INFORMATION TECHNOLOGY (IT) EXAMINATION (E) WORKING GROUP
Conference Call
Wednesday, October 13, 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	Eleanor Lu	Wisconsin
Dmitriy Valekha	Maryland		
NAIC Staff Support: Jacob Steilen			

AGENDA

1) Receive an update on Drafting Group activities to address referrals
    a) Update on Chief Financial Regulator Forum referral   Attachment 1
    b) Update on RFAWG referral   Attachment 2

2) Discuss updates on ransomware   Attachment 3

3) Other Matters

4) Adjournment

Attachment One

Chief Financial 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.

EXECUTIVE OFFICE • 444 North Capitol Street NW, Suite 700 • Washington, DC 20001-1509   p | 202 471 3990   f | 816 460 7493
CENTRAL OFFICE • 1100 Walnut Street, Suite 1500 • Kansas City, MO 64106-2197   p | 816 842 3600   f | 816 783 8175
CAPITAL MARKETS & INVESTMENT ANALYSIS OFFICE • One New York Plaza, Suite 4210 • New York, NY 10004   p | 212 398 9000   f | 212 382 4207

www.naic.org
© 2021 National Association of Insurance Commissioners

Cyber Vulnerability Response Plan

OVERVIEW

Cyber vulnerabilities have become increasingly prevalent and significant as cyber criminals seek to exploit vulnerabilities to breach a company's IT security defenses. Conducting a preliminary investigation of possible exposure to these vulnerabilities as they arise can help financial regulators evaluate the operational resiliency of their groups/domestic insurance companies and determine whether a cyber event has occurred that would require further investigation.

However, it is important to note that reported vulnerabilities do not necessarily indicate a cyber breach that would trigger formal notifications and consumer protection requirements, as companies should be addressing vulnerabilities before they can be exploited. As such, many states assign the responsibility for investigation of significant reported vulnerabilities to financial regulators either as a follow-up to ongoing financial exam work in assessing and monitoring IT security controls or as part of an ad-hoc financial analysis inquiry where appropriate. Recent examples of such vulnerabilities include the Microsoft Exchange server weaknesses, SolarWinds remote code execution vulnerability, and Qualys cloud storage vulnerability. Vulnerabilities include threats to the company's internal systems as well as breaches at third parties which host, or have easy access to, company confidential data.

The primary purpose of this document is to guide examiners and/or analysts through the ad-hoc inquiry that may be necessary when a cyber exposure or vulnerability has been identified or alleged in the period between full-scope examinations.

The results of the ad-hoc inquiry may warrant additional investigation to follow up on concerns related to IT controls, which could include calling a targeted examination, performing interim work, and/or follow-up on recommendations by the department analyst. If additional investigation is warranted, examiners should consult Exhibit C – IT Work Program in the Financial Condition Examiners Handbook to identify relevant procedures. If, after investigating potential vulnerabilities, the domestic/Lead State determines that a cyber breach has occurred, information on the breach should be promptly shared with market conduct regulators and other impacted states in accordance with existing regulatory guidance. Guidance in the _Market Regulation Handbook_ can then be utilized in situations where a breach has occurred, specifically the post-breach checklist in Addendum A to Operations/Management Standard 17 Chapter 20 – General Examination Standards.

Terms & Definitions

- **Vulnerability** - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

- **Incident** - An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- **Breach** - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose.

*Definitions provided by the NIST glossary linked here. *(NIST SP 800-53 rev. 5, page 421)*

ACTION ITEMS FOR REGULATORS AFTER A VULNERABILITY HAS BEEN IDENTIFIED

The following section provides common questions and answers to help regulators determine an appropriate course of action in responding to identification of an emerging vulnerability.

1. **Which insurers should regulators contact regarding an identified vulnerability**?
   Professional judgement should be used by the department in determining which insurers to contact based on the size and severity of the vulnerability identified.

2. **Which state(s) should lead the effort of responding to notification of an emerging vulnerability?**
   In recognition of the Lead State approach to financial regulation and deference to a domestic regulator, as well as to reduce the number of overlapping requests and to create efficiencies for both insurers and regulators, the Lead State (for groups) and/or domestic regulator should lead the effort of investigating significant vulnerabilities.

