

Embedded Governance: Automating Compliance

When Edwards Deming, the US management guru, outlined his fourteen points for achieving corporate excellence in “Out of the Crisis”, he cited the importance of building quality into the process as his third principle (behind good communications first and adaptability second). His premise was that post-production inspection is both inefficient and costly. He advised that attention should focus instead on embedding quality into each step of the underlying process so that after-the-event error detection becomes minimised, if not obviated. It was a philosophy that transformed quality control in manufacturing and the many other industries that embraced it but one that, strangely, found little traction in banking and finance.

So Mr. Deming would probably be aghast at the philosophy and practices that still prevail in financial institutions today: from ex-post audits whose limitations have been severely exposed (SOX did not prevent the collapse of Lehmans, nor did the FSA presage the fallout at Northern Rock) to the ubiquity of end-of-day (or worse still, next day) reconciliation processes, all of which look at symptoms rather than causes, reflecting an old-world focus on outputs rather than inputs. He would probably be agog too at the apparent failure of financial institutions to associate compliance with quality and hence view it not as costly after-the-event overhead of completing business but rather as an integral component of delivering it in a predictable, controlled and efficient manner. In industry this approach is referred to as “in-line” or “in-process” inspection for achieving quality control. In finance it can achieve its alluring but elusive counterpart: Embedded Governance.

Embedded Governance is governance that naturally and continually ensures quality, compliance and control throughout the organisation; governance that is automatic, real-time and constant and, finally, governance that provides what stakeholders and regulators alike want: confidence that the business is being conducted in a complete, competent, and sustainable manner.

This convergence of stakeholder and regulatory objectives reflects a recent evolution of compliance. In former times, stakeholder response to new regulation was a resigned but reluctant allocation of additional budget for compliance, but not one in which an assessment of business value or ROI expectations featured. Within lines of business, profit was the king that compliance (or rather non-compliance) must not be allowed to undermine. However, the demise of Lehmans and the resulting market turmoil focused attention on knowing not just within lines of business, but right across the bank, what the cumulative exposures were and to whom. Unfortunately the simplicity of the question belied the difficulty in answering it as the painful consequences of the “compliance later” approach arose: counterparty data across departments was inconsistent, prices varied, valuations differed.

And as the middle office struggled to quantify the bank’s exposure in its existing books it became apparent the same data deficiencies must be simultaneously preventing the front office from accurately assessing the risk in today’s new transactions. This was truly a real-time problem. Stakeholders swiftly realised the benefit that real-time compliance could provide by ensuring that all products, transactions and supporting activities were serviced by accurate data and processes. The regulatory demands, had they been fully honoured at each step along the way, would have ensured that data was both correct and used correctly. Compliance, rather than undermine profits, could in fact underpin them.

The irony, however, is that financial institutions already spend a lot of money on data management, so where and why does the problem of inaccuracy and inconsistency arise? Largely it is because data management is traditionally regarded as an event (albeit a recurring one) focusing on remediation of errors identified through batch reconciliation. Very often data is repaired at source after it has been already consumed and as a result, while the source may ultimately become Golden Copy at close of day, the reports, valuations and investment decisions made upon earlier versions may have been based on a much less gilded standard. More insidiously, what is, or at least purports to be, “Golden Copy” may not in fact be the source used by downstream systems and throughout the organisation: the position-keeping system may take its rates from a direct feed, risk management from the data warehouse and fund management from the risk system – but only after the risk system has made adjustments that apply for it and it alone. Credit Risk may take it from somewhere else again and what appears to be an appropriate, validated source may not always be the case: Chinese whispers meet data management.

