



The “Cloud” as a Life Insurance Policy Administration Solution

TABLE OF CONTENTS

Policy Administration in the Cloud.....	2
Benefits and Risks.....	5
Cloud Adoption in Life Insurance.....	9
Preparing for the Cloud.....	11
Prediction.....	12
Summary.....	12



“ I’ve looked at clouds
from both sides now.
From up and down,
and still somehow,
It’s cloud illusions
I recall. I really don’t
know clouds at all.”

“Both Sides, Now” by Joni Mitchell



One of the most prophetic lyrics in all of folk/rock music may be Joni Mitchell's "I really don't know clouds at all."

NIST Definition of Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

- ▶ On-demand self service
- ▶ Broad network access
- ▶ Resource pooling
- ▶ Rapid elasticity
- ▶ Measured service

Service Models:

- ▶ Software as a Service (SaaS)
- ▶ Platform as a Service (PaaS)
- ▶ Infrastructure as a Service (IaaS)

Deployment Models:

- ▶ Private Cloud
- ▶ Community Cloud
- ▶ Public Cloud
- ▶ Hybrid Cloud

Cloud software takes full advantage of the cloud paradigm by being service-oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

More than 40 years after penning such wonderful words, the illusion of "the cloud" has burst onto the technology scene and dominates headlines and industry discussions.

Part of the illusion – or perhaps more appropriately, confusion – is the marketing hype. In article after article, the cloud is described as "transforming," "disruptive," "game-changing," "a seismic paradigm shift" and "revolutionary." Predictions of adoption and growth rates are reminiscent of the early dot-com era. In the cloud's new world order, corporate IT departments shrink or even disappear. Technology is easily deployed, configurable, frictionless, always current and on-demand. Furthermore, the end user doesn't need to worry about cost or security.

Most technologists would subscribe to the NIST (National Institute of Standards and Technology) definition of Cloud Computing. But contributing to the cloud's illusion/confusion is the fact that "cloud" no longer refers to a pure technology definition. It's basically become an easy way of describing anything happening off-premises – whether it is application-based or remote computing capabilities. "In the cloud" is now a broadly-used term.

While "cloud computing" as a term or brand may have recently been defined, many of the elements of the concept have been around for several decades. The concept of remotely accessing computer power and applications is nearly as old as computing itself. In fact, one might argue that the cloud is more reminiscent of the time-sharing service bureau model for computing of the 1950s and 1960s. In early 2000, with the trend toward IT outsourcing increasing, then-Sun Microsystems CEO Scott McNealy was quoted as saying, *"Five years from now, if you're a CIO with a head for business, you won't be buying computers anymore. You won't buy software either. You'll rent all your resources from a service provider."*¹

Driving the increasing conversation about the cloud are several macro trends. First, from a technological perspective, the acceptance and expansion of IT outsourcing by large corporations have provided a model for moving to the cloud. Off-site data centers, networking services, desktop maintenance and generic networked applications became more acceptable methods of conducting technology operations over time.² In the late 1990s, it was rare to encounter off-shore service providers. Today, it is rare to encounter an organization that does not have some portion of their operation managed remotely.

¹ Quoted in Paul Davis "Infrastructure and Application Solutions Overview", Bank of America Securities, May 2000.

² Harvard Business School – Publication 9-801-310: Application Service Providers", Professor Thomas Eisenmann and Research Associate Sanjay Pothen, January 2001



In this post-recession economy, organizations are faced with a need to deliver new, innovative and enhanced services without increasing risk.

The proliferation and usage of applications on mobile devices is another trend driving the move to the cloud. As much as “eCommerce” meant to the business models of the last decade, mobile commerce, or “mCommerce,” is projected to create even more significant shifts on existing applications, infrastructure and processes. The pervasiveness of internet and mobile technologies makes the cloud a growing reality for business.

However, perhaps the most influential macro trend driving consideration and acceptance of cloud computing is not a technological factor but an economic one. In this post-recession economy, organizations are faced with a need to deliver new, innovative and enhanced services without increasing risk, and operating under flat or even reduced budget levels. There appears to be a broad consensus that cloud computing will save money. Therefore it is natural that the cloud would receive heightened consideration by many organizations and their leadership.

