



INFORMATION TECHNOLOGY (IT) EXAMINATION (E) WORKING GROUP
Conference Call

Monday, April 19, 2021

12:00 p.m. ET / 11:00 a.m. CT / 10:00 a.m. MT / 9:00 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/Matt Milford	Pennsylvania
Shane Mead	Kansas	Dave Jensen	Wisconsin
Dmitriy Valekha	Maryland		
NAIC Staff Support: Jacob Steilen			

AGENDA

1. Receive an update on Working Group Projects & Referrals
 - Discuss referrals received
 - Referral from Receivership Financial Analysis Working Group Attachment 1
 - Referral from Chief Financial Regulator Forum Attachment 2
2. Discuss priorities & action steps
3. Other Matters
4. Adjournment

Attachment One

RFAWG Referral



To: Jerry Ehlers (IN), Chair of Information Technology (IT) Examination (E) Working Group (ITEWG)

From: Toma Wilkerson (FL) and Donna Wilson (OK), Co-Chairs of the Receivership Financial Analysis (E) Working Group (RFAWG)

Date: March 22, 2021

RE: Data Transfer Guidance in the IT Work Program of the *Financial Condition Examiners Handbook*

The RFAWG has discussed concerns noted in recent receiverships of insurance companies whereby receivers and guaranty funds continue to face challenges, including technical challenges, related to the timely and efficient transfer of data (e.g., claims data and policyholder records) from the insurance company in receivership to the receiver and/or guaranty funds. This generally occurs when data is not stored in a usable format or data is stored in information technology (IT) systems that are not easily extractable or transferable. Challenges with data and records may arise when insolvent insurance companies have used third-party administrator(s) (TPA) or have multiple IT platforms and legacy systems. In the case of a TPA, it is not uncommon for data to be comingled between clients. Understanding an insurance company's IT systems and data in advance of any future insolvency helps to minimize costs and delays in claims payments at the onset of the receivership process.

The RFAWG recognizes that the *Financial Condition Examiners Handbook* contains some existing guidance regarding receivership considerations, including the following language that was added to the Considerations for Potentially Troubled Insurance Companies section of the Handbook in 2019:

If receivership or liquidation is triggered, and assets are transferred to the receiver or guaranty fund to settle obligations, it is important that the company's data be maintained in such a format to ensure that policies can continue to be maintained and claims can continue to be paid. For example, the company should have the ability to export its claims data through a defined format (Uniform Data Standards [UDS]) that would allow the data to be received and utilized by a third-party guaranty fund. Therefore, the examination may include additional procedures as part of the IT review to identify and locate data storage and processes, understand the format of the data, and ensure that proper functionality exists for timely and efficient export of policy and claims data in the event of a receivership.

However, given the continued issues noted in this area, RFAWG feels it would be beneficial for ITEWG to consider additional guidance specific to the IT review conducted during a financial condition examination, including the incorporation of specific procedures into Exhibit C – Evaluation of Controls in Information Technology. This is particularly relevant when insurers are considered by the domestic state insurance regulator to be financially troubled or high priority; however, given that correcting data format and system issues may take time for insurers to resolve, claims data formatting and storage considerations may be relevant for all examinations.

The RFAWG recommends that such guidance address the following:

- Gain and document an understanding of the insurance company's IT systems, data storage, data formats and any legacy systems.
- Based on the appropriate RBC level, review and test whether claims data, reserve information and policyholder records held by the insurer and by any TPAs are capable of being easily and timely accessible and extracted, and if necessary, translated into a format used by receivers and guaranty funds in the event of insolvency.
 - Property and Casualty Guaranty Funds utilize the Uniform Data Standards (UDS) reporting system for the timely and efficient transfer of claims data and policyholder records.

- Life and Health Guaranty Associations do not utilize UDS; however, they require easy and timely advance access to data to establish agreements and infrastructures to either transfer or continue administration of the insolvent company's policyholders.
- Information often needed in receivership includes for example: in force; policyholder information (policy master files), policy values; policy forms; claims files & history; rate files & history; reserves; information by line of business, provider/vendor agreements.
- Encourage mitigation by the insurance company or its TPA of any data or IT system format, storage and transferability issues found during examination.
- Consideration of utilizing receivers and guaranty funds as resources at any point in the data evaluation and mitigation process.

If you have questions, please contact Jane Koenigsman, NAIC Staff, at jkoenigsman@naic.org.

Attachment Two

Chief Regulator Referral

MEMORANDUM

TO: Jerry Ehlers (IN), Chair of the IT Examination (E) Working Group

FROM: Judy Weaver (MI), Facilitator of the Chief Financial Regulator Forum

DATE: March 16, 2021

RE: Referral on Cyber Vulnerability Guidance

On its March 16, 2021 call, the Chief Financial Regulator Forum discussed the recent cyber vulnerabilities and exposures that may have impacted various insurance companies, including the Solar Winds cyberattack and the Microsoft Exchange Server zero-day vulnerabilities. In discussing these potential exposures, financial regulators indicated a need for additional guidance on how to address significant vulnerabilities with the potential to impact domestic insurers in a timely manner as they emerge.

While existing IT Examination guidance in the *Financial Condition Examiners Handbook* includes procedures for evaluating cybersecurity controls in place at an insurer, including patch maintenance and intrusion detection processes, those procedures are typically only conducted during a scheduled full-scope examination. As such, the Chief Financial Regulator community is requesting that the Working Group consider the development of additional guidance and procedures for regulator use in evaluating an insurer's response to significant emerging vulnerabilities and exposures, outside of a full-scope financial examination. Such procedures should be flexible enough to be incorporated into limited scope/interim examination efforts, the ongoing financial analysis process, or even into ad-hoc inquiries/requests for information.

In developing such guidance, the Working Group is encouraged to consider whether it would be more appropriate for such guidance to be included in NAIC handbooks, or as a separate best-practice tool maintained elsewhere. In addition, the Working Group is encouraged to consider coordinating efforts in this area with the Market Conduct Examinations Guidelines (D) Working Group, given its role in maintaining a post-breach checklist and related guidance in the *Market Regulation Handbook*.

If there are any questions regarding the proposed recommendation, please contact either me or NAIC staff (Bruce Jenson at bjenson@naic.org) for clarification.

Thank you for your consideration of this referral.