WHENEVER INSURERS ARE SURVEYED ABOUT THE ARRAY OF CHALLENGES CONFRONTING THEM, THEY ININVARIBLY IDENTIFY DEALING WITH REGULATORY COMPLIANCE AS A TOP CONCERN.

In response to the compliance challenge, insurers increasingly rely on technological solutions. They’re finding there is no better way to deal with the blizzard of regulations and guidance documents issued by federal and state agencies.

“If you look at the IT budgets of insurance companies, we estimate today that up to 25% to 30% of annual budgets are spent on risk management and security management, including disaster recovery and business continuity management measures,” said Juergen Weiss, managing vice president of Gartner, where he heads the insurance advisory team.

The changing nature of compliance and risk management has transformed how insurers use technology, Weiss said.

“Risk management topics used to be largely in the domain of the actuaries, who used to do risk modeling on desktop applications. In most organizations, there was not an enterprise-wide approach for risk and security management. Increasingly that is changing,” he said.

“Basically, what we’re seeing is a much stronger business dimension of risk. In Solvency II, for instance, new regulations are being positioned as, ‘Can you guarantee sustainability and the competitiveness of your organization?’ It’s no longer just an actuarial question, but one that needs to be answered by the CFO or the CEO. In fact, some of these regulations stipulate that the CFO or CEO basically confirms in writing that he or she has a proper risk management practice in place, and an audit trail in place. I think it’s a shift away from a pure actuarial focus to a much broader business and proactive risk management perspective.

“Actuaries used to maintain their company’s risk management practices on desktop spreadsheets, and that’s no longer good enough. If you need to provide an audit trail to the regulator and full transparency, you cannot

Insurers increasingly rely on advanced software to comply with rules and regulations.

by Angelo John Lewis
say, ‘Here, we’ve got a spreadsheet that is stored on a file server but we do not really have access control and we do not really know who’s modifying the spreadsheets.’ And even if you stick with spreadsheets, you would have to have a much more rigorous approach by using, for instance, spreadsheet control software.”

Different Approaches

Using an enterprise approach—in which information technology resources and data are not siloed in individual departments but shared across an entire organization—is helping insurers cope with a range of compliance challenges. These include work flow and document management, updating pricing and product changes, tracking licensing and certification of brokers and third-party administrators, and uncovering fraud.

Software solutions include full-throated enterprise platforms from vendors like SAP or Oracle; compliance-centric global, risk and compliance (GRC) platforms from vendors such as MetricStream, B Wise and IBM; and a range of applications that focus on specific solutions, such as credentials tracking or document management.

Some platforms focus especially on the front end of regulatory change management by providing insurers with updates on directives in the pipeline.

An example of these front-end solutions includes an online Wolters Kluwer’s tool that combines regulatory intelligence content from the company’s NILS INSource regulatory database with implementation project work flow and audit functionality.

This allows insurers to track regulatory activity impacting anywhere from one to 90 insurance sublines that have been proposed or have taken effect, as well as implementation projects based on market conduct corrective actions that have been issued.

“There’s a very large mass of data that needs to be monitored because many of those changes directly impact compliance. So it’s knowing what’s in the pipeline, when these requirements become effective and how much time is required to get systems up and running,” said Kathy Donovan, senior compliance counsel, Insurance Compliance Solutions at Wolters Kluwer Financial Services.

A parallel tool that focuses on the property/casualty world is the ISO Electronic Rating Service, which when compared to manual processing reduced the cost of processing complex ISO circulars by 38% and cut labor time by three months, according to a study by the Novarica Research Partners Program.

Carriers rely on ISO to help them stay on top of loss cost trends, new product forms and regulatory changes. For compliance purposes, this information is critical because it may include changes in policy language, rules and rates that have been approved by state regulators.

“ISO comes out with 70 or more circulars each week. Simply managing the product compliance issues is a huge challenge for many insurers,” said Karlyn Carnahan, a research director in Celent’s insurance practice.

“Research I’ve conducted has shown that most carriers that handle these types of changes in a manual process take six to nine months or even longer to get a change implemented and it can be quite costly. So if there’s a tight turnaround, it can be difficult for carriers to get these things done in a timely manner.”