Given its conservative nature, the life insurance market remains guarded when it comes to cloud-based services. Recent industry analyst reports suggest that the adoption of cloud computing in core insurance systems is still relatively low with less than 5% of carriers having adopted some Software-as-a-Service model, and more than 75% of carriers indicating they are not considering the cloud in the near term.³ There does appear to be some movement in certain circumstances, including niche or specialty products, smaller blocks of policies and smaller carriers, and more acceptance in Europe than in North America.⁴

POLICY ADMINISTRATION IN THE CLOUD

There are two typical models for delivery of policy administration services (PAS) in the cloud.

1. Application Service Provider (ASP)
2. Software-as-a-Service (SaaS)

The models are very similar and share a common objective of reducing IT overhead. However, there are several distinguishing characteristics between the approaches. The table on the following page highlights a few of the differences compared to the traditional, licensed software approach.

³ Novarica Insurance Technology Research Council: Cloud and SaaS at US Insurers: Experience and Expectations, November 2010

⁴ Celent Research: Cloud Computing, Software as a Service and Technology Outsourcing for Insurers, October 2009



TYPES OF POLICY ADMINISTRATION

	SaaS	ASP	Traditional Licensed Software
<i>Overview</i>	<ul style="list-style-type: none"> ▶ PAS developed specifically for and accessed via the internet. ▶ SaaS technologies are designed specifically for multiple, simultaneous users (multi-tenant) on shared hardware, which lends to a lower costs. ▶ The vendor supports the application and related hardware. 	<ul style="list-style-type: none"> ▶ PAS is hosted at a remote location on servers that may or may not be owned by the insurer. PAS is accessed via the internet. ▶ The PAS is typically still single tenant (single instance application). ▶ The vendor supports the application and related hardware. 	<ul style="list-style-type: none"> ▶ PAS licensed and installed at the insurer. ▶ Insurer assumes responsibility for server maintenance, troubleshooting, data backups and security. May or may not contract with software vendor for application maintenance.
<i>Contract</i>	<ul style="list-style-type: none"> ▶ Software access/software subscription model. ▶ Contract period may be as short as month-to-month. ▶ Insurer must understand and manage service level agreements. 	<ul style="list-style-type: none"> ▶ Software access/software subscription model. ▶ Term is typically three years (as short as one; as long as three). ▶ Insurer must understand and manage service level agreements. 	<ul style="list-style-type: none"> ▶ Software license agreement. ▶ Typically no term commitment (may be a minimum maintenance period required). ▶ Agreement covers purchase and ongoing maintenance.
<i>Customization</i>	<ul style="list-style-type: none"> ▶ Because of multi-tenancy, as little customization as possible is preferred. 	<ul style="list-style-type: none"> ▶ Because of single tenancy, as little customization as possible is preferred. However, more customization is done in an ASP mode. 	<ul style="list-style-type: none"> ▶ Insurer typically customizes application heavily.
<i>Upgrades</i>	<ul style="list-style-type: none"> ▶ Frequent – Release upgrades are mandatory and are automatically made by the vendor. ▶ Because of multi-tenancy, changes affect all users simultaneously. 	<ul style="list-style-type: none"> ▶ Typically less frequent. Insurer can influence release content and schedule. Upgrades are made by the vendor but lack of multi-tenancy means multi-instance upgrades. 	<ul style="list-style-type: none"> ▶ Infrequent – Insurer must install the upgrade. ▶ Upgrade, could incur additional expense, if not specified in contract.
<i>Data</i>	<ul style="list-style-type: none"> ▶ Insurer owns its data. Contract should address retention and data rights/retrieval. 	<ul style="list-style-type: none"> ▶ Insurer owns its data. Contract should address retention and data rights/retrieval. 	<ul style="list-style-type: none"> ▶ Insurer owns and maintains its data.



In the SaaS model, the offering needs most functionality to perform in the same way for each client and in order for an application to deliver the value that it promises.

By definition, a policy administration application is the system of record for all policies that an insurance company has written. While somewhat standard by design, policy administration systems are highly tailored for a specific carrier and its product offerings. The nature of policy administration applications begs the question, is an application that requires heavy customization appropriate for the cloud?

