SOCIETY OF ACTUARIES®

Article from

CompAct

October 2018
Issue 58

Protecting our Most Valuable Asset: Reinventing Actuarial Data Governance

By Alex Zaidlin, Ben Farnsworth and Natalie Huang

From collection and transformation to application and analysis, actuarial data in life insurance companies is used by various functions for their unique needs. Throughout its lifetime, actuarial data must be carefully monitored to ensure its accuracy and completeness. Incorrect, missing, or inconsistent data, or data misinterpretation and misuse, can lead to significant errors.

Data issues in actuarial modeling and analysis processes can go unnoticed and may result in misstatement in company financial reports. Management of this data should be consistent, transparent, and controlled. Policies and standards around actuarial data management and controls are collectively referred to as actuarial data governance.

WHY DO WE NEED ACTUARIAL DATA GOVERNANCE?

Life insurance companies collect, store, manage, and analyze vast amounts of data, such as confidential policyholder information, actuarial assumptions, and product information.

- Policyholder information includes policy attributes, risk factors, account value and balances, financial transactions, underwriting information, reinsurance information, and other support data.
- Actuarial assumption data includes both economic and noneconomic assumptions plus market and demographic assumptions.
- Product information includes product features and riders, historic sales and policyholder behavioral data, historic financial results, competitive intelligence, and financial and insurance market data.

Actuarial operations rely on data for experience analysis, modeling, reserving, pricing, underwriting, and product development as well as marketing and financial reporting. Unfortunately, this critical information is error prone due to its breadth and complexity. Described in Figure 1 are common pitfalls that can result in misused, misinterpreted, and incorrectly modified data.

Figure 1
Pitfalls in Actuarial Data Management

In addition to wasting time and resources on resolving data issues, these pitfalls can result in error-prone transformation processes, storage wasted from multiple copies of the same information, numerous unvalidated spreadsheets with overlapping functionalities, and process errors resulting in misstatements and delays in reporting. Implementation of an actuarial data governance framework can mitigate these risks and define protocols and policies to be applied if these errors occur.

Components of Actuarial Data Governance

The actuarial data governance framework is a conglomerate of policies, processes, and controls put in place to manage availability, usability, accessibility, integrity, and security of data. A sound actuarial data governance framework would include

a data governance committee, a defined set of policies, and a roadmap to execute and manage those policies through day-to-day operations. The drivers of initial and continuous success for a sound actuarial data governance framework include:

- Seniority and influence of the governance committee members
- Clarity and ease of adaptability of the actuarial data governance policies
- Periodic critical review, communication, and updates to the governance policies and compliance monitoring
- Establishment and periodic critical reevaluation of effectiveness of controls
- Timely update and implementation of function and current data management software and hardware.

There are many approaches in the insurance and other industries for defining and implementing data governance frameworks. We offer an approach that breaks the actuarial data governance into seven independent components that together constitute a sound governance framework.