3. **What area of the department should take responsibility for investigating cyber vulnerabilities and breaches?**
   While it is up to each department to determine which area should take responsibility for investigating vulnerabilities, which could be impacted by subject matter expertise and availability, the NAIC has primarily classified follow-up procedures for known breaches as a market regulation activity and has included such procedures in the Market Regulation Handbook. This is primarily due to the importance of ensuring adequate consumer protection post breach. However, given that a breach can also affect an insurer's solvency position, coordination with financial regulators in post-breach follow-up activities is encouraged.

   Investigations related to significant vulnerabilities are typically viewed as following up on financial exam work to assess IT security controls. As such, it is recommended that financial regulators take the lead in addressing significant identified vulnerabilities.

However, given the potential for a vulnerability exposure to turn into a breach, early coordination with market regulation is encouraged.

4. **Does the adoption status of the** [**NAIC's Insurance Data Security Model Law**](#) **(or other relevant state law) affect a state's response**?
As this guidance focuses primarily on addressing an identified vulnerability, as opposed to an incident or breach, it is not clear whether information on the vulnerability and how it has been addressed would be reported to the department unless or until an actual incident or breach has occurred. As a result, it may be appropriate to proactively address an identified vulnerability even if your department has reporting requirements already in place. Proactive investigation of identified vulnerabilities with insurers may help prevent breaches from occurring that the department would otherwise have to address down the line. However, before taking steps to address an identified vulnerability, the regulator should ensure that the department has not yet received a notice from the insurer on this exposure.

5. **If the investigation of cyber vulnerabilities identifies a need to take additional steps in addressing IT control processes, how can this work be performed so that it can be utilized on the next full scope exam?**
The most effective way to conduct this investigation in a manner that would allow the results to be integrated into an upcoming full-scope exam would be to utilize the interim work concept as defined by the *Financial Condition Examiners Handbook* (see Section 1-1, part I). Interim work is intended to provide examiners the opportunity to conduct exam procedures in areas that are considered inherently risky but are not known to present an immediate concern. A separate examination report is not required in the interim period as information deemed appropriate for report purposes will be included within the full-scope examination report. However, results of interim work are expected to be documented in Exhibit AA—Summary Review Memorandum.

Example Scenario:
Let's assume a software vulnerability was identified and the team wants to check the insurer's patch management protocols. To investigate the vulnerability, the team performs interim work and learns that the company has an updated patch negating the vulnerability. Additionally, the team selects a sample of insurer servers to verify they are at the right version/patch level. The team concludes that the insurer as taken appropriate steps to mitigate concerns related to this vulnerability.

At the time of the full-scope exam, this work could be used to help address the DSS 05.01 procedure on Exhibit C. However, before leveraging interim work, the exam team should perform roll-forward procedures to determine whether the processes tested in the interim period are still in place and substantially the same, as changes may impact the

conclusions that were reached in the interim period. For additional guidance about rolling forward interim work procedures for use in the full-scope exam, see Section 1-1 in the *Financial Condition Examiners Handbook*.

POSSIBLE QUESTIONS IN DETERMINING AN INSURER'S EXPOSURE TO A KNOWN VULNERABILITY

The following questions can be used to help a regulator determine an insurer's exposure to a known vulnerability, as well as any steps taken to mitigate and address the vulnerability (if exposed). These questions should be customized to the specific situation identified. As the topics addressed and questions raised are largely in-line with topics covered during an examination IT review, regulators are encouraged to work with their IT specialists, if necessary, to customize the inquiries, evaluate the appropriateness of responses received and determine if any additional follow-up is necessary. If specialist resources are not available to a state in this area, NAIC IT security staff may be available to assist in this regard. Where appropriate, corresponding topics from Exhibit C – Evaluation of Controls in Information Technology from the *Financial Condition Examiners Handbook* have been included to assist in evaluating an insurer's response to a specific question.