The ASP model emerged as the preferred application hosting model with the initial emergence of internet-accessed applications. Over time, however, the ASPs and their clients discovered that the cost of customizing and maintaining multiple instances of the same application was greater than anticipated. Economies of scale could not be achieved and anticipated savings did not materialize.

In the SaaS model, the offering needs most functionality to perform in the same way for each client and in order for an application to deliver the value that it promises. The SaaS model of shared software with little or no customization may suffice for some “commodity” financial products. Is this acceptable for your core system that must differentiate itself with unique capabilities?

A policy administration system is a critical business application that integrates and interacts with other core business applications every day. The system receives input from and produces information for multiple other systems. This interaction requires business process mapping and technological integration with a carrier’s internal systems – not to mention a new approach to security. These complex activities demand customization combined with a close-knit and flexible relationship between the vendor and carrier IT organizations. This requirement tends to favor the ASP approach and appears to be a disadvantage to the SaaS model.

To achieve a higher level of effectiveness in the cloud, a policy administration application should take a hybrid approach – one that is a robust, customized ASP model for core functionality with a more-common SaaS approach to transaction interface and data reporting and analysis. In this hybrid approach, the customization and interaction with a carrier’s other core systems can be achieved through the core application, maintaining the unique carrier product functionality, while at the same time obtaining some of the cost efficiency and benefits of non-differentiating business processes through the use of standard web-based access tools.



A life insurance carrier should consider both the benefits and risk when planning to outsource any policy administration core system.

BENEFITS AND RISKS

The cloud promises several business and technological benefits, but has risks as well. A life insurance carrier should consider both the benefits and risks when planning to outsource any policy administration core system.

COST SAVINGS

The promise of cloud computing is that the “as-a-service” paradigm will save money. In a cloud environment, the cost drivers of network operations and monitoring, data center operations, application development and support shift from the carrier to the vendor. In financial terms, it shifts the traditional capital expenditure component of technology costs (licensing, infrastructure, etc.) to an operating expense paid over time associated with volume.

An insurer should consider the fully-loaded costs of hosting applications on site (the traditional licensed software model) and include that in the technology acquisition and evaluation model when comparing to the associated costs of the cloud model. The internal costs of initial licensing, data center costs and IT staffing – as well as the ongoing costs of ongoing upgrades – need to be factored into any analysis. The promise of the cloud is that many of these infrastructure costs can be shared among a vendor’s clients and achieve shared economies of scale.

A carrier should also consider the robustness and risk of the cloud application. Will implementing the service increase employee productivity? Will it facilitate or expedite growth? Will it deliver service more efficiently to the enterprise? These questions should all be factored into a carrier’s decision-making process.

When considering policy administration solutions in the cloud, the need to customize and integrate with a carrier’s other critical systems may erode some of the initial savings expected by a pure cloud solution which anticipates a standard approach and model. Likewise, an implementation which requires conversion of existing policies onto a cloud application will incur similar conversion costs as under a traditional licensed software approach. Over time, the economies of scale should still provide the opportunity to deliver a cloud solution at a lower total cost of ownership than a traditional licensed software approach.

CONCENTRATION ON CORE COMPETENCY

In times when budgets are tight and carriers are expected to do more with the same or even fewer resources, shifting to the cloud can provide the opportunity to transfer certain tasks to the cloud provider (such as capacity planning, load balancing, upgrades and upgrade management). In addition, it allows a carrier to focus its resources on more strategic business needs. However, be forewarned, some of those resources should be shifted to increased demands for governance and monitoring of the outsourced relationship.