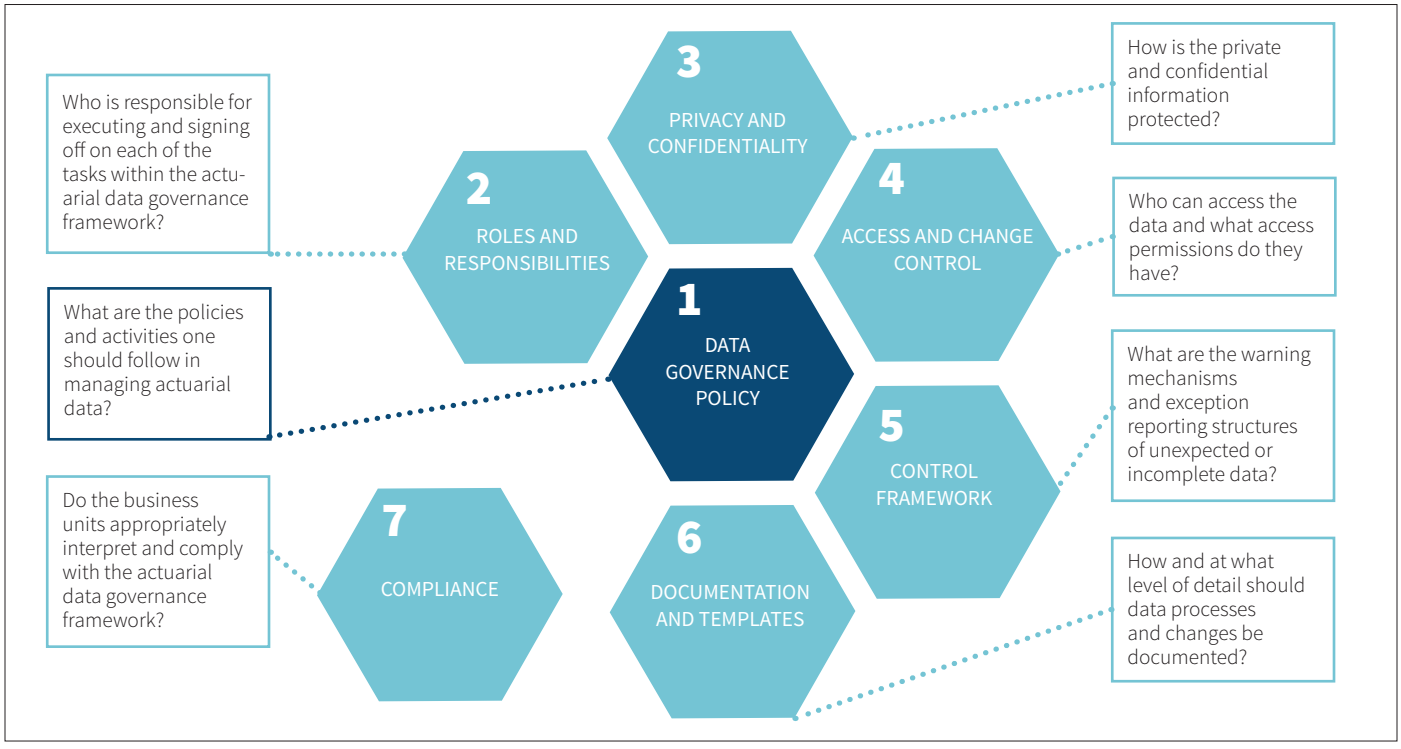
While each component and its purpose is individually defined, all seven are to be developed and implemented in tandem in order to establish a functional and cohesive governance framework. Figure 2 shows the components of actuarial data governance.

1. DATA GOVERNANCE POLICY

The data governance policy is the foundation of any governance framework. It is not meant to be used as process documentation, but rather as guiding principles that are periodically reviewed, updated, and communicated to the impacted groups within the organization.

The actuarial data governance policy consists of a set of standards around retrieving, managing, transforming, preparing, and archiving data. It also contains guidance around data validation, controls, and documentation processes. The policy is typically generalized to be inclusive of multiple areas within the organization. It should include an appendix or supplemental materials that interpret and customize the policy to include standards that are made specific to the application of various groups within business units. These standards encompass internal and external data sourcing to identify quality controlled data sources, data dictionaries, and naming conventions for consistency in data elements across actuarial functions. There are data quality standards to improve data usability, issue management standards to provide standard approaches to manage data-related issues, change management standards

Figure 2
Components of Actuarial Data Governmance



over business case implementation, and testing and data management standards over the data life cycle.

Actuaries do not need to "reinvent the wheel" when it comes to data governance policies. Most organizations have IT or risk groups that produce and manage technology and data related policies for the organization. Teaming with these groups in developing actuarial data governance policies, would ensure consistency in spirit and approach to the more general policies within your company.

2. ROLES AND RESPONSIBILITIES

Clearly defining roles and corresponding responsibilities within the company and its business units is critical to successful actuarial data governance framework implementation. However, embedding a governance structure within the actuarial data domain is often not sufficient or sustainable. Life insurers should aim to build a strong foundation for their enterprise-level data governance framework and have actuarial data governance embedded in the overall policy as one of the segments.

