NAIC National Association of Insurance Commissioners

IT EXAMINATION (E) WORKING GROUP
Conference Call
Thursday, October 29, 2020
3:00 p.m. ET / 2:00 p.m. CT / 1:00 p.m. MT / 12:00 a.m. PT

ROLL CALL

Jerry Ehlers, Chair	Indiana	Kim Dobbs/Cynthia Amann	Missouri
Ber Vang, Vice-Chair	California	Justin Schrader	Nebraska
Blasé Abreo	Alabama	Eileen Fox	New York
Mel Anderson	Arkansas	Metty Nyangoro	Ohio
Ken Roulier/Bill Arfanis	Connecticut	Eli Snowbarger	Oklahoma
Ginny Godek	Illinois	Melissa Greiner	Pennsylvania
Shane Mead	Kansas	Dave Jensen	Wisconsin
Dmitriy Valekha	Maryland		
NAIC Staff Support: Jacob Steilen			

AGENDA

1. Receive an update on Working Group Projects

    - Adopt Minutes — Attachment 1
    - Adopt ITPQ revisions — Attachment 2
    - Approve Exhibit C mapping document — Excel Document

2. Discuss future projects for the group

3. Other Matters

4. Adjournment

Attachment One

Meeting Minutes

Draft: 9/30/20

Information Technology (IT) Examination (E) Working Group
Conference Call
September 17, 2020

The IT Examination (E) Working Group of the Examination Oversight (E) Task Force met via conference call Sept. 17, 2020. The following Working Group members participated: Jerry Ehlers, Chair (IN); Ber Vang, Vice Chair (CA); Blase Abreo (AL); Mel Anderson (AR); William Arfanis and Ken Roulier (CT); Ginny Godek (IL); Dmitriy Valekha (MD); Kim Dobbs and Cynthia Amann (MO); Justin Schrader (NE), Eileen Fox (NY); Metty Nyangoro (OH), Eli Snowbarger (OK); Melissa Greiner (PA); and Dave Jensen (WI).

1. Adopted its March 12 Minutes

The Working Group met March 12. Mr. Vang made a motion, seconded by Mr. Roulier, to adopt the Working Group's March 12 minutes. The motion passed unanimously.

2. Exposed Revisions to the ITPQ Section of Exhibit C Within the *Financial Condition Examiners Handbook* (Handbook)

Mr. Ehlers explained that the proposed revision to the Information Technology Planning Questionnaire (ITPQ) adds "cyber self-assessment tools" to the list of items requested at the beginning of an IT examination. He expressed that the goal of this revision is to help IT examiners obtain and better utilize third-party work to complete their IT examinations more efficiently. The Working Group agreed to expose the proposed addition for a 30-day public comment period ending Oct. 17.

3. Exposed Market Conduct Mapping and Expanded Model Law Mapping

Mr. Ehlers recalled the Working Group's discussion of the 2020 project list from the Working Group's previous conference call on March 12. In that discussion, the Working Group agreed to continue work on its Exhibit C mapping project, which included mapping Exhibit C to a document from the M*arket Regulation Handbook* entitled, "Insurance Data Security Pre-Breach and Post-Breach Checklists" and expanding a previously completed mapping document, which mapped Exhibit C procedures to the *Insurance Data Security Model Law* (#668). The Working Group previously mapped Section D of the model law to Exhibit C procedures; the updated mapping has been expanded to now include Sections E and F of the model law.

Mr. Ehlers said the mapping document will serve as an optional tool, available through the Working Group's NAIC webpage, that an IT examiner could utilize in conducting IT examinations.

Jacob Steilen (NAIC) provided an overview of the Exhibit C mapping document. He explained that the native format of the mapping document would be a multi-tabbed Microsoft Excel spreadsheet. He stated that the advantages of this format include: 1) hosting multiple mapping spreadsheets in a single document, which reduces the amount of documents an IT examiner has to download and organize; and 2) additional mappings that the Working Group might decide to pursue in the future.

Mr. Steilen said the "Market Conduct Breach Checklist" tab of the document maps Exhibit C to the "Insurance Data Security Pre-Breach and Post-Breach Checklists." He said this tab includes instructions explaining how the mapping is to be used and describes the normal roles and responsibilities of Market Conduct examiners. He said the "Data Security Model Law" tab includes the mapping of Sections D, E, and F of Model #668 to Exhibit C procedures. The Working Group agreed to expose the mapping document for a 30-day public comment period ending Oct. 17.

Tom Finnell (Finnell and Co. LLC) asked what would happen if this document were to be adopted after the 30-day public comment period. Mr. Steilen said if adopted, the document would be made available for download on the Working Group's webpage. He said if the Working Group desires to expand the mappings available in the document, it could consider that at a future time.

Having no further business, the IT Examination (E) Working Group adjourned.

Attachment Two

Exhibit C - ITPQ

PART ONE – INFORMATION TECHNOLOGY PLANNING QUESTIONNAIRE (ITPQ)

For the questions below, provide the requested documentation and the name, title, telephone number and e-mail address of the individual who will be most able to discuss and clarify the information presented.