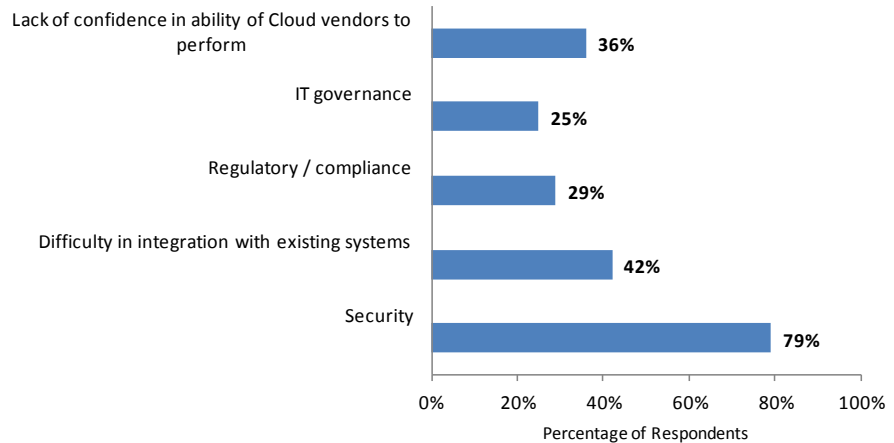


Since the cloud model is designed for remote accessibility, a carrier representative can cooperate with an agent on a complex illustration, or a customer service representative can interact with an insured online.

VIRTUAL-MULTIPLE ACCESS

One of the benefits of a cloud-based solution is the capability to provide simultaneous access to information by multiple stakeholders securely via the internet. Since the cloud model is designed for remote accessibility, a carrier representative can cooperate with an agent on a complex illustration, or a customer service representative can interact with an insured online. Online access expansion could even reduce the amount of carrier support resources, as agents and insureds can access data and transact certain authorized business transitions directly. The traditional “client-server” software license and behind-the-firewall model would require a massive overhaul to be able to meet the expectations of this “connected” virtual environment.

Key barriers to Cloud adoption



Figures in the chart do not add up to 100 percent as multiple responses have been chosen by each respondent

Source: KPMG's *The Cloud: Changing the Business Ecosystem*, 2011

SECURITY

The key issue behind the insurance industry's cautious approach to cloud computing thus far has to be the security and data privacy concerns. Outsourcing technology increases the carrier's responsibility for understanding the disaster recovery/business continuity capabilities and overall reliability/stability of the SaaS provider. In a true multi-tenant environment, concerns over data being compromised, mixed with data from other customers or released by mistake is often cited as the sole reason for ignoring consideration of the cloud for policy administration solutions.



Given that remote computing has been proven successful as a model in many industries for many years, data security should not be the sole reason for eliminating cloud computing as a strategic option.

There is no doubt that operating in a shared infrastructure introduces risks and issues that do not exist in an exclusive “behind-the-firewall,” traditional software environment. However, given that remote computing has been proven successful as a model in many industries for many years, data security should not be the sole reason for eliminating cloud computing as a strategic option. Instead, a carrier should proceed with caution in evaluating the security, privacy, regulatory and compliance aspects of a cloud provider. The carrier should firmly establish security expectations and precautions. Data should be classified by sensitivity to determine exposure tolerance. Logical partitioning, vulnerability testing, penetration testing, data encryption and data obfuscation/masking are examples of tools and processes which minimize security risk. The carrier should understand the jurisdiction in which the data is stored and the cloud provider’s ability to move or process the data without the carrier’s knowledge.

A cloud vendor should undergo an extensive SSAE 16 examination annually to provide a level of assurance that both its business process and information technology controls are suitably designed and operating effectively. The carrier should consider the SSAE controls in regards to its overall internal control operating environment.

While a carrier can outsource its applications and data, it must maintain the responsibility and accountability for its control environment and security. This means working closely with its cloud provider. A secure environment is a joint effort between the cloud provider and the carrier’s security and compliance departments. Increased collaboration between the two should result in effective implementation of controls and improve processes to reduce the overall risk. It is essential that the carrier and cloud partner provider act in tandem to create an effective environment.

INTEGRATION/CUSTOMIZATION

As previously mentioned, a SaaS model is best equipped to deliver promised cost benefits when standardization is high and customization is low. Cloud vendors like to tout their “plug and play” capabilities. Unfortunately, many purchasers have learned the hard way that things are hardly ever that simple. Most severely underestimate the efforts required to integrate with their existing systems.

Many carriers have already made significant investments in hardware, networks, application support, customization and integration. Thus, any move from their existing environment proves difficult. The greater the number of integration points and interfaces, the greater the effort required to migrate to the cloud. Integration and customization, therefore, presents additional challenges to the adoption of a cloud model for policy administration systems.