1. Does the insurance company have any exposure to the discovered vulnerability?

2. If applicable, has the insurance company deployed updates to affected [*application*] servers?
    a. What are the insurance company's patch management protocols?
    b. Was the recommended patch applied?
    c. What steps were taken between when the vulnerability was discovered and when the patch was applied to mitigate the risk?
    d. If the insurance company has not been able to patch, have they followed [*application vendor/developer*] instructions for how to mitigate through reconfiguration?
        See Exhibit C ITPQ question #5
    e. Has the insurance company taken steps to investigate their systems and logs for exploitation, persistence, or evidence of lateral movement? If so, has the insurance company remediated any identified exploitation or persistence and investigated their environment for indications of lateral movement?
        See Exhibit C DSS 05.07

3. For vulnerabilities derived from breaches at insurer third parties:
    a. Was company data exposed, or does the 3rd party have easy access to your data?
    b. Has access been restricted?
    c. What steps have been taken to mitigate the risk that your data was exposed?
    d. What communication has taken place?
    e. Has the insurance company addressed this issue with their third-party service providers, if applicable?
        See Exhibit C ITPQ Question #3

Conclusions & Next Steps

Conclusions Reached			
No breach or control issues discovered. Mitigating factors were strong and/or further procedures proved there was no additional material risk.	**No breach discovered, but concerns noted on adequacy of controls.** No signs of a breach occurring, but during inquiry and investigation concerns were noted regarding the adequacy of controls.	**Further information still required.** Still not certain whether a breach occurred and/or information was extracted by an unauthorized party.	**Breach discovered.** Information was accessed and extracted by an unauthorized party.
⬇	⬇	⬇	⬇
No further action required. Findings can be incorporated into the next scheduled exam.	Document the risk identified and the control processes surrounding that risk. Communicate with analyst for ongoing monitoring. Schedule a targeted exam or interim work to look into the issue further.	Consider calling a targeted exam regarding the issue. Perform additional interim work. Analyst provides ongoing monitoring.	Contact Market Conduct department (or similar department) and begin hand-off of the investigation to them.

Additional Resources

Cyber Alerts & Bulletins:

https://us-cert.cisa.gov/ncas

Publicly disclosed cyber vulnerabilities:

https://cve.mitre.org/

National vulnerability database:

https://nvd.nist.gov/

Reported breach tracker for health information:

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Attachment Two

RFAWG Referral

-Section 1-3
-Exhibit C

NAIC National Association of Insurance Commissioners **& The CENTER for INSURANCE POLICY and RESEARCH**

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.

- o 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.
  - o 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.

- Elements of a training that are tailored to the employee's specific roles, responsibilities, and access rights.

Since cybersecurity threats are constantly evolving, it is important to have a strong and up-to-date training regimen. Additionally, in a strong cybersecurity program trainings should be performed on a consistent and periodic (e.g. annually) basis to ensure the information reaching the employees is commensurate with the modern-day threats facing the company. As regulators evaluate the appropriateness of the program, they should consider whether the training is mandatory for all employees and whether it includes procedures and instructions for employees to follow in the event that the employee has a good faith, fact-based belief that a breach or cybersecurity event may have occurred.

Vulnerability Management

In the most robust information security programs, companies understand that not all vulnerabilities can be eliminated, typically due to business needs or time and resources. However, companies should have an understanding and should inventory their identified vulnerabilities as well as have a plan to ensure vulnerabilities that can't be eliminated are mitigated as much as possible. For instance, if the insurer is unable to confirm that a third-party service provider is able to secure their own access to the company's information system, the company should ensure they monitor the service provider's access to determine if improper activity occurs on the company's network. As many vulnerabilities originate with a company's patching practice, it is important that regulators obtain an understanding of the company's patch management. Research suggests that in any given year, the majority of breaches have a root in a Common Vulnerability and Exposure (CVE) that often has been known and identified for several years. An insurer should maintain a strong practice of patch management, or at least a practice of understanding and mitigating existing vulnerabilities as an important part of a robust security program. For vulnerabilities discovered between exam periods, the NAIC maintains a Cyber Vulnerabilities document on the IT Examination (E) Working Group webpage with company questions and follow-up procedures to learn more about the extent of the vulnerability, how that information can be used going forward, and possible actions to be taken, if warranted (e.g., targeted exam procedures, additional interim procedures, etc.).

