Deloitte.



Data Risk & Resiliency: Proactive data management in the Life & Health Insurance Industry

The data risk landscape is evolving rapidly, demanding a shift from reactive firefighting to proactive risk management.

Introduction

Data is no longer merely a supporting element; it's the very engine driving the life insurance industry. From personalized customer experiences to automated underwriting and "next best offer" predictions powered by Artificial Intelligence (AI) and Machine Learning (ML), data fuels every facet of the modern insurance value chain. This reliance is only accelerating, with AI and Machine Learning (ML) transforming how insurers assess risk, personalize products, and interact with customers. However, this increased dependence on data brings a heightened set of challenges. The very data that fuels innovation also exposes insurers to new levels of risk. One can imagine the consequences of a data breach exposing sensitive customer health information, now amplified by the interconnected nature of AI systems. Consider the reputational damage and regulatory scrutiny that could stem from biased algorithms used in automated underwriting. Indeed, many (if not all) operational risks (third-party vulnerabilities, cyberattack, natural disaster, fraud, privacy breach, etc.) share a common damaging consequence: the disruption of data access.

These scenarios underscore the critical importance of robust data risk management – a strategic imperative brought into sharp focus by regulatory guidelines like OSFI E-21.

A Shift in (Re)prioritizing Data Risk

The life insurance industry is experiencing a fundamental shift in its approach to data. No longer a back-office concern, data risk management is moving to the forefront as a strategic imperative. The key trends we observe are 4-fold:

1) Shifting from reactive to proactive data management
2) Board & management visibility into data health & risks
3) Indicator to measure the level of data risk
4) Increased regulatory scrutiny

The data risk landscape is evolving rapidly, demanding a shift from reactive firefighting to proactive risk management. Insurers must anticipate threats, implement preventive controls, and foster a data-aware culture. This requires transparency at all levels, from executives making data-driven decisions to operations teams ensuring data integrity.

Key Risk Indicators (KRIs), encompassing everything from data breaches to unstructured data risks, provide quantifiable metrics for informed decision-making and resource allocation.

This proactive approach is further underscored by increasing regulatory scrutiny, exemplified by OSFI E-21, which mandates robust data governance, security, and quality.

Ultimately, embracing proactive data risk management not only ensures compliance but also strengthens organizational resilience and fosters trust.

OSFI E-21: A Framework for Data Resiliency

OSFI E-21 exemplifies the increasing regulatory scrutiny of data risk management in the insurance sector. Robust data risk management is crucial not only for compliance but also for mitigating a range of interconnected risks, ensuring business continuity, and maintaining the trust of policyholders and partners.

Data Risk plays a critical role as the anchor point for these intertwined risks. Consider two illustrative examples:

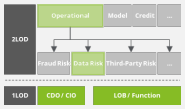
1) Business Continuity: Data Disruptions can paralyze core insurance functions. A cyberattack crippling claims systems could lead to delayed payments and reputational damage. Loss of access to critical actuarial data could hinder reserve calculations and jeopardizing financial stability and regulatory compliance. Robust data backup and recovery plans are no longer optional; they are essential for maintaining

Ultimately, embracing proactive data risk management not only ensures compliance but also strengthens organizational resilience and fosters trust.

Emerging Trends In Managing Data Risk

1 Shifting from reactive to proactive data management

From **reactive** to establishing a forward-looking data management



for **proactive** risk management

2 Board & management visibility into data health & risks

Ask for transparency and effectiveness:

- Executives: *nonbiased decision-making*
- Business units: *actionable levers*
- Operations teams: *effective monitoring*

3 Indicator to measure the level of data risk

Building transparent confidence index of data risks for enlightened decision making, including on complex ones as unstructured data risk

4 Increased regulatory scrutiny

Driving requirements for better, more organized, granular and traceable data

business continuity and fulfilling obligations to policyholders. These plans must encompass all critical data assets, including policyholder information, claims data, and actuarial models.

2) Third-Party Risk: Insurers are increasingly reliant on third parties – brokers, reinsurers, technology providers – whose data security practices directly impact the insurer's risk profile. A breach at a partner organization exposing sensitive customer data can lead to regulatory fines, legal liabilities, and reputational harm for the insurer. Vetting third-party data security controls, establishing strict data sharing agreements, and conducting regular audits are essential for mitigating these risks and protecting policyholder information. This includes implementing robust due diligence processes and ongoing monitoring of third-party compliance with data security standards.

Turning Data Risk into Business Advantage while building a resilient organization

Many insurers grapple with common data challenges, often stemming from siloed systems, manual processes, and inconsistent data definitions. These issues hinder operational efficiency, prevent a holistic view on the exposures, complexify value creation after major transformations, and expose insurers to unnecessary risks.

Applying this concept to a recent transformation: IFRS 17, as an illustration.