A carrier must consider how to arrive at an acceptable arrangement with a vendor that governs business, legal and technical matters.

It was previously noted that a hybrid approach to policy administration in the cloud provides the best model for success. The hybrid model leverages the customized ASP core model for integration and interaction with the carrier, while taking advantage of the cost efficiency and standardization of transaction processing and data access normally associated with a cloud SaaS approach. A hybrid approach should also be able to include private-cloud features such as limitations on the size of the client base and access rights. Under the hybrid approach, upgrades can be delivered more frequently and the carrier and vendor can work more closely together to create an effective IT environment.

VENDOR READINESS

Operating in the cloud is a different business model than the traditional licensed software and implementation approach. Just because a vendor may be good at delivering capabilities through a license does not mean it will be solid at cloud delivery.

A carrier must consider how to arrive at an acceptable arrangement with a vendor that governs business, legal and technical matters. Historically, a carrier focused on a vendor's functionality, approach to research and development and cost. Procurement was often limited to a few individuals negotiating the license terms and costs.

In a cloud environment, more parties must be involved in the procurement assessment. Legal, security, IT, business, compliance all need to understand the relationship with the vendor. It is no longer just about cost and R&D. It is also about how the vendor runs its operations, its data center and its control environment. As an extension of the carrier, does the vendor understand it operates in a highly regulated industry in terms of compliance and security? Has the vendor made the fundamental shift from being a software development entity to a technology service delivery organization? Do they have the service and support infrastructure in place to deliver on the contractual commitments and agreed-upon service levels? Do they have the culture to be a service provider and understand they are an extension of the carrier's operations?

A carrier needs to assess its ability to manage and monitor the relationship to a cloud vendor in terms of its IT governance, procurement and relationship models. It is about collaborating as a team to achieve a joint objective.



Cloud computing offers small insurers the opportunity to reduce the cost burden and IT expertise needed in the traditional approach and enable them to compete more effectively with larger organizations.

CLOUD ADOPTION IN LIFE INSURANCE

As previously highlighted, adoption of cloud computing in policy administration life insurance is low and is expected to receive little attention in the near future. Historically, policy administration cloud computing occurred as business units bypassed IT departments, typically in small or niche circumstances, to achieve a lower cost point or more rapid time-to-market.

As carriers express concerns over regulation, security, complexity and integration, some are considering the cloud for policy administration and are carefully testing the water.

SMALLER INSURERS

Smaller insurance carriers have largely been unable to take advantage of robust IT solutions due to the high upfront and ongoing costs of traditional licensed software products. Cloud computing offers the opportunity to reduce the cost burden and IT expertise needed in the traditional approach and enable them to compete more effectively with larger organizations. Early adoption of cloud technologies can perhaps provide a smaller organization with an opportunity to transform its service models, change perception and gain a competitive edge. It is, therefore, expected that adoption of the cloud among smaller carriers will initially be higher in comparison to the rest of the market.

NEW PRODUCT LAUNCH

Often, the investment to launch a new product in the carrier's traditional licensed software environment can prevent the product from actually coming to market. The hurdle rate is simply too large. IT department backlog and dealing with current production issues can limit the timelines. We talked recently with one carrier where a "simple" new product launch was going to cost over \$1 million and system work could not even begin for 15 months (if approved quickly). Carriers thus compromise on product design and features or miss market opportunities due to this environment.

Some carriers are turning to the cloud as an alternative. Once the initial interplay with other enterprise systems is in place, a cloud provider should be able to provision a new product in a much more cost-effective and timely manner. The real potential of the cloud is to provide the opportunity to enter new markets and offer new services that result in a competitive advantage during periods of rapidly shifting markets.



For speciality, niche or complex products, a carrier can obtain a well-designed and supported cloud solution vs. an inefficient and costly work-around alternative from their core system.