Company Acquisitions

Finally, in situations where a company has recently acquired/integrated another company, the IT examiner should also pay special attention to the procedures performed in integrating company systems. This is often when companies are most vulnerable to cybersecurity threats as controls are often in flux and mistakes in integration may create vulnerabilities that are not easily identified or remedied.

Exhibit C, Part Two (Instruction Note 3) includes specific mention of risk statements and sections of the exhibit that can be applied to ensure the examination has an appropriate response to identified cybersecurity risks.

Note that the findings identified through the review of the company's cybersecurity control environment should be communicated to the financial examiner via the IT Summary Memo.

Uniformity of Data for Timely & Efficient Transfer

Legacy systems with uncommon and difficult-to-access data structures should be flagged for further investigation as part of the IT review. Companies with multiple IT platforms, multiple cloud storage providers, or that rely on MGAs or TPAs may be at a higher risk, especially if its data is stored in a commingled environment. The ability to migrate and transfer data may be relevant in a number of scenarios including switching service providers, mergering with or acquiring another company, company insolvency necessitating the transfer of policyholder data to the guarantee fund, etc.. If the data is found to be in a format that is not conducive with timely and efficient data transfer, the IT examination team is encouraged to notify the insurer to discuss data migration and the possible need for a more uniform data standard (for example, Uniform Data Standards—UDS—for property and casualty companies). The IT exam team may also review contracts with third-party data storage providers for clauses on data transfer rights. The solvency outlook of the company may be considered when discussing if data migration to a more uniform format is necessary. See DSS 01.01 in Exhibit C for common controls, information requests, and possible procedures regarding the quality, timeliness, and availability of

data. In summary, the data should be stored in a format which allows it to be accessed, utilized, and efficiently transferred, if necessary.

Note: While Uniform Data Standards apply specifically to property and casualty companies, all companies should have the ability to export claims data through a defined format that would allow the data to be received and utilized by a third-party guaranty fund, if necessary. See the NAIC UDS Operations Manual for more information. This manual is maintained by the National Conference of Insurance Guaranty Funds. The following sections would be most applicable to examiners:

- A Record Extended Table Appendix: IX
- B Record Extended Table Appendix: XIX
- G Record Extended Table Appendix: LVIII
- F Record Extended Table Appendix: LIV
- I Record Extended Table Appendix: LXV
- Coverage Codes: 15-1
- Transaction Codes: 14-1
- Other Code Tables: 16-1

Customization for Small Companies

When conducting an IT review of a small company or a company with a non-complex IT environment, it is acceptable to limit the extent of test procedures performed. However, the examination must adhere to the six-step process outlined above. This includes obtaining the ITPQ responses from the insurer, completing a basic work program, and preparing a summary memo concluding on the results of the IT review and its impact on the rest of the examination.

The most significant area to be customized for small insurers is the IT work program. Regardless of size or complexity, some level of testing is required to be performed to verify the design and operating effectiveness of the insurer's IT environment; however, the presentation of such work may vary. It is recommended that IT examiners perform some level of review for IT general controls in place within each domain of the COBiT Framework. This may be shown using a customized version of Exhibit C – Part Two, where a limited number of controls applicable to the insurer are populated and reviewed. In limited circumstances, as described below, IT examiners may bypass the utilization of Exhibit C – Part Two:

1. If the CPAs or the company's internal audit function (if deemed independent) have performed a review of ITGCs that sufficiently cover risks within each of the COBiT domains, the IT examiner may rely on such work without mapping or linking the work to a separate work program. However, the IT examiner must document their comfort with and planned reliance on the work performed.

2. When the IT environment is simplistic and the insurer utilizes purchased software programs from well-known vendors, IT examiners may choose to summarize, in memo format, the procedures performed for each domain of the COBiT Framework. However, before determining that it is appropriate to bypass the utilization of Exhibit C, IT examiners should consider whether the company has made significant modifications to the software being used, as modifications may impact the software's reliability. In situations where significant modifications have been made and continue to be made, IT examiners should utilize Exhibit C – Part Two to document a consideration of risks relating to change management.

