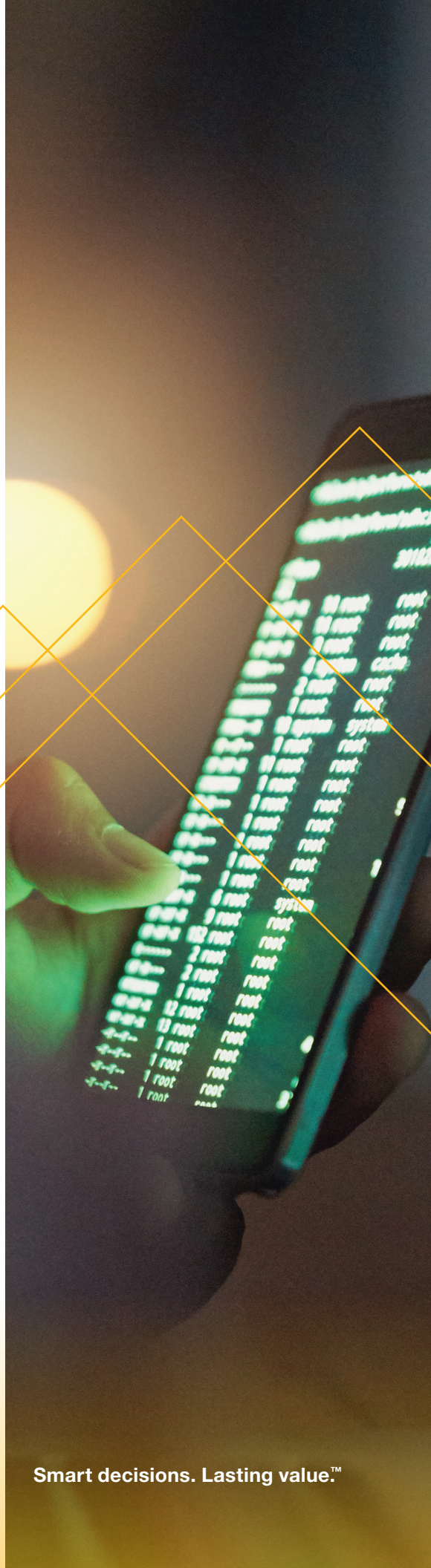
Crowe

Checklist

7 Steps You Need to Take Now

Assessing Your NAIC Cybersecurity Program Compliance Readiness



Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.℠

The National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (Model Law), passed in October 2017, establishes standards for data security that insurers will need to adhere to, as well as standards for investigation and notification of a cybersecurity event.

Because individual states most likely will adopt the Model Law with minimal modifications, insurers can begin the compliance process without waiting for guidance from the states where they do business.

The challenge will be to strike the right balance between doing too much and not doing enough to establish and maintain a cybersecurity program. The Model Law is prescriptive rather than descriptive. That means individual insurers may determine a compliance approach commensurate with their risk tolerance, the size and complexity of their organization (including their use of third-party service providers), and the sensitivity of information they control or possess.

There is no one-size-fits-all approach to Model Law compliance. Instead, it is up to each insurer to assess its current cybersecurity effort, identify gaps between it and the requirements of the Model Law, and create a sustainable program that aligns with the insurer's risk tolerance and assessment.

Following are seven steps insurance companies can take to help maximize Model Law readiness.

✓ Assess Current Compliance Readiness and Maturity.

While full compliance with the Model Law is the objective, most insurers will want to be strategic in how they roll out cybersecurity programs and allocate resources without overinvesting in compliance. Some insurers will enter the process with sophisticated policies in place, while others will need to earmark more time and resources to meet the requirements.

Assessing current compliance readiness and maturity will help insurers identify areas that already conform to the standard and those that fall short, and then invest strategically in closing the gaps.

Crowe has several tools and processes to assess an insurer's current state and determine if its cybersecurity program complies with NAIC Model Law standards. In addition to performing a high-level, two-day health check and developing a road map, Crowe can provide a technology infrastructure evaluation designed to identify gaps in networks and servers. After the gap analysis, Crowe will recommend how the insurer can modify existing technology or acquire new solutions.

✓ Conduct a Risk Assessment.