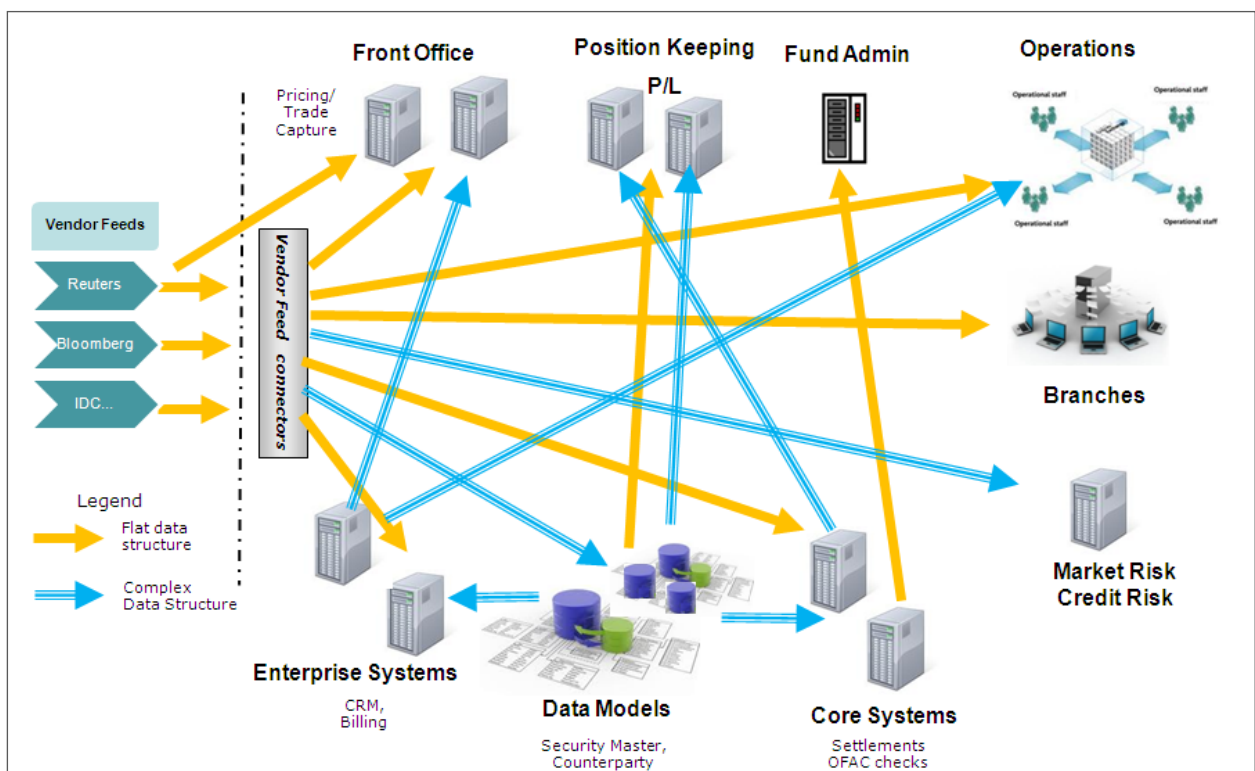


Figure 1: Inconsistent and uncontrolled consumption of enterprise data

Recent developments in risk management and compliance have driven the evolution of data management from a ‘back-room’ technically-focused approach above to a more process-centric transparent activity embedded in key business processes. Thus, maintaining Golden Copy data for the business processes that use it in a transparent and audited manner is the central task of an enterprise data management system. As illustrated below it must feed the Golden Copies of the multiple downstream systems that will use it. The type of data and frequency of changes to it will determine the intensity of the processes, intense for prices, less so for terms & conditions, but in all instances the benefits of process apply: controlled, repeatable, consistent and audited steps.