B. Materiality

The examiners should consider materiality before planning and conducting examination procedures and when evaluating the results of those procedures. Materiality is defined as the dollar amount above which the examiner's perspective of the company's financial position will be influenced. It is determined at two levels during the initial planning stage: (1) an overall level as it relates to the annual statement taken as a whole; and (2) an individual balance (annual statement line item) level.

EXHIBIT C
EVALUATION OF CONTROLS IN INFORMATION TECHNOLOGY (IT)

The evaluation of controls in information technology (IT) is a critical element of the examination process. Determining the complexity of a company's IT environment and the extent of work that must be performed to evaluate the controls in place is not always easy. Guidance on how to conduct an IT review is included within the General Information Technology Review guidance provided within Section 1, Part III of this Handbook. The tools included in this exhibit have been developed to assist the examiner in gaining an understanding of and evaluating the effectiveness of the company's general IT controls in mitigating common IT risks, as outlined within the General Information Technology Review guidance.

There are two main sections to this exhibit. Part One, the Information Technology Planning Questionnaire (ITPQ), is a tool designed to assist the examiner in planning the extent of IT control work that might be necessary on an examination. The ITPQ provides the insurance department with a high-level overview of the company's information technology environment. It is used to plan the scope and extent of IT control work to be performed and assist the examiner in determining which sections or risks included in the Evaluation of Controls in Information Technology (IT) Work Program (Part Two of this exhibit) should be prepared for the examination. To achieve maximum benefit, the ITPQ should be completed in advance of even normal examination planning, so that the examiner can begin planning what work the examiner will complete within Part Two.

Part Two of the exhibit is the Evaluation of Controls in Information Technology (IT) Work Program. The IT Work Program has been created to assist the examiner in identifying general IT risks, and to provide example controls and potential test procedures to assist the examiner in evaluating how well the company mitigates its general IT risks. Part Two of the exhibit replaces the Information Systems Questionnaire that has been included in previous editions of this Handbook, and should be used as the primary tool to evaluate a company's general IT controls. For more information on how the two parts of the exhibit should be used during the examination, please refer to narrative guidance included in the General Information Technology Review caption in Section 1, Part III of this Handbook.

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 an SLA exists for each of these services and if data stored at the TPA is comingled with other data sets or clearly segregated.

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.

- Security Awareness Training – Discuss the security awareness training program required for all employees including how often it's required and how participation is tracked. Also discuss the contents of the training program and whether advanced techniques such as anti-phishing campaigns are conducted to reinforce the program.

- IT Asset Inventories – Discuss the inventory management program in place for physical devices, software and applications.

- Third–Party Vendor Management – Discuss the program to assess and address security risks posed by third-party service providers including the group(s) responsible risk ranking or tiering.

- Data Loss Prevention – Discuss the program in place to detect and prevent protected information from leaving the company

c. Provide a description of the types of sensitive information that is maintained or accessed by the company (e.g. Social Security numbers, protected health information, personally identifiable information, etc.) and the approximate amount of records containing each type of information. For each type of sensitive information, provide the number of outside vendors who have access to or maintain sensitive information.

d. If applicable, provide a description of updates to the company's controls and/or processes to ensure compliance with the General Data Protection Regulation (GDPR) or other applicable data protection requirements.

6. Information Technology (IT) Security – Incident Response

a. Provide documentation of the response plan in place for cybersecurity incidents. (Note that this may be covered by the disaster recovery plan, but the plan provided should include consideration of IT-specific events.)

b. Provide a listing of any instances in which confidential company or policyholder information was or was likely to have been breached. Include the following information in the response provided:

- How the event was detected.

- Correlation of events and evaluation of threat/incident.

- Resolution of threat, or creation and escalation of an appropriate work order.

- Post-remediation analysis, including any resulting change in controls/operations to mitigate threat of event reoccurrence.

