REGULATORY OUTLOOK FOR THE INSURANCE INDUSTRY

SUMMARY

Internal audit's relationship with insurance and banking regulators was discussed by a panel of regulatory experts at The IIA's 2017 Financial Services Exchange. Insights included what is expected of internal audit by regulators in the challenging areas of cybersecurity, big data, and technology. The annual Exchange hosted by The IIA's Financial Services Audit Center provides members and professionals better understanding of financial services issues.

Technology and cybersecurity are two of the biggest issues challenging internal audit functions in insurance industry organizations. What regulators are looking for from internal auditors in the digital arena was shared recently at The IIA's 2017 Financial Services Exchange, along with insight on the growing coordination between banking and insurance regulators.

Three insurance regulatory experts discussed issues internal audit is dealing with, offered by Barb Bergmeier, a former chief audit executive and current consultant at EY, who says she has seen a lot of changes come into the insurance industry over the last 25 years. Bergmeier outlined the regulatory oversight and higher standards for insurance holding companies brought in under the U.S. Dodd-Frank Wall Street Reform and Consumer Protection Act, and drew advice from panelists regarding working with regulators, overseeing cybersecurity, and embracing new technology.

Cooperation Between Banking and State Insurance Regulators

"A monkey wrench thrown into how insurance is regulated" is the way Adam Hamm describes what happened when Dodd-Frank went into effect, which brought about the Financial Stability Oversight Council (FSOC). Hamm is a former state insurance commissioner and currently a Protiviti managing director. He says at first there was a fundamental disconnect in regulatory approach between the insurance regulators and federal banking regulators. But from 2010 to 2015, state insurance commissioner representatives and federal banking regulators worked out the day-to-day regulation process for state and federal regulators, a very difficult undertaking. "There were a ton of growing pains, at times it got very tense," Hamm says. "But in 2015 we saw a dramatic improvement that continues today."

Dodd-Frank, plus the Gramm-Leach-Bliley Act, provided more explicit lines delineating responsibilities and roles across the financial services regulatory agencies, and "added fuel to the need to more closely coordinate," says Jeffrey Johnston, managing director of financial regulatory affairs for the National Association of Insurance Commissioners (NAIC). The NAIC is a standard-setting body, not a regulatory agency, with committees of state regulators creating model laws taken back to the states for passage.

Johnston says from a national and state perspective, cooperation between state insurance regulators and federal banking regulators — the Federal Reserve, and to a lesser degree the Office of the Comptroller of the Currency (OCC) — has worked well. NAIC leadership has been engaged with leadership at the Federal Reserve Board as well as district bank heads for the last four to five years, including weekly calls. Senior NAIC staff, who are technical experts on things such as insurance products, financial analysis, and financial accounting, provide support behind the scenes, particularly when it comes to continually educating other financial services regulators on the insurance regulatory system and the controls and activities that take place on a weekly basis, Johnston says.

Thomas Hampton, a former District of Columbia insurance and banking commissioner and currently a senior insurance regulatory advisor for the D.C. law firm Dentons US LLP, says from the insurance side, the state insurance commissioner has full authority and that financial regulation is harmonized with relative laws. But on the banking side, examinations and licensing processes are difficult to do because they must always involve the federal government and the FDIC in the whole process, while also keeping tabs on opinions coming down from the OCC, the Federal Reserve, and elsewhere.

"That involvement makes the process a little more difficult for the state banking commissioners. But, out of that dynamic, a lot of positive things have come," Hampton says. For example, individuals selling variable products are required to have both a securities license and an insurance license. When an enforcement action comes down in one area, it is easier to monitor activities under the other license. Also, the bank examination process and the risk-focus process on the insurance side are closely related, reducing some costs in managing the entire procedure.

While overall coordination between banking and state insurance regulators has continued to improve, some challenges exist, including the need for a better exchange of information. "When insurance examiners are conducting onsite exams — doing risk assessments, documenting management systems, internal controls, any detail testing — those work papers as well as the final examination report are being provided to the point of contact at the district bank," says Johnston. "The reverse has not been consistent, meaning the extent of the work being done by bank examiners, including the final Federal Reserve Bank examination report, is not always making its way back to state insurance examiners."

Another challenge is fungibility of capital meaning the minimum amount of capital appropriate to support business operations before any dollars can be withdrawn or given in dividends. Due to the extensive holding company regulations around an insurance company, determining the right Risk-based Capital Ratio percentage that must be maintained by an insurance company is problematic, Johnston says.

Audit Focus

IIA Standard 1220: Due Professional Care

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1220.A1 Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives.
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
- Adequacy and effectiveness of governance, risk management, and control processes.
- Probability of significant errors, fraud, or noncompliance.
- Cost of assurance in relation to potential benefits.

IIA Standard 2120: Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

2120.A1 The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's objectives.
- Reliability and integrity of financial and operation information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

Technology and Cybersecurity Top Insurance Issues

The insurance industry is moving forward with technology, incorporating automation by using chat bots for customer service online, for example, or handling claims payments by submitting photos. The world of internal audit is changing right along with it and must tackle the increased risk that accompanies these evolutions. "Obviously as you collect more information and store it electronically, you increase cybersecurity risks," Bergmeier says. "How do insurance regulators examine automated processes and data stored electronically?"

NAIC uses National Institute of Standards and Technology (NIST) guidelines as a basis for what they include in examiners handbooks. Guidance for examiners and internal auditors regarding cybersecurity and big data begins with knowing what personally identifiable information exists in an insurance company, along with the databases and systems.