If a particular section does not apply to your company, give a brief explanation of why it does not apply. All responses should be in the form of a separate summary memorandum, headed with the corresponding section label. Where possible, electronic responses are preferred.

1. Use of Information Technology

If the company does not process its business electronically, provide a narrative description explaining how the company's business is processed. The remainder of this section does not need to be completed.

If the company only processes business electronically on a stand-alone personal computer and does not use networking technology, provide a narrative description explaining how business is processed, including the type of application software being used. The remainder of this section does not need to be completed.

2. Information Technology Governance

a. Provide the name, telephone number and e-mail address of the chief information officer (or equivalent).

b. Provide specific detailed organizational charts for the company's IT department, and/or any affiliates providing IT services, that show its various functional divisions (i.e., operations, programming, support services, etc.). Show reporting relationships of the IT department within the organization.

c. Provide an executive overview of your company's IT strategic plans, including plans for e-commerce.

d. Provide an executive overview of your IT steering committee, or other group that establishes and directs IT policies and strategies, indicating the membership of the group and the frequency of their meetings.

e. Provide an overview of ERM program, if not already provided, and associated touchpoints in relation to IT risks.

f. Describe the frequency, type, and content of interaction with the company's board of directors regarding key IT risks, such as cybersecurity.

3. Information Technology Infrastructure

a. Provide the name, telephone number and e-mail address of the chief technology officer (or equivalent).

b. Provide a listing of the locations of all data-processing centers used by your company, whether owned by the company or by a third-party administrator that processes data for the company.

c. Provide a system-wide map or topography, showing all hardware platforms and network connections, indicating all internal and external access points. In addition, complete a separate Systems Summary Grid for each platform (see Attachment 1). A sample Systems Summary Grid is provided with this questionnaire (see Attachment 2).

d. Provide a narrative explanation of the application-level interfaces (manual and automated) among the various programs/platforms (e.g., claims system feeds into the accounting system).

e. Provide a list of any business or data-processing services provided by the company to any other entities, including affiliates, indicating the type of service provided and a summary of the terms of the agreements (e.g., named parties, effective date, period and services covered). Also indicate if a service level agreement (SLA) exists for each of these services.

f. Provide a list of any business or data-processing services performed by any other entities on behalf of the company, such as a third-party administrator (TPA, MGA, GA, etc.) or an affiliate, indicating the type of service provided and a summary of the terms of the agreements (e.g., named parties, effective date, period, location and services covered). Also indicate if a SLA exists for each of these services.

g. Describe any business the company is conducting through electronic channels, indicating the type and volume of business and the date when it was implemented. **Note:** E-commerce methods of transmission might include voice recognition units (VRUs), the Internet, third-party extranets, and wireless and broadband communications media.

4. Information Technology Audits, Reviews and Risk Assessments

a. Provide the name, telephone number and e-mail address for the partner of your company's independent external audit team and the internal audit director (or equivalent), if they exist.

b. Provide a list of any IT audits/reviews performed within the past two years, including e-commerce areas, cybersecurity assessments and any IT related reviews of financial significant 3rd party vendors Include the dates, review subjects and who performed the audits/reviews (e.g., internal audit, external audit, SOC 1 Type II Reports, SOC for Cybersecurity reports, cyber self-assessment tools, Sarbanes-Oxley, state insurance departments, governmental agencies, and/or any other contractor or affiliate that might have performed an audit/review).

c. Arrange for a copy of the IT work included in the most recent audit workpapers to be provided from the company's external audit firm. The workpapers should be provided no later than the response date identified for the IT Planning Questionnaire.

d. Please provide all current assessments of the company's IT risks, whether internally or externally conducted.

5. Information Technology Security

a. Provide the name, telephone number and e-mail address for the chief security officer (or equivalent).

b. Provide a copy of all IT security related policies.

If not explicitly described in the policies or if formal, written policies exists, please provide a detailed description of:

- Data Confidentiality – Discuss how data elements are classified and who determines which individuals/roles have access to data elements.
- Data Encryption – Discuss if confidential data is encrypted both at rest and in transit, including the process and methods of encryption.
- System and Network Access Controls – Discuss how access is controlled (network-level, server-level, application-level, or a combination), which directory services are used for network access, whether authentication servers are used, etc.
- Multi-Factor Authentication – Discuss the current use of multi-factor authentication including where it's used, the type being used, and any plans for expanding its' usage.
- Anti-virus/Anti-malware – Discuss the anti-virus/anti-malware software, and patch management program in place including the systems used and the strategy for keeping these products current.
- Security Logging & Monitoring – Discuss the process and tools used for logging and monitoring security events across network devices, servers, endpoints, systems and applications. Also discuss how the company aggregates and correlates this information across the breadth of monitoring points.
- Intrusion Detection & Prevention – Discuss the program in place to detect and prevent intrusion into the company's network and systems including the types of tools and technology being used.
- Vulnerability Management – Discuss the company's vulnerability management program including the scope of coverage, tools and techniques, frequency of scanning, reporting of known vulnerabilities, remediation, etc
- Penetration Testing – Discuss the types and frequency of penetration testing and whether it's conducted by internal employees or external firms. Also discuss whether the company uses advanced techniques such as red and blue team exercises.