- Extent of involvement of senior levels of management.

- Extent of expenses (including legal claims to be incurred) as a result of the incident.

- Details on the information that was compromised (both in quantity of information breached and type of information that was breached).

7. System Development/Change Management

a. Provide the name, telephone number and e-mail address for the system architect/chief software engineer (or equivalent).

b. Provide an executive overview of the company's system development life cycle (SDLC) and change-management methodologies and indicate whether the company uses internal personnel and/or external vendors to develop and/or change its systems or programs. Include discussion of the process used when purchasing application solutions.

 c. Provide the name, vendor, version number and platform for all change management/system development software, if utilized.

8. **Business Continuity**

 a. Provide the name, telephone number and e-mail address of the individual responsible for maintaining, updating and testing the company's business continuity and disaster recovery plans.

 b. Provide a copy of your IT business continuity and disaster recovery plans (if not already provided in response to the above questions), including information on any contracts for alternate sites (i.e., named parties, site location, type of site, effective date and period covered). Also, provide evidence of the last test results for the plans and management's resolutions of any test discrepancies.

 c. Provide a description of your company's data and systems backup strategy, including your records retention policy.

 d. Provide a copy of the most current business impact analysis.

9. **Financially Significant Systems**

 a. If the company uses multiple platforms/systems to process financial transactions — including premium, claim, reinsurance and investment transactions — include a reconciliation of amounts processed on each separate system to total dollar amount processed during the prior year. Indicate whether the company anticipates any change in processing volumes during the current year. *Note: The Technology Summary tool provided on iSite+ or a comparable substitute that provides the same information should be used to accomplish this purpose.*

 b. Identify and discuss other significant critical management reporting/operational systems, such as data warehouses, sales and marketing systems, communication systems, management dashboards and any other management information systems.

 c. Discuss the accessibility and transferability of significant datasets (i.e., policy admin data, claims data, etc.). Indicate whether data is able to be queried and transferred in the event of an audit, new storage service provider, or other event that would require data to be relocated.

Systems Summary Grid

For each primary hardware platform, list the application software products used in each of the insurance business cycles.

Hardware Platform (manufacturer/model)	
Operating System*	
Access Control Software**	
Program Management Software	
Database Management Software	
Hardware Location	
Business User Location(s)	
Individual Responsible	

Process/Application	Product Name and Version	Software Source: Developed Internally Purchased – Not Modified Purchased – Customized Outsourced/Service Center	Developer/Vendor	Application Support: Internal/External (Provider Name)	Date of Initial Implementation	Date of Last Significant Update	Is the data stored in accessible and readily transferable format? (Y/N/NA)
Policy Management (including premium-transaction processing and policy record management)							
Claim Management (including claim-transaction processing and record management, and reserving)							
Financial Reporting (general ledger and accounting)							N/A
Investment and Fund Management (including investment-transaction processing and record management)							N/A
Reinsurance Management							
Producer Management (including commissions-transaction processing and agent record management)							
Data Warehouse / Data Mart							

NOTE: Make as many copies as necessary to represent every primary hardware platform being used. These might include mainframe, minicomputer and/or network server systems. Additional financially significant applications should be inserted as needed.

* e.g., z/OS, z/VM, Clearpath, OS/400, i5/OS, Windows Server 20XX, Open Enterprise Server, Linux, Unix, AIX, Open Solaris, etc.
**e.g., RACF, Top Secret, ACF2, BSafe, Active Directory, eDirectory, Solaris.

INSTRUCTION NOTE 1: After the examiner has identified controls over the company's IT environment, based on the company's responses to the ITPQ and other information provided to the examiner, the examiner may determine that these controls over the company's IT environment should be tested for operating effectiveness. Section 1, Part III of this Handbook provides specific guidance on sampling for tests of controls and should be utilized by the examiner when testing the company's identified controls. In some cases, the examiner may be asked to assist in the financial examination, as outlined in the "General Information Technology Review" in Section 1, Part III of this Handbook. If it is determined that some of this work includes substantive testing, the examiner should utilize the substantive sampling guidance provided in Section 1, Part III of this Handbook.

