Bank matter [1], the monitoring exclusions were the result of documented budget and design decisions — not operational errors in an otherwise sound system.*

1.2 The Budget Paradox

US and Canadian financial institutions spend $61 billion per year on financial crime compliance (LexisNexis Risk Solutions [4]). Of this, 79% goes to personnel and only 9% to technology. Within that 9%, the overwhelming majority funds detective tools: transaction monitoring, KYC platforms,

reporting systems.

Preventive tooling — specifically, tools that verify process design correctness before deployment — represents a negligible fraction of compliance spending. This is not a market inefficiency. **It is a market gap. The category does not exist.**

1.3 The ROI Question

A fair challenge: does this add to costs or reduce them? Honest answer: initial adoption increases costs — skilled analysts are needed to standardise BPMN models and triage counterexample output. The ROI case rests on two mechanisms:

- **Penalty avoidance:** The TD Bank settlement ($3.09B) covered approximately 17 years of the bank's entire technology compliance budget. A single prevented enforcement action funds a verification programme for decades. The asymmetry between prevention cost and remediation cost is the core economic argument.
- **Release cycle compression:** Pre-deployment verification replaces multi-week manual compliance sign-off with a deterministic automated gate. Banks piloting analogous formal methods in adjacent domains (network configuration verification, smart contract auditing) report 30–60% reductions in pre-release review cycles.

Formal verification is not a cost-reduction tool in year one. It is a tail-risk elimination tool — and tail risks in banking compliance have a documented cost in the billions.

1.4 Why Detection Systems Dominate: A Historical Note

The dominance of detective tooling in compliance is not an oversight — it reflects the technological context in which the current infrastructure was built. Understanding this is important for any honest assessment of where formal verification fits.

The post-1991 wave of AML regulation — FATF Recommendations, BSA amendments, the EU's First Money Laundering Directive — coincided with the early commercial maturity of relational databases and transaction processing systems. The technology available and the regulatory metrics being tracked were transactional. Monitoring fitted the moment: it could be built, sold, and audited against measurable outputs (number of SARs filed, transaction coverage percentages).

Process modelling as an enterprise discipline only gained a vendor-neutral standard with BPMN 2.0 in 2011. Formal verification tools for process models emerged in academic literature in the early 2000s — BProVe, Apromore, Alloy-based approaches — but remained in research environments. Graph-based exhaustive reachability analysis at the scale of enterprise banking processes required both the computational resources and the process standardisation that only became widely available in the last decade.

The market built what was technically and commercially viable at the time. Detection was viable. Pre-deployment structural verification was not — until recently. This paper argues that the gap between academic maturity and commercial deployment in this category is now closeable.

SECTION 2

Taxonomy of Compliance Tools

The compliance tooling landscape can be ordered along two axes: (1) *when* in the process lifecycle — pre or post-deployment — and (2) *what* is analysed — individual transactions or process topology. Mapping existing tools onto this matrix reveals a structural gap:

	INDIVIDUAL TRANSACTIONS	PROCESS TOPOLOGY
PRE-DEPLOYMENT	PRE-DEPLOY · TRANSACTION **Rule Engines** Threshold rules, screening lists. Applied transaction-by-transaction. Pre-deployment in configuration, post-deployment in effect.	PRE-DEPLOY · TOPOLOGY ← THE GAP **Formal Process Verification** Exhaustive reachability analysis across all execution paths before deployment. No mainstream BPM platform integrates this into the standard design workflow.
POST-DEPLOYMENT	POST-DEPLOY · TRANSACTION **Transaction Monitoring** NICE Actimize, Fenergo — event-based detection after execution. Identifies violations that have already occurred.	POST-DEPLOY · TOPOLOGY **Process Mining** Celonis, QPR — conformance checking on event logs. Proves the deployed process matched the design. Requires execution history.

This is not an argument against process mining tools — it is an argument for using both. Formal verification proves the design is structurally sound before deployment. Process mining later proves the running code did not deviate from that design. A process that passes formal verification but fails conformance checking in production points to an **implementation gap** — a developer hardcoding a bypass that the BPMN model does not show. Neither tool can find that gap alone. They are complementary layers of assurance, not competitors.