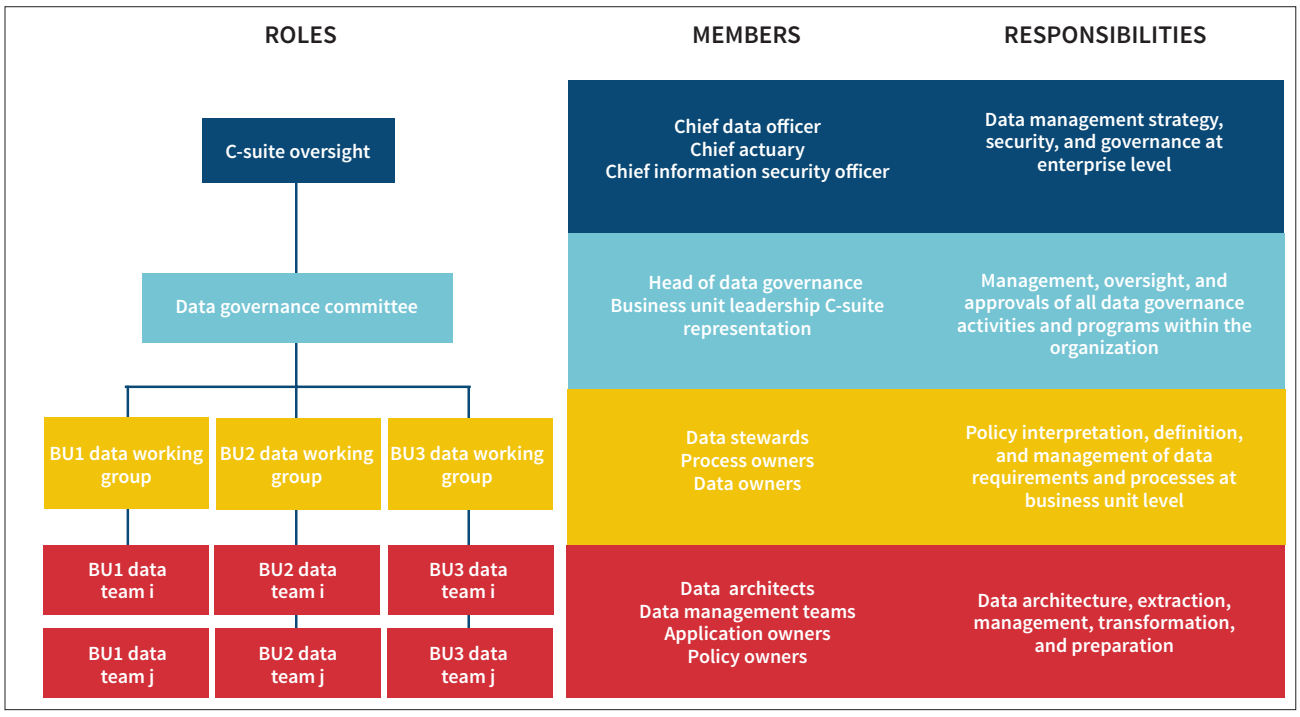
Buy-in and oversight from senior management has proven to be critical for sound actuarial data governance framework structures. The company's senior management program oversight committee should include C-suite executives or their second-in-commands from the Chief Data Office, Chief Actuary Office, and Chief Information Security Office. This group is tasked with overseeing the data management strategy, security, and governance at the enterprise level.

Each representative may have veto power in the decision-making process as various considerations of the actuarial data governance framework are developed. At the next level down, a data governance committee should be formed consisting of business unit leadership, the head of data governance, and potentially C-suite representatives. This committee is typically responsible for the management, policy oversight, and approvals of all data governance activities and initiatives within the organization.

Data working groups and business unit focused data teams should be identified for each business unit within the company. These data working groups, consisting of data stewards, process owners, and data owners, are typically responsible for the business unit's policy interpretation and personalization, definition and management of data requirements, and processes. Data teams will then be responsible for data architecture, extraction, management, transformation and preparation.

Actuaries should be working closely with their IT counterparts to assign roles and responsibilities within the governance structure based on the "right skill for the right job" principle. It is not uncommon to see two individuals, an actuarial business

Figure 3
Data Roles and Responsibilities



owner and an IT technology/data owner, teaming up to fill in a role as they bring different, yet complimentary, skills and institutional knowledge to these roles. An illustrative breakdown of a company's data- oriented committees is depicted in Figure 3.

3. PRIVACY AND CONFIDENTIALITY POLICY

This policy is supplemented by access and change controls and is in place to protect private and confidential data from being viewed, used, or removed by an unauthorized party. The office of the chief information security officer is traditionally responsible for strategy and oversight of this policy. Various data classifications exist within the organization, from policyholders' personally identifiable information (often referred to as PII) to proprietary actuarial assumptions.