INSTRUCTION NOTE 2: The following issues are addressed in Part One (ITPQ) and Part Two (Evaluation of Controls in IT Work Program). If the ITPQ is utilized and subsequently it is determined that all sections and risks included in the IT work program should be addressed, the responses received in the ITPQ should be considered when requesting information on the corresponding sections of the IT work program listed below.

Information Technology Planning Questionnaire (ITPQ)	Evaluation of Controls in Information Technology (IT) Work Program
2b	APO 01.01-01.02, MEA 02
2c	APO 02
2d	APO 02, APO 04
3e	APO 09
3f	APO 10
4a – 4d	MEA 02
5b	DSS 05.01 – 05.04
7a	APO 03
7b	DSS 03.05, BAI 02.04, BAI 03.05, BAI 06
8b – 8d	BAI 03.02, BAI 04.02, DSS 04
9a – 9c	DSS 04.04, DSS 04.07, DSS 05.01

INSTRUCTION NOTE 3: Examiners may determine that cybersecurity risks are significant for the insurer under examination. This may be based on responses provided to the ITPQ, results of planning and examiner's judgment. To ensure that the examination procedures performed include an adequate response to the insurer's cybersecurity risk, which can affect multiple facets of the IT environment, examiners may consider performing procedures in relation to risk statements APO 1, APO 10, APO 12, DSS 02 and DSS 05. Note these risk statements and associated procedures may or may not explicitly mention the threat of cybersecurity in the language presented, but examiners should customize the procedures provided to respond to this risk as appropriate. Examiners may determine that additional risks are relevant when considering cybersecurity exposure, and should tailor their work program based on information available on the exam. Additional considerations for cybersecurity concerns are located in Section 1-III (A) of the Examination Handbook guidance, entitled "General Information Technology Review."

INSTRUCTION NOTE 4: Examiners should consider the overall accessibility and transferability of the company's claims and policyholder data. Holistically, the exam team should determine whether the company would be able to transfer its data efficiently and effectively to another location should that need occur (e.g., when switching service providers, in the event of an audit or receivership, etc.). Companies that rely heavily on legacy systems, MGAs, multiple cloud platforms, TPAs, or that commingle claims data may be at a higher risk. Risk statements APO 03, APO 04, and DSS 04 can be referenced for procedures surrounding data quality, infrastructure, security, and portability.

PART TWO – EVALUATION OF CONTROLS IN INFORMATION TECHNOLOGY (IT) WORK PROGRAM – DELIVER, SERVICE AND SUPPORT (DSS)

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
DSS 01	The quality, timeliness and availability of business data is reduced due to an ineffective data-management process.	DSS 01.01	All data expected for processing is received and processed completely, accurately and in a timely manner, and all output is delivered in accordance with business requirements.	Provide evidence of the controls that ensure all data expected for processing is available and processed completely and in a timely manner.	Interview company personnel to verify the process controls over data management to determine whether there is responsibility over the availability and completeness of data and the timeliness and accuracy of data processing.
			Procedures are defined, implemented and maintained for IT operations.	Provide a copy of the policy and procedures for IT operations.	Review the standard IT operational procedures and verify the propriety and effectiveness of the procedures for abnormal operating system termination, the inclusion of a callout list in the case of emergency, etc. Verify that batch job duties and responsibilities for each computer operator exist along with shift schedules.
			Claims and policy admin data is stored in a format that allows it to be transferred and utilized, if necessary (for example, in the event of a receivership or audit, changing vendors, etc.).	Provide documentation regarding the accessibility and transferability of company claims and policy admin data.	Review the claims and policy admin data and determine if there would be any accessibility or transferability issues if the company needed to move its policy admin data.
			The scheduling and completion of jobs is organized into a sequence, maximizing	Provide a copy of the job run log showing batch job execution.	Verify that the log is reviewed on a routine basis and on a timely manner.
				Provide a copy of	Verify that procedures include points of contact

Attachment Three

Ransomware Updates

Ransomware Updates to Consider

Section 1-3: Letter A: General Information Technology Review

Proposing new sub-section which covers ransomware concepts and cyber hygiene at a high level.