2.1 Why Syntax Validation Is Insufficient

Before examining the tool matrix, it is worth establishing precisely what existing pre-deployment tools do — and do not — check. This distinction is frequently misunderstood by compliance teams and is central to the gap this paper identifies.

A BPMN syntax validator confirms that a process model is *well-formed*: sequences connect correctly, gateways have valid cardinalities, task references are defined, the XML schema is valid. This is analogous to a grammar checker on a document: it confirms correct structure, but makes no claim about meaning or logical content.

Syntax validation does not check **behavioural properties**:

- Whether a specific state (e.g., "sanctions screening") is reachable on all execution paths from the initial state
- Whether all paths to terminal states pass through a mandatory control node

- Whether unreachable states or compliance-critical deadlocks exist in the graph
- Whether a compensation or rollback path is reachable for every forward-path execution

A syntactically perfect BPMN model — one that passes every validator in every major BPM tool — can contain a structurally bypassed sanctions check, an unreachable compliance node, or a deadlock on an exception path. Syntax validation cannot find any of these, because they are not syntactic properties. They are properties of the process *behaviour* across all reachable states.

> *"The model passed validation" and "the model cannot bypass the mandatory control" are claims of entirely different classes. The first is a syntactic statement. The second is a behavioural one — and it requires a different class of tool to verify.*

2.2 Tool Comparison Matrix

The matrix below characterises tool categories based on publicly available product documentation as of Q1 2026. It does not claim to represent the complete feature set of any vendor, and vendors are invited to submit corrections. The purpose is to locate each tool category relative to the pre-deployment reachability gap — not to evaluate overall product quality.

Tool / Category	Pre-Deploy	Reachability	Event Logs	Formal Proof	Regulatory Packs
ARIS (Software AG)	Design-time	Not stated	Not required	Not stated	Not stated
SAP Signavio	Design-time	Not stated	Not required	Not stated	Not stated
Camunda	Design-time	Not stated	Not required	Not stated	Not stated
Celonis / QPR	Post-deploy	Conformance	Required	Not stated	Not stated
BProVe / Apromore	Pre-deploy	Supported	Not required	LTL (partial)	Not stated
DCR Solutions	Pre-deploy	Partial	Not required	Partial	DK public
Pre-Deployment Verification Layer *(e.g. VEIL)*	**Pre-deploy**	**Full reachability**	**Not required**	**Certificate + trace**	**Basel / DORA / SOX**

Capability levels: Supported · Partial / stated with qualification · Not a stated feature = not documented in publicly available materials as of Q1 2026. This characterisation does not imply the capability does not exist — vendors may offer features not reflected in public documentation. The VEIL Governance row describes a reference architecture for the verification category described in this paper.

SECTION 3

What DORA Article 8 Opens Up

The EU's Digital Operational Resilience Act (DORA), effective January 2025, is widely discussed in terms of ICT risk management. A close reading of Article 8 raises a question the market has not yet answered with tooling [3]:

> *DORA Article 8 requires financial entities to "identify, classify and document all ICT supported business functions and processes" and to design "protection and prevention measures" such that "these mechanisms **cannot be circumvented through the normal functioning of the ICT systems**."*

DORA does not explicitly mandate formal graph-based verification of process models. What it does create — as this paper argues — is an **evidentiary question**: how does a financial institution demonstrate — to an auditor, not just assert in a policy document — that a protection mechanism cannot be circumvented?

Current tooling provides two responses that this paper argues are inadequate for the evidentiary standard implied by the regulation:

- **Assertion by documentation:** compliance teams write that controls exist. This may satisfy the letter of a questionnaire, but the language of Article 8 — "cannot be circumvented" — implies a design guarantee, not a policy statement.
- **Retrospective conformance:** process mining tools show whether deployed processes matched the design — but only after execution, on event logs. They do not produce evidence about what *can* happen before deployment.

Neither response provides what this paper argues a rigorous auditor should be able to verify before deployment: a systematic analysis demonstrating that a protection mechanism cannot be bypassed given the designed process topology. Formal verification is one approach to producing that evidence — and, as of this writing, the only known automated, auditable, and pre-deployment approach.

