Certification of True Copy

I, the undersigned, Timothy Prellwitz, appointed Notary Public with Notary ID 20191219, hereby certify that the client presenting the attached document has been identified by me through a government-issued photo ID. I verify to the best of my ability and based on the information provided, that the attached document is a true copy of the documents represented to me.

If there are any questions or concerns, please contact me through the details below.

Stockholm 2026-01-25

Timothy Prellwitz – Notary Public
Document ID: 1-86c7trvmm

Author: Paul Sheridan
Title: Director, Advanced Digital Transformation (ADT)
Affiliation: ADT Framework (Independent Research and Governance Initiative)
Date: January 2026

ADT — Governance-Native Digital Transformation

Abstract. *Advanced Digital Transformation (ADT) is a governance-native, human-guided framework for the design, delivery and operation of large-scale digital and industrial systems. By embedding governance directly into the processes that create systems, ADT ensures accountability, compliance, transparency and quality by design rather than through downstream enforcement. This paper provides an executive overview of how ADT embeds good governance, followed by a structured sanity check assessing conceptual coherence, structural integrity and economic plausibility.*

Companion Document: For an illustrative economic model that contextualises potential savings referenced in this paper, see the Companion Economic Illustration .

1. Executive Summary

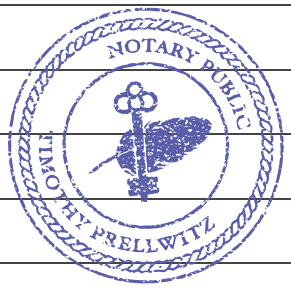
Digital transformation initiatives increasingly fail not because organisations lack automation, but because governance is applied after systems are already operational. This downstream governance model results in escalating remediation costs, excessive compliance overhead and fragile systems that rely on manual policing rather than structural control.

ADT addresses this failure mode by shifting governance upstream into the processes that create systems. Governance is treated as an intrinsic system property rather than an external control layer. Humans define intent, policy, authority, acceptable risk and escalation thresholds; automation enforces and verifies routine execution. Non-routine or exceptional conditions are explicitly escalated to human judgement.

By governing process creation rather than individual processes, ADT ensures that every workflow, platform, service or integration instantiated within the system is compliant, accountable and auditable by design. Governed improvements become reusable system assets, enabling continuous, controlled innovation consistent with emerging Industry 6.0 principles.

1.1 Governance Model

Dimension	ADT Approach
Governance Scope	Process creation and system design (meta-level)
Accountability	Explicit, enforced and traceable by design
Compliance	Built-in, automatic and continuously verified
Oversight	Human authority with automated enforcement
Transparency	Real-time, factual and shared
Outcome	Scalable quality, auditability and control



2. How ADT Embeds Good Governance

2.1 Governance as a Design-Time System Property

ADT embeds good governance by encoding governance principles directly into the architecture of the system. Governance requirements are translated into mandatory process steps, enforceable constraints, explicit decision rights and continuous measurement. Governance is therefore executed continuously as work progresses, not inspected retrospectively.

2.2 Accountability by Construction

ADT enforces accountability structurally. Every decision, approval and action has a single accountable authority, recorded at the point of

execution along with decision context and rationale. Outcomes are traceable back to authorised intent, eliminating ambiguity and supporting regulator and auditor assurance.

2.3 Transparency through an Authoritative Data Source

ADT establishes a single Authoritative Data Source (ADS) that feeds all dashboards, controls and reports. This eliminates parallel spreadsheets and narrative reporting and provides real-time visibility of status, risk, cost, performance and benefits. All stakeholders operate from the same factual, verifiable information.

2.4 Preventive Control and Risk Management

Risk management is embedded directly into execution. Compliance obligations are enforced as mandatory workflow conditions, dependencies and constraints are explicitly modelled and event-driven logic surfaces emerging risk early. This shifts governance from reactive remediation to preventive control.

2.5 Strategic Alignment and Value Assurance

ADT ensures continuous alignment between strategy and execution by explicitly linking initiatives to approved objectives and measurable outcomes. Expected benefits are defined at authorisation and monitored throughout delivery and operation, making misalignment visible before value is lost.