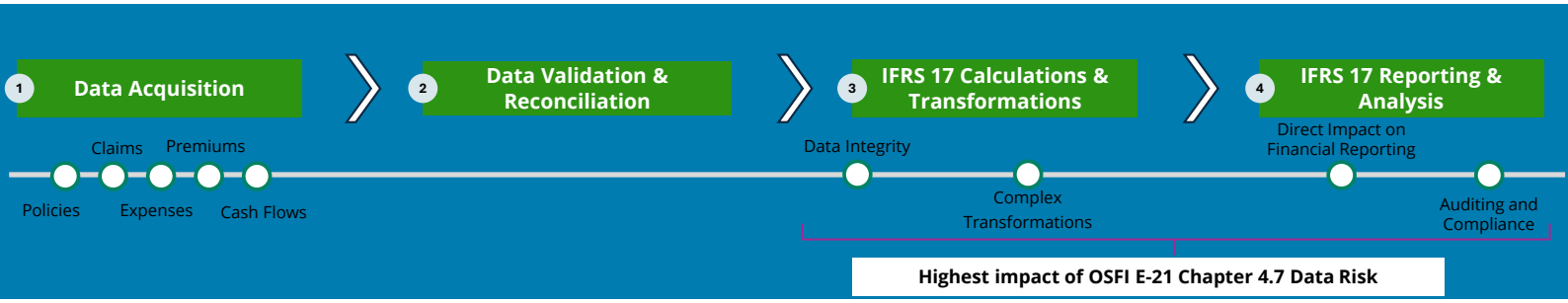
Fragmented policy data scattered across disparate systems makes it difficult to gain a unified customer view, impacting both underwriting decisions and cross-selling opportunities. Similarly, manual premium adjustments performed in spreadsheets increase the risk of errors and create audit trail nightmares.

These challenges are not merely technical hurdles; they represent missed opportunities for improved profitability and strategic decision-making.

However, by embracing the principles of OSFI E-21 and embedding them within their IFRS 17 processes, insurers can turn these pain points into strategic advantages. By implementing robust data governance, quality management, and security controls at each stage of the data lifecycle—from data acquisition to reporting and analysis—insurers can build a strong foundation for data integrity and reliability. This translates into more accurate financial reporting, reduced risk of errors, and enhanced auditability.

The benefits extend far beyond compliance. A well-governed data ecosystem empowers insurers to gain deeper insights into their business. For instance, by reconciling business information with finance and actuarial data at a granular level, insurers can conduct more sophisticated profitability studies. This unified view enables them to identify profitable customer segments, refine pricing strategies, and optimize product offerings and improve overall business performance.

Robust data risk management is crucial not only for compliance but also for mitigating a range of interconnected risks, ensuring business continuity, and maintaining the trust of policyholders and partners.



Enabling The Business With Data Resiliency: IFRS17 Illustration

Imagine being able to analyze profitability not just at the product level, but also by distribution channel, customer demographics, or even specific policy characteristics; all of that with the confidence that business, finance and actuarial have the same definition. This granular insight is only possible with a robust and well-managed data foundation.

Furthermore, streamlined data processes and automated controls free up valuable time and resources, allowing staff to focus on higher-value activities such as strategic analysis, product innovation, and customer relationship management. Robust data security measures not only protect sensitive information but also build trust with customers and regulators, enhancing the insurer's reputation and brand value.

In essence, a proactive approach to data risk management becomes a catalyst for operational excellence, profitability, and competitive differentiation.

Embrace Data's Potential While Mitigating Its Risks

In today's data-driven insurance landscape, proactive data risk management is no longer optional; it is a fundamental requirement for success. The rise of AI and ML in decision-making processes will only amplify this imperative.



OSFI E-21 provides a valuable framework, but true success lies in embracing data's transformative potential while mitigating its inherent risks. By embedding data quality, security, and governance into the core of their operations, insurers can build more resilient, efficient, and customer-centric organizations.

Conclusion

In the end, data risk management is not just about avoiding negative consequences; it's about offering a unique vision of the data ecosystem, unlocking the full potential of data to drive sustainable growth and create long-term value

> "Proactive data risk management is no longer optional; it is a fundamental requirement for success."
>
> *- Nicolas Gemin, Insurance Risk Leader, Deloitte Canada*

Contact us:

Nicolas Gemin
Risk Leader For Insurance
Email: ngemin@deloitte.ca

Andreas Witz
Data Risk & Compliance
Email: awitz@deloitte.ca

About Deloitte

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please seewww.deloitte.com/aboutfor a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

To learn more about how Deloitte's approximately 330,000 professionals, over 11,000 of whom are part of the Canadian firm, please connect with us onLinkedIn,Twitter,Instagram, orFacebook.

© Deloitte LLP and affiliated entities.