The **SR 11-7 analogy** [5] is offered as context, not as a legal precedent. The US Federal Reserve and OCC introduced mandatory formal validation standards for quantitative models (credit scoring, stress testing) after the 2008 crisis demonstrated that untested models create systemic risk. There is no equivalent standard for process models. This paper argues that the structural logic of the SR 11-7 intervention applies — but does not assert that regulators will or should adopt an equivalent requirement for process models.

SECTION 4

Four Archetypes of Process Failure

Based on analysis of enforcement actions and regulatory findings, compliance failures in banking cluster into four structural archetypes. Each is detectable through formal verification before the first transaction is processed.

ARCHETYPE 1

The Bypassed Control

A mandatory check (sanctions screening, dual approval, KYC verification) exists in the process model, but a parallel execution path allows the process to complete without passing through it. TD Bank: entire transaction categories were excluded from the monitoring topology. The exclusion was a process design decision.

Formal verification asks: are all terminal states reachable only through the mandatory control state? If not — a counterexample trace is generated showing the bypass sequence.

ARCHETYPE 2

The Orphaned Branch

Process branches introduced for edge cases, regulatory updates, or product expansion fail to integrate properly into the compliance core. They create reachable states with no compliant exit — structural deadlocks that manifest as frozen transactions or manual workarounds at operational scale.

Formal verification asks: do reachable states exist with no outgoing compliant path? Cycle detection and reachability analysis identify them structurally — without executing the process.

ARCHETYPE 3

The Invisible Rollback

Compensation flows in saga-pattern processes — refunds, reversals, regulatory notifications — are designed for the happy path and not verified for exception paths. Under failure conditions, compensation may be unreachable or execute in the wrong sequence, violating Basel III atomicity requirements [8].

Formal verification asks: for every forward-path execution, is a corresponding compensation path reachable in reverse sequence?

ARCHETYPE 4

The Breached Time Boundary

Regulatory frameworks impose temporal constraints: transaction holds cannot exceed defined durations, SAR filing must occur within prescribed windows. Under branching or failure conditions, a path may exist in which a deadline is structurally unreachable before the process completes.

Timed automata analysis: a distinct class from structural bypasses, with its own state-space challenges. Where time constraints are formally modelled, verification can prove whether a deadline is reachable in all execution paths.

SECTION 5

What the Market Needs

A tool addressing the gap identified in this paper must satisfy four conditions simultaneously. Tools satisfying conditions 1–3 but not 4 are academic model checkers — mathematically correct but inaccessible to compliance teams.

1

Pre-deployment operation

The tool must work before the first production run, without event logs. It analyses the process model as designed, not as executed.

2

Exhaustive reachability analysis

Must verify properties across all possible execution paths — not sample or simulate. Output: formal proof ("this property holds in all reachable states") or concrete counterexample trace ("this execution sequence reaches a non-compliant state").

3

Two-layer regulatory policy packs

Base layer (mathematical): the engine checks universal structural properties — deadlocks, unreachable states, mandatory node bypass, cycle detection. No legal claims. Pure graph analysis.

Mapping layer (regulatory): policy packs provide structural patterns associated with specific regulatory contexts (DORA Art.8, Basel III, SOX, FCA). These are not legal opinions — they are structured audit scaffolding for qualified compliance counsel.

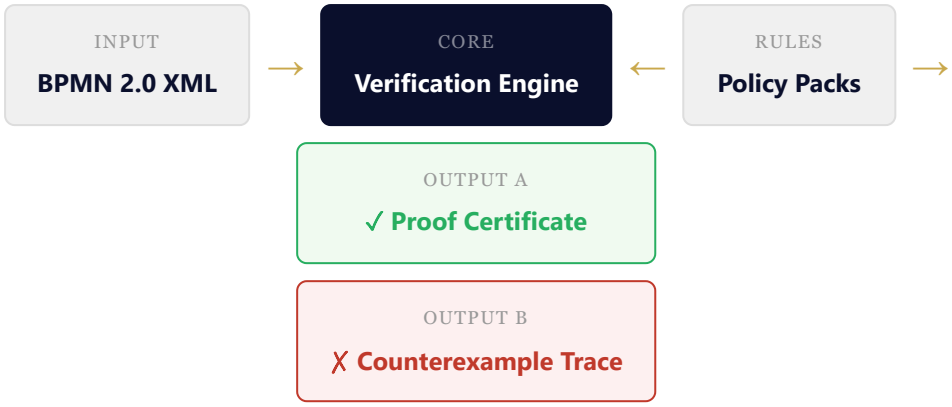
4

Integration with existing BPMN toolchains

Banks have invested significantly in BPMN tools (ARIS, Signavio, Camunda). A verification layer must import from these tools — not replace them. BPMN 2.0 XML import is the minimum viable integration point.