2.6 Continuous Auditability

Because governance controls are embedded in normal operation, audit trails are generated automatically and evidence is produced as a by-product of execution. Audit effort therefore focuses on assurance rather than reconstruction, enabling continuous compliance rather than episodic certification.

2.7 Specification-Authorised Execution and Cybersecurity

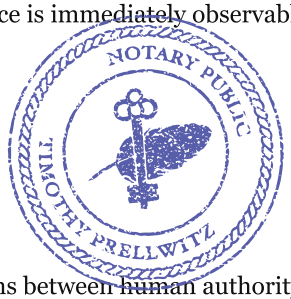
Conventional cybersecurity approaches focus primarily on preventing unauthorised access to systems and detecting malicious activity within operational environments. While these controls remain necessary, they operate largely at the infrastructure and perimeter level and are inherently probabilistic. ADT reframes security at a more fundamental level by treating legitimate system execution as a governance concern rather than an environmental assumption.

Through Specification-Driven Development (SDD), ADT establishes explicit, authoritative specifications that define not only what systems are intended to do, but under what conditions execution is permitted, by whom, and for what declared purpose. Execution that is not authorised by an active specification, validated through the appropriate control domain, and evidenced via the Authoritative Data Source is considered structurally invalid, regardless of whether it is technically possible.

This approach introduces specification-authorised execution as a security primitive. Software components may exist, be copied or even be executed in isolation, but without governance alignment they cannot produce outcomes that are recognised as legitimate within the system of record. The absence of required authorisation, control validation or telemetry is itself a deterministic indicator of unauthorised activity.

Importantly, ADT does not replace existing cybersecurity controls such as network security, identity and access management, vulnerability management or monitoring. These remain essential hygiene measures and continue to reduce exposure and operational risk. However, their role shifts from being the primary arbiters of trust to supporting controls within a governance-native execution framework.

The practical effect is a material reduction in the value of many common cyberattacks. Even where infrastructure is compromised or credentials are misused, unauthorised execution cannot silently generate compliant, auditable or value-bearing outcomes. Detection is simplified because missing or invalid governance evidence is immediately observable, shifting assurance from statistical anomaly detection to continuous validation of authorised execution.



3. Sanity Check and Validation Analysis

3.1 Conceptual Coherence

ADT presents a logically consistent separation of concerns between human authority and automated execution. Governance is treated as an intrinsic system property rather than an external overlay, aligning with established principles of quality-by-design, systems engineering and safety-critical system design.

3.2 Structural Integrity

The framework maintains alignment between intent, mechanisms and outcomes. Upstream governance logically produces downstream reductions in remediation, audit effort and compliance friction. While expressed at an executive and policy level, operational instantiations require disciplined implementation and appropriate technical realisation.

3.3 Economic Plausibility

Economic plausibility is illustrated using estimates from the Consortium for IT Software Quality (CISQ), which reported that poor-quality software imposed costs of $2.41 trillion on the U.S. economy in 2022. ADT's value proposition is based on reducing systemic quality failure through preventive governance. All savings figures are illustrative and adoption-based, not predictive.

3.4 Boundary Conditions

ADT does not eliminate the need for governance expertise; it repositions it upstream. Claims of reduced policing and overhead assume disciplined implementation and alignment between technical, organisational and legal authority structures. Governance failures arising from misaligned incentives or institutional constraints cannot be resolved by technical means alone. In ADT, such failures remain fully visible, traceable and attributable through the Authoritative Data Source, ensuring that accountability is preserved even where corrective action lies outside the system's authority.

4. Conclusion

ADT is conceptually sound, structurally coherent and economically plausible as a governance-native transformation model. Its principal contribution lies in repositioning governance as a design-time system property, enabling scalable, accountable and human-guided automation suitable for complex, regulated and safety-critical environments.

References

1. Consortium for IT Software Quality (CISQ). *The Cost of Poor Software Quality in the US: A 2022 Report*.
2. ISO/IEC 25010:2011. *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE)*.
3. Deming, W. E. *Out of the Crisis*. MIT Press.
4. Leveson, N. *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.

This document is an executive-level analytical overview. Figures are illustrative and not financial forecasts.