SPECIALTY LINES AND PRODUCTS

Andesa has nearly 30 years of experience in the life insurance industry, serving the unique needs of the COLI and BOLI market for several of the largest life insurance carriers in an outsourced environment. In addition, Andesa has helped its carrier clients target specific markets or products with complex designs and features including Private Placement, Stable Value Wrapped, Hybrid products, Market-Value Adjusted products, Experienced Rated products, Illiquid Fund Processing, etc.

To avoid the diversion of focus and resources from the carrier's main strategy, consideration of the cloud for niche lines and products is gaining momentum as an alternative. For specialty, niche or complex products, a carrier can obtain a well-designed and supported cloud solution vs. an inefficient and costly work-around alternative from their core system.

CLOSED BLOCKS

Carriers want to control current and future costs. For a variety of valid reasons, many carriers have a number of closed blocks (no longer actively being sold and positioned for run-out). For a carrier focused on the future, closed blocks are often treated as non-core operations.

Outsourcing closed blocks of business is gaining acceptance. Depending on where that particular carrier finds itself in regard to cost position, manual processes, size and nature of the product and strategic focus, there are a number of possible cloud solutions. Carriers can consider outsourcing to the cloud for a technical solution – or outsourcing the full business process and customer support as well.



The cloud is a business strategy that warrants careful thought and consideration.

PREPARING FOR THE CLOUD

Successful cloud deployment starts with a comprehensive cloud strategy. An insurer should not move to the cloud solely to be in the cloud. The cloud is broader than an IT strategy. It is more than renting servers and storage on demand to reduce infrastructure costs. Its scope extends beyond platforms and applications to encompass multiple system interactions, business processes, compliance, etc. It is a business strategy that warrants careful thought and consideration.

An insurance company considering the cloud for policy administration as a strategy should consider these actions:

1. Understand the current condition and scope of your entire IT infrastructure and application portfolio. Plan your move to the cloud cautiously. Consider the commercial and technical issues unique to your situation – including the state of your existing investments, complexity and availability. From this assessment, identify a prioritized list of applications which could move to the cloud and what should be associated sequence and timing.
2. Understand that while you can outsource applications and tasks, you cannot outsource accountability and responsibility. The relationship with your vendor should be based upon an understanding of clear governance and service level expectations. If you want to be successful in the cloud, focus on the contract. Set the standards for success and provide the necessary oversight. Assess and appraise frequently.
3. Keep your cloud efforts on track. Remove operational and technical barriers. Redesign key processes to support cloud implementation. Changes to procurement and IT skill sets are examples of differences related to operating in a cloud environment. Organizations that have successfully migrated to the cloud cite involvement of the audit, security and compliance departments from the beginning as one of their most critical success factors.⁵

⁵ ComputerWorldUK, “Best practices for scaling up SaaS”, February 14, 2012



PREDICTION

The overall market for cloud-delivered solutions will continue to increase. Over the next five years, insurance carriers will cautiously explore core policy administration solutions and measure and monitor the benefits.

SUMMARY

- ▶ Acceptance of cloud computing is increasing, although adoption for core policy administration applications is expected to be cautious.
- ▶ A hybrid approach which permits customization and integration while enforcing cost-effective standards for interaction and data retrieval may prove to be the best approach for policy administration cloud services.
- ▶ A carrier must consider both the benefits and risks associated with a move to a cloud environment.
- ▶ Adoption for smaller insurers, new product launches, unique niches, complex products or closed blocks may be the early uses of cloud policy administration.
- ▶ In a cloud environment, multiple parties should be involved in the procurement assessment and contracting process to ensure a successful evaluation, understanding and ongoing relationship.



ABOUT ANDESA SERVICES

Andesa Services provides comprehensive, integrated policy administration, plan administration and support solutions for life insurance and annuity carriers and producers.

Andesa began as a pioneer in the field of COLI/BOLI policy administration. Today, more than 30 years later, we partner with seven of the top 13 life and annuity carriers and several top brokers. We offer a suite of SaaS and ASP services, all backed by decades of proven, practical expertise in the industry.

Andesa's highly experienced team of U.S.-based professionals is made up of devoted client advocates who help industry leaders save time, reduce risk and tap unrealized value.



For more information, please contact:

Ron Scheese – President and CEO
ron.scheese@andesaservices.com
610-821-8980

or visit our web site at andesaservices.com.