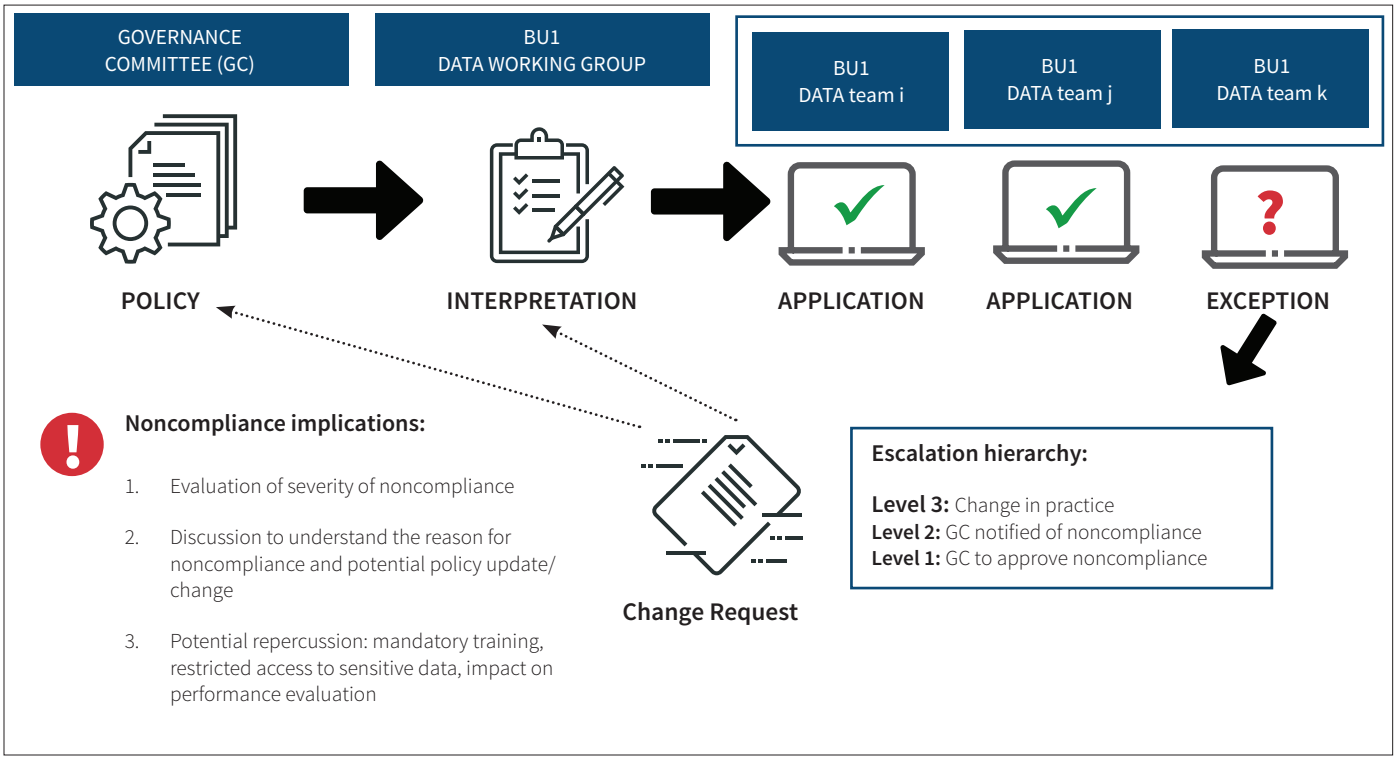
Implementation of this policy begins with classifying the levels of confidentiality of all actuarial data sets and identifying the abilities of technological components to read, maintain and output data. Once the policy describing the treatment of confidential data is rolled out and embedded within the organization, it should be periodically reviewed and updated for new data processes and data sets. Periodic mandatory data privacy and security trainings should be conducted for all relevant groups within the organization to communicate policy changes and keep pulse on policy compliance and data access protocols.

4. ACCESS AND CHANGE CONTROL

Access and change controls are designed to guard against unauthorized access to actuarial data sets within the organization. These controls are also used as safeguards against the misinterpretation or misuse of this complex data that may lead to incorrect analysis conclusions. The ability to access and change actuarial data should be limited to qualified individuals who understand the data and are familiar with how to interpret each of its elements.

Many insurers are moving away from spreadsheets and independent databases as data repositories. These have become cumbersome to manage and do not lend themselves well to be integrated into a sound governance framework. Companies are moving towards enterprise-level data solutions with embedded controls where access and change management are easier to implement. They automate their production processes to

Figure 4
Illustrative Compliance and Remediation Cycle



minimize the need for human access to and interaction with the data.

5. CONTROL FRAMEWORK

The data control framework should be developed, embedded, and automated into the actuarial production processes to track and report the timeliness, accuracy, and completeness of the data as it travels through various production processes. Since controls are integral to a sound actuarial data governance framework, they should be built into every stage of the actuarial data life cycle and be viewed as a vital components of actuarial production processes.

Depending on the criticality of data, both active and passive controls should be implemented into the data processes. Active controls are developed to try and remediate any data errors that occur throughout the process (populate a default value if one is missing, for example), while passive controls are merely there to report on the "health" of the data as it travels through the process. These should be periodically evaluated for adequacy, effectiveness, and implications of failure.