Example Architecture

A platform implementing these principles would follow a verification pipeline. The architecture below illustrates the logical flow — input from existing BPMN toolchains, processing by a formal verification engine cross-referenced against regulatory policy packs, and output as either a proof certificate or a counterexample trace:



THE CORRECT PRODUCT CLAIM VS. THE INCORRECT ONE

> "We have mathematically proven that control node X cannot be bypassed in this process architecture — here is the proof, with attribution to the DORA Art.8 structural pattern it satisfies."

> ~~"Your process complies with DORA."~~

SECTION 6

Known Limitations and Honest Caveats

Any analytical tool has boundaries. The following limitations are real, not theoretical — and any organisation evaluating formal process verification should factor them into its adoption decision.

The BPMN Cleanliness Problem

Real-world enterprise BPMN models frequently contain non-standard annotations, embedded scripts, external system calls, and undocumented conventions that do not export into valid XML. A formal analyser can only verify what is actually represented in the model. The practical implication: the largest adoption barrier is not buying the tool — it is **cleaning and standardising existing process assets** to the point where they can be ingested meaningfully. This is an organisational project that precedes the technical one.

Law-to-Algorithm Translation Risk and Vendor Liability

Regulatory policy packs translate statutory language into structural verification patterns. Legal texts are intentionally flexible and context-dependent. A perfectly correct mathematical proof can confirm a structurally sound process while the underlying regulatory interpretation embedded in the rule is contestable. A tool claiming "your process complies with DORA" becomes a potential defendant if the bank is subsequently fined. The technically and legally correct framing is two-layer: the engine proves structural properties; the policy pack provides regulatory mapping context. **The bank's compliance officer and legal counsel own the conclusion.**

State Space and Practical Scalability

Complex banking processes with hundreds of branching points produce exponentially large state spaces. In practice this is managed through state abstraction, bounded verification windows, and semantic tagging that limits analysis to compliance-relevant state transitions. Very large unstructured processes may generate a high volume of counterexample traces — some theoretical rather than operationally significant. **Analyst triage and rule scoping** are required to keep signal-to-noise ratio manageable.

Cultural and Organisational Adoption

Compliance teams accustomed to producing documentation will need to engage with counterexample traces and reachability graphs. This is a change management challenge of similar scale to the technical one. The 30-year gap between academic maturity and commercial adoption in this space is explained primarily by this barrier. Adoption is most realistic as **a pilot on a single high-risk process class** — not as an immediate organisation-wide deployment.

> *"Formal process verification is not a silver bullet. It does not prevent intentional misconduct, compensate for under-resourced compliance teams, or substitute for legal judgement. What it does — uniquely — is make structural process gaps explicit, auditable, and provable before the first transaction is processed. That is a narrower claim than transformation. It is also a more defensible one."*

SECTION 7

Recommendations

For Banks and Financial Institutions

- Audit the current process verification lifecycle: establish whether any process deployed in the last 12 months received structural reachability analysis before go-live.
- Map DORA Article 8 requirements to your existing BPM toolchain and identify whether "cannot be circumvented" claims are supported by formal evidence or by documentation alone.
- Pilot formal verification on one high-risk process class (AML onboarding, sanctions screening, payment authorisation) before the DORA compliance deadline.
- Evaluate BPMN import tooling: the most critical barrier to adoption is the conversion of existing process models — prioritise vendors who provide AI-assisted BPMN-to-verification workflow.