An NAIC data working group launched last year is looking into so-called black boxes (proprietary software) used by insurance companies, the variety of data insurance companies are using in their rating processes, the algorithms used to create rating models, and asking the questions necessary to secure an understanding of what is taking place. Further, to avert any concerns about non-regulatory staff evaluating models, the NAIC created the Innovation and Technology Task Force, made up of 15 commissioners who sit down with the insurance industry to review how technology advances impact existing state insurance laws and regulations. A cyber model is planned for introduction to the states soon.

Three Cybersecurity Steps to Take

What do regulators want from internal audit when it comes to cybersecurity? Using the NIST framework and lessons learned from a few bad breaches in the insurance industry, Hamm says regulators concentrate on five areas: identify, protect, detect, respond, and recover.

- **Identify:** Companies must do the hard work to identify their "crown jewels," the critical assets in terms of business data and the data they hold for customers. What are the absolute data that cannot be taken in the event of a breach and what is being done about that? For example, regulators learned a lot recently from an event where segmentation was an issue. A breach launched via a phishing email on one computer provided access to the records of 80 million Americans because the company in no way shape or form segmented its data, Hamm says.

- **Protect**: Companies have a responsibility to develop and implement appropriate safeguards to limit or contain the impact of a potential cybersecurity event. Some examples provided by Hamm included Access Control, Awareness and Training, and Data Security and Information Protection.

- **Detect**: Regulators want to know what systems are in place to detect in as real time as possible when a breach is occurring. What metrics are available to show regulators internal audit is working on these issues and bringing timeframes down? A company can spend tens of millions of dollars on cybersecurity and have a very sophisticated team and yet not detect a breach for 11 months if insufficient resources are spent on detection.

- **Respond**: Companies promote their incident response plans but often response and recovery is not nearly as effective as what they said it would be. Regulators want to not only see the incident response plan, but also want to know when it was first developed and every iteration after that. Revised plans must be based on exercises, table tops, and activities held to actually try and break the plan to discover the holes in it. Regulators want proof that flaws have been addressed in further

Rating Models and Data Disclosure

One major concern for the insurance industry regarding big data is the many sources and types of data — genetic, social, medical, etc. — that can be used to create rating models. Applicants for insurance don't always know what data the insurance company is using to set its rates and make decisions on whether to provide or cut coverage. So data disclosure by insurance companies may be coming in the next few years.

iterations of the plan. Keep the incident response plan current with regular reviews and testing.

- **Recover:** Companies' response plans must address how capabilities and services will be restored after a cybersecurity event. Timely restoration is expected to occur to minimize the impacts to consumers and the financial results of the company. Recovery plans should address how communications will occur.

"Regulators want proof of what companies are doing to identify, protect against, detect, respond to, and recover from cybersecurity events. If you can do those things, you'll be in a good spot when regulators examine your company for compliance with cyber regulations," Hamm says.

New Laws and Regulations

The NAIC insurance regulatory structure is unique to the United States and has been very effective in providing uniformity and consistency in insurance regulation, even though they are not a regulatory body and do not enact laws. Model laws created by the NAIC in most cases become law in the 50 states, the District of Columbia, and five U.S. territories represented.

Hamm says he has been questioned by insurance regulators from other countries who wonder how state commissioners are able to enforce standards over different jurisdictions. "I always tell them the secret sauce is the accreditation committee," Hamm says. "When a model law or regulation from the NAIC has been blessed by the accreditation committee it is typically adopted by a state legislature or governing body. Why? Because no state can risk losing its accreditation."

If a state loses its accreditation because they fail to enact or adopt a model law, other states, D.C., and U.S. territories may not rely on financial examinations being performed on that particular state's domestic insurance companies. For example, if the Illinois Insurance Department lost its accreditation from the NAIC, all the large insurance companies domesticated in Illinois would be subject to financial examinations from not only Illinois but from virtually every other state in the country. If a big company is subject to financial exams from multiple states as opposed to just Illinois, a company may decide to re-domesticate to a state that is accredited. The economic impact of losing domestic insurers is incentive enough for governors, insurance commissioners, and legislatures to never risk losing their accreditation.

While the accreditation committee has harmonized financial regulation, they have not been as successful with developing consistent processes for market conduct examinations and product review and rate filings. At the state level, legislators will often make nuanced changes to proposed laws to show they are responding to constituent complaints, Hampton says. This occurs particularly if the commissioner of that state is elected versus appointed.

Audit Focus

IIA Standard 2130: Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's, governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

IIA Standard 2210: Engagement Objectives

Objectives must be established for each engagement.

2210.A2 Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

Bergmeier has experienced firsthand the impact of different expectations from banking and insurance regulators on internal audit functions. Historically, the regulators have conducted their examinations independently with no reliance on each other, increasing costs and compliance burdens for companies. But she says collaboration is increasing and expectations are becoming more consistent. "I'm very optimistic about the coordination of bank and insurance regulatory efforts going forward," she says.

About the Financial Services Audit Center

Established in 2015, the Financial Services Audit Center (the Center) is a specialty offering of The IIA for financial services auditors. The Center was established to provide financial services auditors with low-cost, high-quality professional development; networking opportunities for knowledge sharing among financial services stakeholders; and ongoing, timely, and relevant reporting on trends, benchmarking, and thought leadership in the audit profession.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla. For more information, visit www.theiia.org.

Disclaimer

Copyright

Financial Services
AUDIT CENTER

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746-5402, USA

Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org/FSAC