Historically, controls over technology and data have been owned by risk groups within IT departments. However, in the recent years, we have observed close collaboration within many organizations of actuaries designing, implementing and monitoring controls over actuarial processes. Typically, actuaries are responsible for business and actuarially focused controls (for example, reserve trending from quarter to quarter, or logical DAC amortization pattern), while IT teams remain responsible for the technical controls over data accuracy and completeness.

6. DOCUMENTATION AND TEMPLATES

Documentation is key from the very technical comments in the transformation code to change requests and approvals for a sound governance framework. Templates are often created to ensure all the required information is populated to expedite and streamline the documentation process. There are multiple levels of documentation and templates that are typically prescribed as part of an actuarial data governance framework including data dictionaries and technical specifications, data set user guides, issue logs, and change requests.

Change request documentation templates are specifically important for a sound governance framework since all data and data transformation changes need to be traceable throughout data sets and over time. These should include a unique sequential ID so that change impacts can be assessed in the correct order, description of impacted data elements, change description, testing documentation, and impact

analysis. Data change testing processes should not only focus on showing that the change impacted the data in a reasonable manner, but also that other data elements were not unintentionally impacted by the change.

7. COMPLIANCE

The last of the seven components of an actuarial data governance framework is compliance with the actuarial data governance framework. Since actuarial data governance policies standards are typically written to encompass all the actuarial data processes within an organization, they are to be interpreted for validity and applicability by the data working groups of each of the corresponding business units.

Actuarial data governance policies may unintentionally restrict or complicate certain data processes. Therefore, these policies should be periodically updated and should define a process to submit requests for updates or exceptions to the data governance committee. Compliance with actuarial data governance and other company policies should be mandatory and is sometimes directly linked to data users' performance evaluation and variable compensation structures. Figure 4 depicts an illustrative compliance and remediation cycle for an actuarial data governance policy.

IMPLEMENTATION OF ACTUARIAL DATA GOVERNANCE

There are three main phases in the implementation of actuarial data governance: initialize, develop, and embed. Each of the seven components of an actuarial data governance framework can be broken down into these three phases.

Phase 1: Initialize

The initialize phase is characterized by identification, classification, and inventory. During this phase, activities such as inventorying all existing data documentation, dictionaries, controls, and data sets and actuarial models occur to evaluate the current state and structure of the company. From there, any gaps in data documentation and procedure and inefficiencies in the data life cycle can be identified to be addressed in the development stage.

Phase 2: Develop

The develop phase addresses the erroneous procedures and data inefficiencies identified in phase one. The actuarial data governance framework must be built to cater to each company's needs, customized for each company's data life cycle from collection of data sources to analysis of outputs. Here, the first draft of actuarial data governance policies is written and circulated for comments from management and data teams. With the development of the data governance policy, the critical actuarial roles are to be established and their responsibilities in the company are to be defined. This stage includes the drafting and development of the privacy and confidentiality policy, access and change controls, the control framework, documentation policies and templates, and compliance protocols.

Phase 3: Embed

The embed phase is defined by the full establishment and finalization of all actuarial data governance policies, standards, and controls. In this stage, all seven components are finalized and put in place to form the big picture of actuarial data governance. The vision and strategy of the governance bodies and end users are aligned. The result of embedding actuarial data governance is a coherent and efficient data life cycle facilitated and integrated by each of the seven components of the actuarial data governance framework.

From conception to implementation, a sound actuarial data governance framework should address the accuracy and completeness of actuarial data and efficiency of data management processes.

Discussion and development of policies and standards by governing bodies should not be isolated from the data managers and end users. Rather, the vision and expectations of the governing bodies must align with the capabilities of the data working groups and teams. For these entities to connect, an effective data governance policy, roles and responsibilities, privacy and confidentiality policy, access and change controls, control framework, documentation, and compliance policies must be initialized, developed, and embedded throughout the company's data life cycle. An implementation of a sound actuarial data governance framework has proven to reduce erroneous conduct and mitigate inefficient, inconsistent, or misguided data use. ■

Benjamin Farnsworth, FSA, MAAA, CERA, CFA, director, Risk Analytics for KPMG. He can be contacted at *benjaminfarnsworth@kpmg.com.*

Alex Zaidlin, FSA, MAAA, ACIA, director, Risk Analytics for KPMG. He can be contacted at *azaidlin@kpmg.com.*

Natalie Huang, associate, Risk Analytics for KPMG. She can be contacted at *nrhuang@kpmg.com.*