Each insurer is required to conduct a risk assessment as the basis for its written information security program. The Model Law states that the assessment should include:

- Recognition of sensitive and confidential assets
- Reasonable foreseeable internal or external threats
- The potential damage of threats
- Assessment of the effectiveness of mitigating controls

The Model Law covers a wide variety of cybersecurity risks, but not all risks are equal. An insurer's business model, technology infrastructure, and operating environment affect the level of risk. Crowe works with insurers to create an individualized risk assessment that identifies specific at-risk areas that require greater protection. For example, an insurer's internet-based applications might be more at risk than its legacy applications.

It is nearly impossible to address every cybersecurity risk, so insurers should prioritize attention based on their particular vulnerabilities. The goal of the risk assessment is to align an insurer's compliance program with its risk profile.

✓ Assess Incident Monitoring, Logging, and Response Plans.

The Model Law states that insurers must include the policies and procedures for detecting, preventing, and responding to attacks, intrusions, or other system failures in their plan. The written plan also should identify clear roles, responsibilities, and levels of decision-making authority for stakeholders.

The Model Law allows a third-party service provider to create, maintain, and execute the incident monitoring, logging, and response plan. Crowe managed security services can support these needs.

✓ Develop a Third-Party Provider Management Program.

The Model Law makes very little, if any, distinction between an incident resulting from an oversight of the insurer or an incident caused by one of its third-party service providers. Insurers must take responsibility and treat any cybersecurity event as if it is internal. The insurer is liable for any attacks and must inform the state insurance commissioner for which the entity is a licensee under that state law of breaches immediately, then update and supplement notifications concerning the event.

In turn, this requires that insurers verify that their third parties that manage sensitive and confidential information also adopt measurable cybersecurity programs. Crowe third-party risk management services help companies risk assess and align third-party cybersecurity programs.

✓ Identify Internal and External Resources to Plan, Implement, and Manage the Program.

The Model Law states that insurers must designate one or more employee(s), an affiliate, or an outside vendor to act on behalf of the insurer that is responsible for the information security program, including assessment, validation, and reporting. At the largest insurers, the task typically falls to a C-level executive, such as the chief information security officer (CISO), chief risk officer (CRO), chief information officer (CIO), or chief financial officer (CFO).

Midsize and smaller insurers typically do not have the staffing resources to manage a compliant cybersecurity program in-house. While insurers cannot outsource compliance liability for a cybersecurity event, insurers can receive external assistance and advisory for cybersecurity program development, implementation, and execution. Because the Model Law allows an insurer to designate a third party, insurers increasingly are looking to engage a virtual information security office (vISO) assistant.

✓ Develop a Strategic Governance Model.

The Model Law requires that insurers include the governance of the cybersecurity program as part of the overall enterprise risk management program. On a long-term basis that extends beyond minimal Model Law compliance, insurers should strive to develop a program that is sustainable, scalable, and efficient.

Leaders providing strategic governance of the cybersecurity program must allocate responsibility across the business and incorporate a written plan with policies and procedures, including notification requirements to the state insurance commissioner.

✓ Verify Participants Understand Their Roles.

Cybersecurity involves all levels of the organization, from hourly and contract employees to the board; from IT to operations; from facilities to the lines of business. A representative of the board of directors and senior management must provide written attestation on adherence to the Model Law.

To establish that the insurer is up to speed on Model Law compliance, Crowe offers board, executive, and employee training and coaching on roles, responsibilities, and best practices for those in oversight positions.

Conclusion

Crowe can help insurers comply with the Model Law. Our services include assessing an insurer's current state and developing a road map that aligns with their business model, resources, and desired future state.

Once the information security program is implemented, Crowe can assist with:

- Preventive controls
- Incident detection, response, and recovery
- Training and culture
- Information security governance
- Reporting
- Program assessments
- Cybersecurity strategy and program guidance
- Amending service level agreements (SLAs) and contracts with third parties to mitigate noncompliance risk

Learn More

For more information on NAIC Insurance Data Security Model Law offerings from Crowe, contact:

Glenn Saslow, Partner
+1 860 470 2103
glenn.saslow@crowe.com

Troy La Huis, Principal
+1 616 233 5571
troy.lahuis@crowe.com

crowe.com

FS-18700-008C