For Regulators and Supervisory Authorities

- Consider issuing guidance that distinguishes "process design validation" from "process conformance monitoring" in DORA implementation guidance.
- Examine the SR 11-7 model validation precedent as a template for introducing process model validation standards for operational processes in critical functions.
- SupTech programmes requiring banks to submit formally verified process certificates at licensing or periodic review would create immediate and proportionate market demand.

For the Research Community

- 30+ years of academic work on formal verification of BPMN models (LTL/CTL model checking, BProVe, Apromore) has produced no commercial product at scale. The barrier is UX and integration, not mathematics.
- Collaboration between compliance practitioners and formal methods researchers is needed to produce regulatory policy packs — structured rule libraries that translate statutory language into verifiable structural properties.

Methodology & Acknowledgments

RESEARCH PROCESS

This paper is based on analysis of publicly available regulatory enforcement documents, official regulatory publications (DOJ, FinCEN, SEC, OCC, European Parliament), third-party market research (LexisNexis, Fenergo, Gartner, IDC), academic literature on formal verification of business processes, and publicly available vendor documentation.

USE OF AI TOOLS

AI-assisted tools (large language models) were used during the research process for literature discovery, cross-referencing of regulatory sources, structural editing, and translation between English and Russian. All factual claims have been verified against primary sources cited in the References section. The analytical framework, interpretations, conclusions, and all errors are solely the author's responsibility.

This disclosure follows the emerging recommendations of the International Science Council (ISC), Committee on Publication Ethics (COPE), and Nature editorial guidelines on AI use in research publications.

Example Implementation: VEIL Governance

The principles described in this paper — pre-deployment formal process verification, two-layer regulatory policy packs, BPMN import, counterexample traces and proof certificates — are implemented in VEIL Governance, a production compliance verification platform.

The platform produces mathematical proofs of structural process properties (reachability, deadlock detection, cycle analysis, saga/compensation validation, SLA boundary analysis). Policy packs provide structured patterns associated with regulatory contexts (Basel III, DORA, SOX, FCA and others), generating auditable evidence for presentation to compliance officers and regulators.

VEIL Governance does not certify legal compliance. It produces the structural evidence base from which qualified compliance and legal professionals draw their own conclusions.

VEIL Governance — veilgovernance.com

References

[1] U.S. Department of Justice — *United States of America v. TD Bank, N.A.* (October 2024). Guilty plea: conspiracy to commit money laundering, combined sanctions $3.09B. justice.gov

[2] Danske Bank A/S — Official announcement: Resolutions with US and Danish authorities regarding Estonia matter (December 2022). Combined penalty $2.06B. danskebank.com

[3] European Parliament and Council — Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Article 8: ICT risk management framework. eur-lex.europa.eu

[4] LexisNexis Risk Solutions — *True Cost of Financial Crime Compliance Study, United States and Canada.* $61B annual; 79% personnel, 9% technology. risk.lexisnexis.com

[5] U.S. Federal Reserve — *Supervisory Guidance on Model Risk Management* (SR 11-7, April 2011). Establishes mandatory validation framework for quantitative models. federalreserve.gov

[6] Fenergo — *Global Financial Institution Fines & Penalties 2024.* $4.3B US enforcement actions; 522% surge in transaction monitoring violations. fenergo.com

[7] DCR Solutions — Formal process modelling with compliance-by-design, spin-off of IT University of Copenhagen. 20+ commercial clients in public sector. dcrsolutions.net

[8] Basel Committee on Banking Supervision — *Basel III: A global regulatory framework for more resilient banks and banking systems.* Operational risk management requirements. bis.org

[9] FinCEN — Assessment of $1.3B penalty against TD Bank (October 2024). Largest FinCEN penalty in history against a depository institution. fincen.gov

[10] SEC — Charges against Danske Bank for fraud: misleading investors about AML compliance violations (December 2022). Civil settlement $413M. sec.gov

[11] OCC — Cease-and-desist order, $450M civil money penalty against TD Bank for BSA/AML deficiencies (October 2024). occ.treas.gov

[12] Weske, M. — *Business Process Management: Concepts, Languages, Architectures* (3rd ed.). Springer, 2019. springer.com

[13] Gartner — *Magic Quadrant for Process Mining Platforms* (2024). Market size $1.1B in 2024, CAGR 18%+. gartner.com