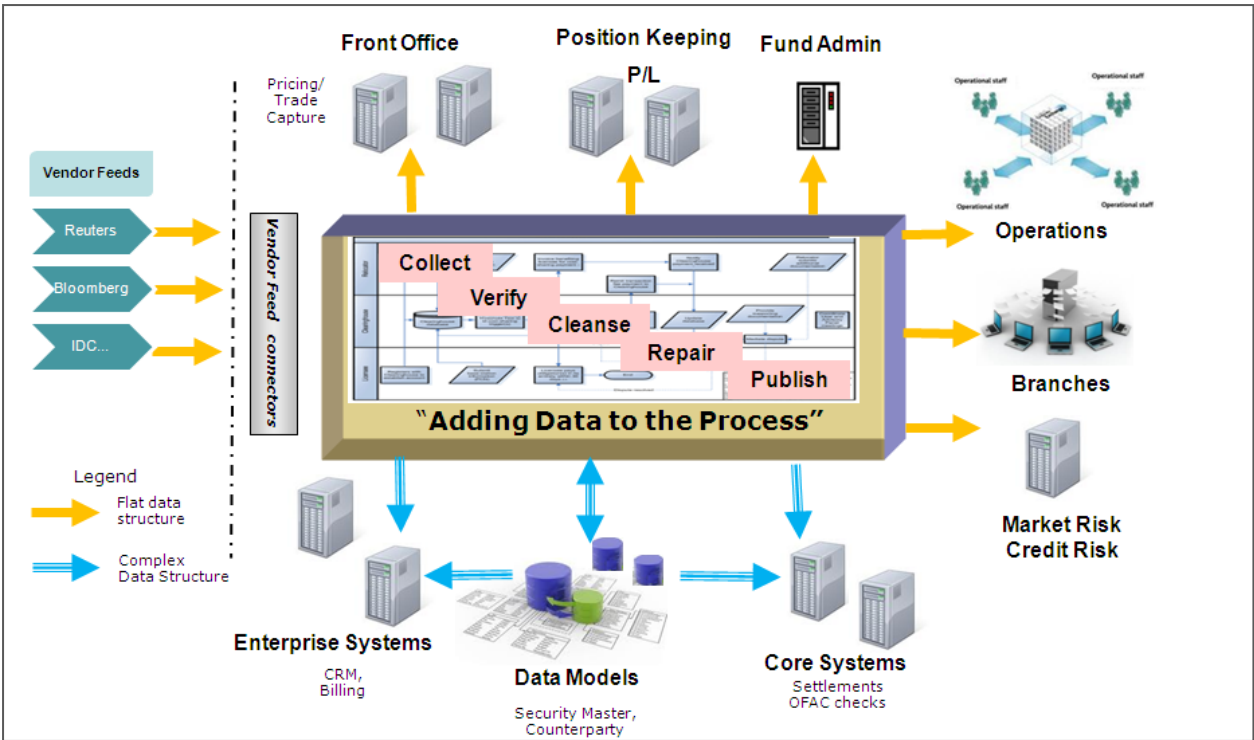


Figure 2: The process approach

However, data quality is not achieved simply when an item of reference data is sourced and validated before being deposited in a database – data quality and transparency increasingly mean tracing requirements and auditing the publication and consumption of that piece of data on its journey throughout the organisation. In its absence the governance gap as illustrated in figure 3 below can arise. Policy may have stated what rates should be used, best intentions may have agreed to use them but practice has a nasty habit of cutting corners - temporary changes become permanent, they are not documented, worse still they may never have been approved. “Compliance later” slowly pervades the organisation.

