## PART TWO – EVALUATION OF CONTROLS IN INFORMATION TECHNOLOGY (IT) WORK PROGRAM

This work program has been created to assist examiners in completing a review of the general controls of a company’s information technology (IT) in accordance with the risk-focused examination process. Detail instructions for completing this program can be found in Section 1, Part III, under “General Information Technology Review.” Due to the inherently high degree of change in IT information technology, the period under review for this work program should generally range from the latest 12 to 24 months of the overall financial condition examination time period. The period under review should generally encompass the last year of the examination period and the period of time up to, and including, the actual examination fieldwork.

This work program assists the examiner in identifying the most common risks that are often inherent within the general IT controls of a typical insurance company. Included with the risk statements are examples of common controls, information requests and test procedures that may assist the examiner in determining how the company mitigates each risk.

This work program is categorized into four sections: Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA). These sections are modeled after the COBIT Framework, due to its wide acceptance and use in the IT community. Although these sections are modeled after the COBIT Framework, they do not incorporate all of the control objectives of COBIT; rather, they incorporate only the most common control objectives that might need to be reviewed in an insurance company examination. APO addresses strategies and tactics and integrates IT into the overall business needs and objectives of the company. BAI addresses the identification, acquisition and implementation of those IT strategies and tactics identified within the APO section. DSS addresses the actual delivery of IT services identified in the BAI section. MEA assesses whether the IT processes from all sections are functioning adequately. The COBIT 5 Framework includes a fifth domain, Evaluate, Direct and Monitor (EDM) that assesses the overall governance of the IT environment. This domain was not incorporated in Exhibit C, Part 2 as the concepts presented throughout this domain are considered in other areas of the exam including the review of corporate governance.

In certain situations, additional language has been added drawing on content within other IT frameworks (e.g., the National Institute of Standards and Technology [NIST], etc.) or drawing on content provided by state insurance regulators.

This work program is meant to be customized to include only the general IT risks that are of concern for the company under examination. As a result, the work program will vary from company to company, as the content will depend on the size and complexity of each company’s IT environment. After the risks of concern have been identified, the examiner should consider making common control examples and information requests available to the company to assist the company in explaining how it mitigates each risk. A separate work program template, intended to be sent to the company, is maintained on StateNet and includes a column for “Company Controls Identified,” where the company will be able to document their specific controls for the risks identified by the examiner. This template is designed to assist the examiner in identifying the risk statements, common controls and test procedures, based on the knowledge gained from the examiner’s review of the company’s response within the Information Technology Planning Questionnaire (ITPQ) and other information gathered as part of the “General Information Technology Review” guidance within Section 1, Part III (A). The IT review team should coordinate with the appropriate staff at the company to request this response. After the response is received, the examiner should perform testing as necessary to corroborate the company’s risk-mitigation strategies.

Third Party Work

To assist in the identification and review of unique risks, examiners should obtain all available reports generated as a result of third-party work to ensure that the examiner has access to relevant findings from other entities. Examiners should understand work performed by other entities in auditing/reviewing the insurer’s IT systems (e.g. independent third-parties, federal regulators, etc.) and consider whether the work performed by other entities contains sufficient testing such that reliance can be placed on their work and whether the findings have been suitably addressed, as appropriate.

The following insights may assist regulators and/or cybersecurity experts as they review work performed by third-parties to assess company information security programs. These insights are intended for informational purposes and do not indicate expectations or requirements for insurers. However, if companies have contracted with third-parties to have such work performed, examiners are encouraged to obtain, review, and leverage the work to create efficiencies within the exam process. Among the more common reports issued by independent third-parties that regulators may consider leveraging are:

HITRUST Reports

Health Information Trust Alliance Common Security Framework (HITRUST CSF) Assurance Program validated reports have become increasingly common due to the rise in cybersecurity exposures. HITRUST CSF was developed to provide healthcare organizations a standard reporting framework which covers a multitude of security frameworks, including COBIT and NIST. Paired with the CSF Assurance Program, these standardized reports may be useful to regulators when evaluating both the insurer’s IT General Controls as well as the insurer’s cybersecurity exposure. In reviewing these reports, regulators should determine whether the report is a CSF Validated Report or a CSF Validated Report with Certification. The Certification is awarded in situations where the organization completes a validated assessment and meets a certain scoring threshold (i.e. rating of 3+ on each of the control domains) as well as meets other specified criteria. Certifications are valid for two years from the certification date on the condition that interim reviews and certain monitoring requirements are met. Each report should contain a “Scope of Systems In the Assessment” (Section 5 of the report) that will allow regulators to quickly determine the specific organizations and systems that were considered within the report. CSF Reports are required to be performed by one of 30+ authorized assessors. The HITRUST limit on entities that can issue CSF Reports may be leveraged by regulators to provide comfort over the qualifications of the professionals performing the work. In situations where an insurer has prepared a CSF Self-Assessment, that work may be leveraged as noted in the Section 2, Phase 1 (C) “Utilization of Company-performed Testing” guidance whereas a CSF Validated Report (with or without Certification) may be leveraged under the subsection “Decision Whether to Utilize the Work of Auditors”.

