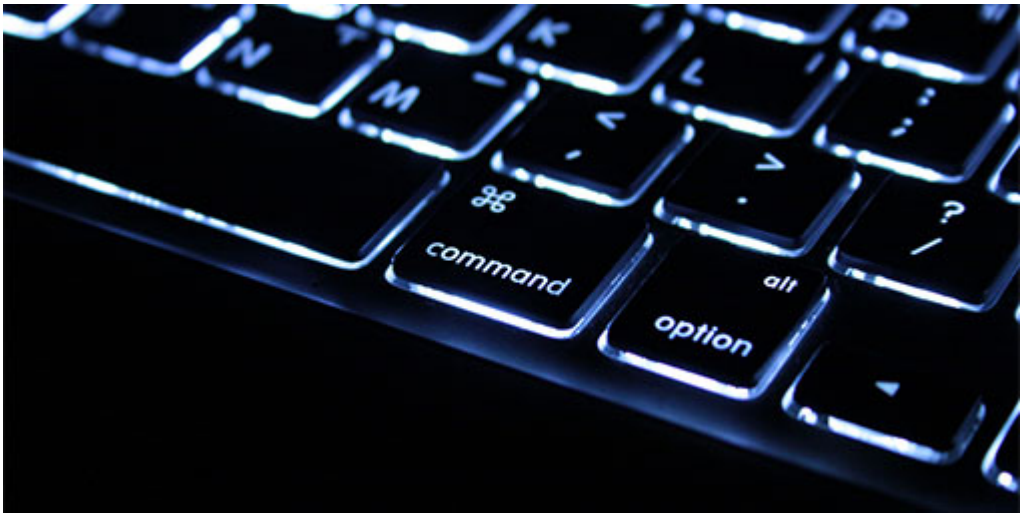
CARLTON FIELDS

What the Recent NAIC Financial Condition Examiners Handbook Changes Mean for Insurers

October 27, 2015

Co-Authored by Gary Slinger, Manager of IS Process & Security



On September 21, 2015, the National Association of Insurance Commissioners (NAIC) IT Examination Working Group adopted amendments to the IT section of the Financial Condition Examiners Handbook ("the Handbook"). The changes are intended to strengthen and enhance the existing cybersecurity guidance, and are consistent with guidelines published by the National Institute of Standards & Technology (NIST) in its cybersecurity framework. Suggestions and recommendations by various state regulatory authorities and other interested parties were also incorporated where appropriate. This article supplies publically-available NAIC website links to the updated amendments. **The Changes and Their Impact on Insurers**

While changes were made to several sections, the following should be of immediate interest: General Examination Considerations, the IT Planning Questionnaire, and the Table for the Evaluation of Controls ("the Table"). **General Examination Considerations**

The General Examination Considerations now include a "Cybersecurity Considerations" section. In short, it says the examiner can consider an insurer's existing risk mitigation strategies and controls, regardless of the underlying system or standard they are based on, and gives the examiner leeway to

consider third-party assessments, testing, etc., as suitable for its own use. This update also details four areas that insurers must specifically consider and address with the right tools, policies, and processes:

- Identification: Establish appropriate risk assessment and risk management processes.
- Prevention: Establish and properly communicate policies and controls.
- Detection: Use anti-virus and anti-malware, intrusion detection and intrusion prevention systems; At all times, watch the data that enters and leaves your networks, and network activity.
- Response and Recovery: Because prevention and detection controls can—and do— fail, you must establish appropriate and tested incident response and disaster recovery plans, as well as broader business continuity plans.

IT Planning Questionnaire

Section 6, "Information Technology Security—Incident Response" to the IT Planning Questionnaire adds high-level statements that specify, in business language, what the examiner will request. These items, which are required, can be part of a larger framework (e.g. ISO 27001 or the NIST Cybersecurity Framework), or can be created specifically to comply with Section 6. **Table for the Evaluation of Controls**

The Table shows the common controls and test procedures the examiner may use. It seeks to ensure that management and employees understand the established policies, and that there is appropriate security awareness throughout the organization. Before an examination begins, familiarize employees with the examination process and information they may be asked to produce. Examiners commonly interview staff and management, so they must be prepared. For sample questions review the Table's Risk Statement "DSS 02" of *Exhibit C – Part Two Work Program.* Note the language and tests regarding incident response plans, and consider whether you have the documented, consistent processes the Handbook requests. Review the indicated checklist edits. Examiners will likely focus on these elements in the immediate future. **Takeaways and Immediate Steps**

- Review the changes in the Table and ensure you can meet the needs indicated under "Possible Test Procedures" and "Preliminary Information Request."
- Conduct a risk assessment of your environment and ensure you establish a program of identification, prevention, detection, and response and recovery that addresses your risk assessment findings.
- Ensure that your current security awareness program is properly implemented and that communication throughout your organization addresses the Handbook's security requirements.
- Seek assistance in developing policies and procedures, or reviewing existing ones, as necessary.

Related Practices

Cybersecurity and Privacy
Life, Annuity, and Retirement Litigation