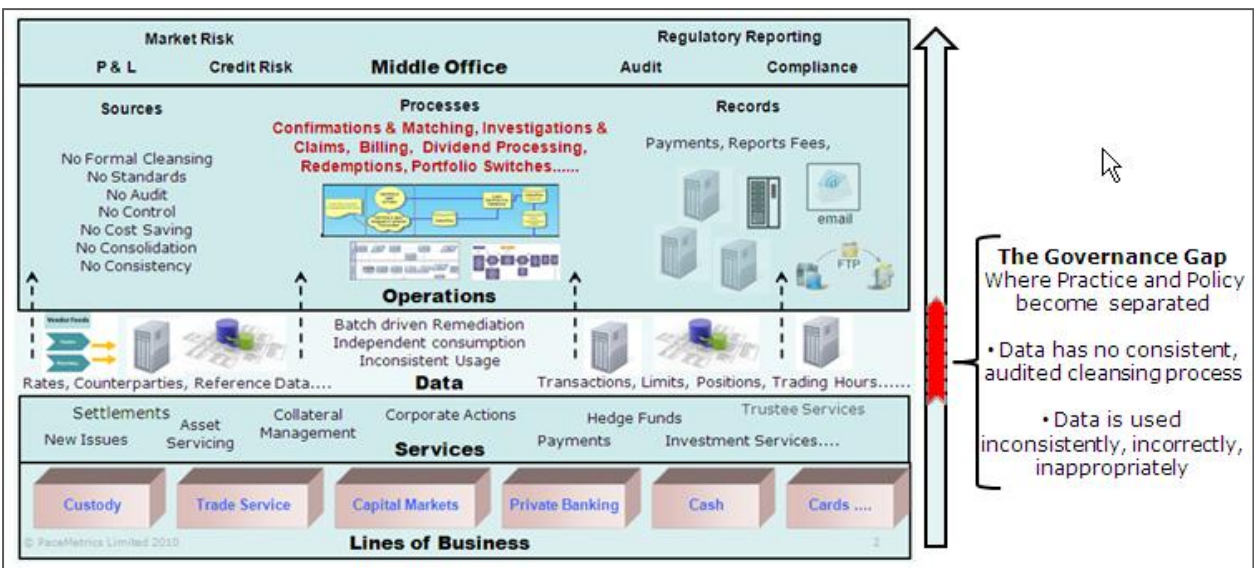


Figure 3: The Governance Gap

Therefore, to close the governance gap illustrated above, what is required is not only 'process around the data' (to ensure it is correct) but also 'data around process' (to ensure it is used correctly); data such as who consumed the data, when, was it still valid, was it amended. Combining the two embeds governance into the organisation by infusing it naturally into the processes that serve it. Consider the example in figure 4 below that illustrates the process of generating regulatory reports.