SOC II Reports

Although all System and Organization Controls Reports may be useful, SOC 2, Type II Reports may provide regulators with the most comfort over an insurer’s IT General Controls and or cybersecurity exposure. The type of testing performed in a SOC 2 engagement is driven by the Trust Principles on which an opinion is being provided. As regulators review these reports, they may find SOC 2 reports with the Security, Confidentiality or Privacy Trust Principles selected as having the most relevance for a regulator performing an IT Review within a financial exam. Regulators may also consider the information provided in the “System Overview and Background” section of the SOC 2 report as this will indicate whether the scope of the SOC 2 report is sufficient to allow the regulator to leverage the work performed. The complimentary user entity controls helps ensure that the controls at the insurer are in line with and compliment the controls at the third party service provider. For example, if the insurer outsources various services, the third party service provider may have good controls around user onboarding and termination (i.e. terminated user accounts are disabled within 24 hours), but the insurer may not have a control that would notify the service provider timely when a user is terminated. Because of the control weakness at the insurer, the service provider's control is not effective despite its good design and effectiveness as assessed by the SOC auditor.

Note that it is possible for a firm to issue a SOC II leveraging the HITRUST CSF controls, but this is not strictly equivalent to having a Validated Report, as referenced in the HITRUST section above. While both reports may provide value, any SOC II Report may have differing value as a HITRUST Report is generally more comprehensive.

SOC for Cybersecurity

SOC for cybersecurity reports were created in 2017 with the aim of establishing a standardized framework for evaluating the effectiveness of an entity’s cyber-risk management controls. These reports are similar to SOC II reports, with several important differences. First, SOC for cybersecurity reports are designed for a more general audience, meaning that a person without intricate knowledge of a company’s IT systems would still be able to glean useful information from this report. Therefore, SOC for cybersecurity reports will not contain details and specific results of testing procedures performed by certified public accountants (CPAs). (Such information is normally available within an SOC II report.) Rather, SOC for cybersecurity reports present information in a context aimed at helping the user understand operating effectiveness of an organization’s cybersecurity controls. Another distinction is that SOC for cybersecurity reports are more customizable that SOC II reports. Management can choose the criteria for SOC for cybersecurity reports so long as the criteria chosen are suitable under the clarified attestation standards. Examiners should take special consideration of the scope of SOC for cybersecurity reports when utilizing information for an examination. SOC for cybersecurity reports are advantageous for determining organizational vulnerabilities from cyber threats, whereas SOC II reports would give an examiner a better understanding of the organization’s IT General Controls.

PCI Compliance Reports

Payment Card Industry (PCI) Data Security Standards (DSS) are designed to help ensure cardholder data is protected. Although generally focused on the security of system components that are located within or connected to the cardholder data environment, depending on the information included in the report provided, regulators may be able to leverage the reports to assist in addressing an insurer’s cybersecurity exposure. Therefore, as these reports are obtained and reviewed, regulators should first consider the scope of the systems reviewed and compare that against the insurer’s broader operating environment. If the scope of the systems reviewed is significantly narrower than the insurer’s IT infrastructure, the value of the report is somewhat limited. However, the report obtained may still be able to provide insights for specific systems within the IT infrastructure, depending on the risks identified within the IT review work program.

Other Third-Party Work, Including Penetration Tests, Cybersecurity Program Assessments and Vulnerability Assessments

Insurance companies have been contracting with third-parties to review, assess, or scan the insurer’s security program and identify recommendations for enhancements. Penetration tests typically analyze the security infrastructure and environment of the insurer. During the test, security risks, vulnerabilities, and physical and logical attack vectors are identified. The results of the test will evaluate the current state of the network and benchmark the network against other similar companies. Often times, the third-party will offer remediation recommendations if vulnerabilities are found. Cybersecurity program assessments typically apply a cybersecurity framework to establish scope and baseline. The insurer’s security policies and practices are then evaluated against the framework. Vulnerability assessments are a process to define, identify and classify the security gaps in the network, communications infrastructure, or applications. Companies also obtain Cyber Risk Analytic reports to provide an overall score and assessment on specific aspects of a company’s information security program. Cyber Risk Analytics may also be used by companies as a control in the vendor management process. Third-party work may also be leveraged by regulators to provide more meaningful insight on the insurance company’s information security program. In situations where the reports obtained were provided by a division of the company (e.g. internal audit, etc.), regulators may be able to leverage the work, but may need to exercise increased professional skepticism as compared to work where the work is performed by an independent expert.