Legacy Concerns

Meeting the ramp-up of compliance challenges that has occurred since the recent financial crisis is particularly demanding for insurers that have not replaced their legacy computing systems. The shortcomings of these systems may have been a factor in a rash of multimillion-dollar unclaimed property settlements, in which multiple insurers were either unable to find life insurance beneficiaries or were not proactive in finding them.

“A lot of carriers have very convoluted core-systems environments which were first deployed as many as 50 years ago, around the time when the Beatles first came to America. Because of their age and complexity, it’s very difficult at times for them to be able to proactively figure out what may or may not have happened,” said Robert McIsaac, a principal at Novarica who focuses on business and technology issues in life insurance, annuities

“Actuaries used to maintain their company’s risk management practices on desktop spreadsheets, and that’s no longer good enough.”

—Juergen Weiss, Gartner
and wealth management.

“Carriers that have particular challenges are those with legacy systems,” added Celent’s Carnahan. “They have real challenges because so much of processing is hard-coded in. It's not a configuration environment where you can simply go in and modify a business rule. You have to go in find the actual code, recode it and test it.”

Noted Weiss: “The challenge with mainframe applications is that they have very few integration capabilities. They’re not really scalable. If you build one integration point, it doesn’t mean you will be able to use that integration for other purposes, so you typically build point-to-point connections, and that drives up your cost.”

Although using legacy systems creates difficulties, that’s not the only issue that blocks insurers’ use of technology to address compliance issues, said Chris Joline, a director for PricewaterhouseCoopers’ U.S. financial services advisory.

“One of the things I’ve seen with large organizations is that they use a ‘set-go-ready’ or maybe even a ‘go-set-ready’ approach. They don’t necessarily think about what they’re going to be using the compliance platform for. They buy them and then try to retrofit everything into them. The second challenge is funding. It’s not unusual to have a number of different kinds of compliance initiatives that are lined up to get into the queue and not enough resources to get them done,” said Joline.

Work Flow Issues

While optimal implementation remains a challenge, Joline and his colleagues agreed there’s been significant improvement in carriers’ use of technology to address work flow and document management issues.

“One thing technology is doing is helping work flow management. When an issue is identified and you get an inventory of these issues that you need to deal with in a particular area, it’s easy to understand and monitor where those things are, no matter what the regulation is,” he said.

Mary Jane Wilson-Bilik, a partner at Sutherland Asbill & Brennan who specializes in insurance regulatory and federal securities law, said she’s especially noticed the improvement of work flow in insurers’ handling of variable annuities. “With variable annuity products, insurers are required to apply the premium on the same day it’s received and get the pricing done correctly. I’ve seen companies improve their systems and I haven’t seen many deficiencies on those issues. They used to be fairly common and that’s a result in improvement of work flow.”

In addition to work flow and document management, insurers that use them have seen major improvements in fraud detection technology. Most states require insurers to report fraudulent claims and/or to have fraud detection policies in place.

“Fraud is an area where technology can have significant benefits, whether it’s doing network analysis using sophisticated predictive models or social media analysis. All of this can absolutely be handled with technology,” Carnahan said.

“But overall in the industry, studies that I’ve done have shown that on average only 15% to 20% of carriers are using the most modern technology for handling fraud. My general impression is that many carriers believe their claims adjusters are pretty good at spotting fraud or may have manual processes that work fairly well to identify fraud,” Carnahan said.

Jim Schweitzer, chief operations officer of the National Insurance Crime Bureau, says that members of his organization monitor fraud in a variety of ways.

“Some make use of sophisticated analytics, while others rely very much on old-school ways of doing so. The use of technology varies among our membership,” he said.

Wilson-Bilik believes cyber-security is a compliance area that needs to be better addressed by insurers. The Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act and the Fair Credit Reporting Act are among the federal laws that impose information security requirements on insurers and other financial institutions.

“This is particularly a challenge if insurers are using a third-party administrator, which is one area where I run into the issue,” she said.

“The new business is coming into a third-party administrator and they have to connect the dots between their contracts, their agent force and the TPA. That’s something that’s almost a manual process.

“I’m not sure any insurer data breaches have happened yet, but...attempts to hack amount to thousands a day industry-wide.”

—Mary Jane Wilson-Bilik, Sutherland Asbill & Brennan

“I'm not sure any insurer data breaches have happened yet, but...attempts to hack amount to thousands a day industry-wide.”

—Mary Jane Wilson-Bilik, Sutherland Asbill & Brennan