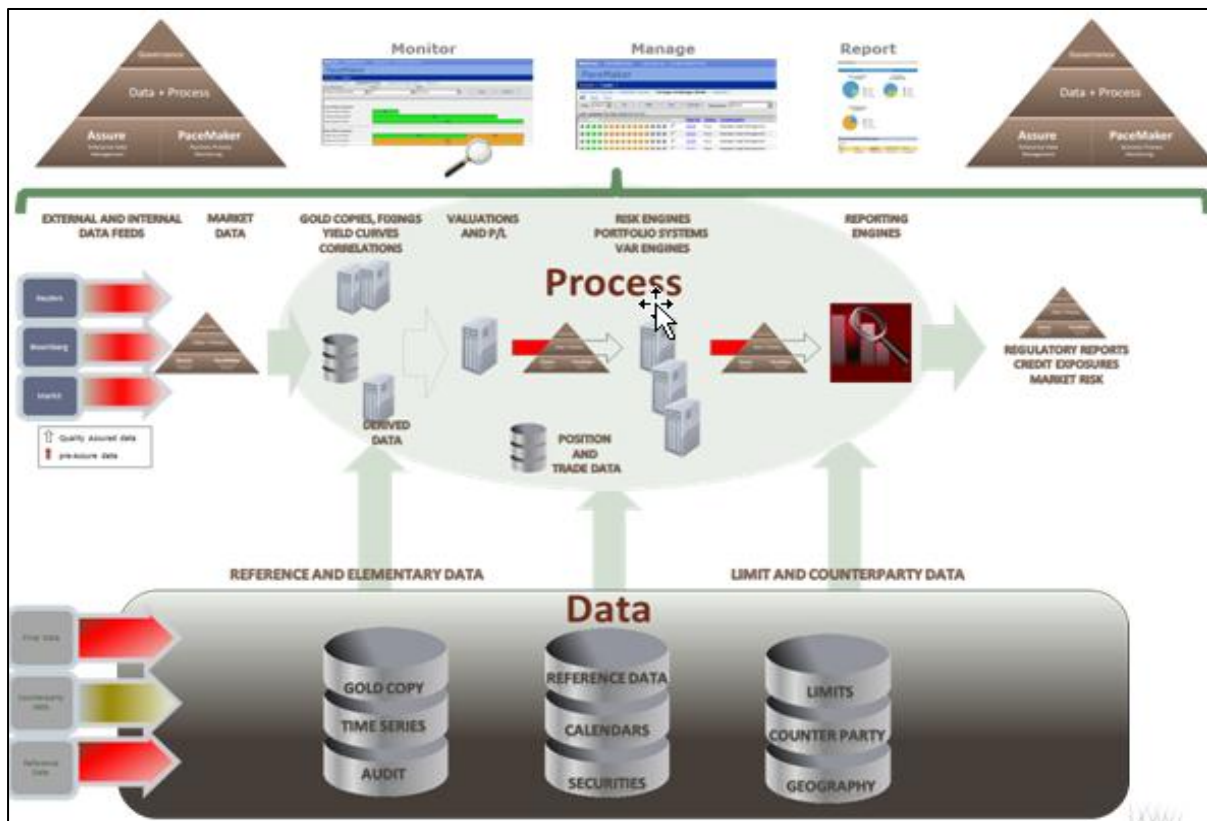


Figure 4: Embedded Governance: Quality Data and Processes

Data cleansing processes are applied not only to data received from external vendors (rates, ratings..) but also to data *in situ* in enterprise databases (reference data, counterparty data, elementary data..) and, critically, but often overlooked, to derived data (fixings, valuations...). There is, after all, as great a need to verify internally derived volatility figures as those sourced from vendors. Process adherence is determined by monitoring the steps along the way: were the files received on time, are they the latest versions, are the counterparties valid, and were they booked correctly? In combination they ensure the right steps are followed and the right data is used. Reports are complete, accurate and timely. Governance has been embedded.

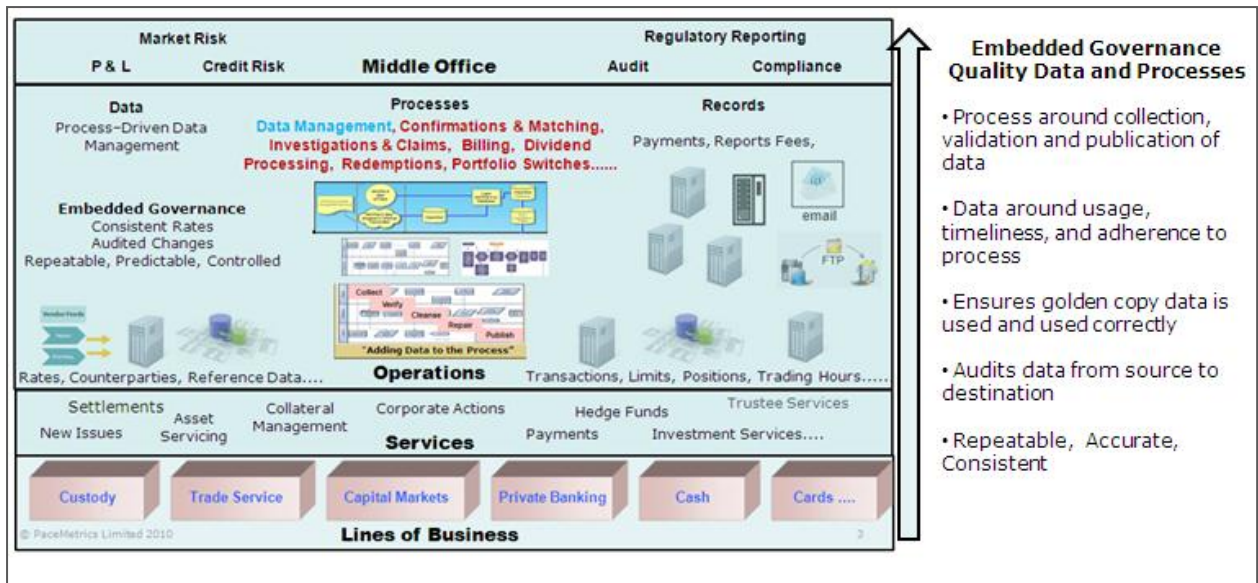


Figure 5: Closing the Governance Gap

Standardised processes are the means by which banks fulfill their transactions and obligations in a consistent and repeatable manner. They cover all aspects of their operation from client on-boarding and settlement procedures through to asset servicing, investigations, new product launch, claims, billing, valuations etc. But process alone is not enough to ensure compliance: accurate algorithms on incorrect positions simply yield inaccurate results. Therefore data management must be added to the process mix to ensure the data they use is accurate and is used appropriately. Compliance is achieved only when the right things are done at the right times and with the right data. Ensuring this, as they occur, is the domain of Embedded Governance. Assuming or hoping they were, and trying desperately to prove it later is the older, more benighted, approach it replaces. Mr. Deming would approve.

[End of Document]

September 2011