Regardless of the report being reviewed, regulators should specifically consider the scope of work, independence of the firm performing the work, qualifications of the vendor performing the work, timing of the work performed, and the findings included in any report received. Based on the regulator’s review of the third-party work, regulators may be able to use the work to enhance the risk assessment, interview, and scoping process performed during the IT review. To the extent that findings are noted in the report obtained, regulators may find it more useful to corroborate the remediation of the findings as opposed to performing an independent review of the company’s controls to confirm the finding’s existence.

Regulators should also consider the sensitivity of the information contained in these reports, as they request access to and document their review of the reports. Regulators should consider whether an on-site, “read only” review is appropriate, especially in situations whether the reports make specific references to identified vulnerabilities. Regulators may also wish to only document a general summary of their review as opposed to making more specific notations of their review based on the sensitivity of the information contained in the reports reviewed.

Note that in situations where management has contracted with third-parties to perform cybersecurity assessments, IT examiners can leverage the procedures performed based on the examiner’s judgment. In determining the degree of reliance, the IT examiner should consider the factors noted in Handbook Section 1, Part III (F) under the subsection “SSAE 18 and Service Organization Control Reports” and Section 2, Phase 1 (C) under the subsections “Decision Whether to Utilize the Work of Auditors” and “Utilization of Company-performed Testing.”

**Small/Medium-Sized Company Guidance**

For many small or medium-sized insurers, a number of the risks and suggested test procedures included within this work program may not be relevant. As such, the risks identified and testing to be performed should be customized to meet the needs of each individual examination. However, the work performed should allow the examination team to determine whether general reliance can be placed on a company’s IT general controls. To ensure that sufficient work is performed, the customized program should continue to address each of the four primary COBIT domains, at least at a basic level. Examiners may find it useful to reference COBIT QuickStart guidance available to assist in customizing the work program for a smaller insurer. In addition, other instructions for completing an IT review for small/medium-sized companies can be found in Section 1, Part III, under “General Information Technology Review.”

Additional explanations for the information included in this document and how it may be used by the examiner are as follows.

Risk Statement

The risk statements provided within the work program are the most common general IT control risks an examiner will likely encounter at an insurance company. This is not designed to be an all-inclusive list of common risks at a company. The information gathered from the ITPQ and other relevant sources should assist the examiner in identifying other risk statements that apply to the company.

Common Controls

The common controls provided within the work program indicate how a typical insurance company might mitigate the specific risks shown in the “Risk Statement” column, but may not apply to each individual company. Each company has its own controls in place to mitigate the identified risks, which may or may not correspond to the common control identified within the work program. Therefore, the company might have adequate controls in place, even if the control does not match the common control listed in the work program. The examiner may wish to provide the common controls to the company under examination to assist the company in developing responses, including controls used to mitigate the identified risk statements.

Preliminary Information Request

The information requests provided within the work program are the minimum level of documentation the examiner will likely need to obtain in order to support the common controls identified within the work program. This list is not designed to be all-inclusive and will not necessarily provide the detailed information necessary to perform all of the possible test procedures listed in the next column. The examiner should also consider that each company has its own form of documentation, which might differ from the information request listed in this work program.The examiner may wish to provide the information request, along with the risk statements and common controls, to provide an understanding of the evidence expected to be provided by the company under examination. In some instances, the examiner will need to request additional detailed information to perform the possible test procedures included in the work program.

Possible Test Procedures

After gaining an understanding of the controls in place to mitigate the relevant risks, the examiner should test the effectiveness of the company’s controls. Examples of possible test procedures are included in this work program. The test procedures provided are not designed to be an all-inclusive list and might not apply to all insurance companies that are under examination. In some circumstances, the examiner will need to develop additional test procedures or modify existing procedures beyond what is included within the work program. As mentioned above, for some possible test procedures, the examiner will need to request additional detailed information to perform testing. In addition, it is not expected that all possible test procedures will be utilized for all companies under examination.

**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.