Ransomware

Ransomware is one of the more common manifestations of a cybersecurity risk. Ransomware attacks pose a significant risk to confidentiality and availability on company data. It is difficult to predict when and where a ransomware attack will strike, so it is important for a company to maintain strong cyber hygiene habits to stay ready for ransomware attacks. At a minimum, insurers with good cyber hygiene do the following:

- Patch their systems/networks regularly, timely, and in accordance with application updates
- Require strong passwords and multi-factor authentication
- Have email filtering and anti-phishing training for employees
- Monitor and react to suspicious activity on their network
- Have system backups that are stored in an air gapped, offline environment that is inaccessible from the internet; this backup can be quickly deployed in the event the production environment is infected. Companies should test backup deployment regularly.
- Have firewalls within the network so someone with unauthorized access cannot move laterally
- Limit user access rights to the minimum necessary to perform their job
- Have and test a robust incident response plan

Exhibit C – Part 2 Narrative guidance – Instructional Notes

Adding areas of focus in the Exhibit C table in a similar format as the procedures related to cybersecurity.

INSTRUCTION NOTE 3: Examiners may determine that cybersecurity risks are significant for the insurer under examination. This may be based on responses provided to the ITPQ, results of planning and examiner's judgment. To ensure that the examination procedures performed include an adequate response to the insurer's cybersecurity risk, which can affect multiple facets of the IT environment, examiners may consider performing procedures in relation to risk statements APO 1, APO 10, APO 12, DSS 02 and DSS 05. Note these risk statements and associated procedures may or may not explicitly mention the threat of cybersecurity in the language presented, but examiners should customize the procedures provided to respond to this risk as appropriate. DSS 04 covers the protection of system backups in the event of a ransomware attack. Examiners may determine that additional risks are relevant when considering cybersecurity and ransomware exposure, and should tailor their work program based on information available on the exam. Additional considerations for cybersecurity concerns are located in Section 1-III (A) of the Examination Handbook guidance, entitled "General Information Technology Review."

Exhibit C – Part 2 Table

Proposing new test procedures to the Exhibit C table.

DSS 04 Risk Statement - Inadequate continuity management may result in the inability to ensure critical business functions.

DSS 04.07:

Common Controls	Preliminary Information Request	Possible Test Procedures
All critical backup media, documentation and other IT resources necessary for IT recovery and continuity plans are stored off-site in a secure location.	Provide a copy of policies and procedures relating to the backup of systems and data, including copies of recovery procedures for off-site backups and information about off-site backup locations and/or service providers.	Inquire and verify that data is protected and secured when taken off-site and while in transit to the storage location. Inquire and verify that the backup facilities are not subject to the same risks as the primary site. Inquire and verify that there is an air gap between the company's production environment and backup systems. The air gap should be designed in a manner that if a ransomware attack infects the company's main production systems, the offline backups could be deployed to replace the infected systems.

DSS 04.08:

The company has procedures in place for backup and restoration of systems, applications, data and documentation that are consistent with its business requirements and continuity plan. The backup environment should be isolated, air gapped, and inaccessible from the internet so that information cannot be accessed remotely.	Provide evidence that backup and storage requirements for critical systems, applications, data and related documents are periodically reviewed and aligned with risks and the continuity plan. Provide evidence that backup and storage environments are properly isolated and inaccessible remotely.	Verify that critical systems, applications, data and related documents that affect business operations are periodically reviewed for alignment with the risk management model and IT service continuity plan. Verify that adequate policies and procedures for backup of systems, applications, data and documentation exist and consider factors including: 1) Frequency and age of backups. Older backups can be used in the event a newer backup copy is infected. 2) Type of backups (e.g., disk mirroring, external media, full, incremental, air gapped offline copy, etc.). 3) Automated online backups. 4) Data types (e.g., voice, optical). 5) Creation of logs. 6) Critical end-user computing data (e.g., spreadsheets). 7) Physical and logical location of data sources. 8) Security and access rights. 9) Encryption.