IT Review Modernization – 2025 Project Proposal

Executive Summary

The IT Examination Working Group (ITEWG) is modernizing the IT examination process to better address cybersecurity risks while maintaining efficient evaluation of IT General Controls (ITGC). This document outlines a streamlined approach that:

1. Separates the ITGC reliability assessment (completed by the end of Phase 2) from the prospective cyber risk evaluation and focuses on areas likely to be in scope for the financial examination
2. Continues to use the COBIT framework (updating to COBIT 2019) for ITGC while incorporating NIST CSF 2.0 for cybersecurity
3. Creates distinct deliverables with clear objectives for each assessment
4. Optimizes the overall IT review without significantly expanding examination time

Introduction and Background

In 2023, the IT Examination (E) Working Group (ITEWG) received a referral from the Cybersecurity (H) Working Group requesting that the ITEWG review the IT examination process and evaluate if there would be a benefit to making the process more cybersecurity focused. The referral suggested several frameworks and documents that could be useful in addressing the request, including the Cybersecurity Performance Goals (CPGs) of the Cybersecurity and Infrastructure Security Agency (CISA), the Cybersecurity Framework (CSF) 2.0 of the National Institute of Standards and Technology (NIST), or the benchmarks of the Center for Internet Security (CIS).

The ITEWG determined that there could be a benefit to enhancing the cybersecurity procedures in Exhibit C and, after evaluating options, decided to incorporate updates based on the NIST CSF 2.0 because it addresses concepts not previously incorporated in the COBIT-based IT review process while also being in a familiar format similar to Exhibit C.

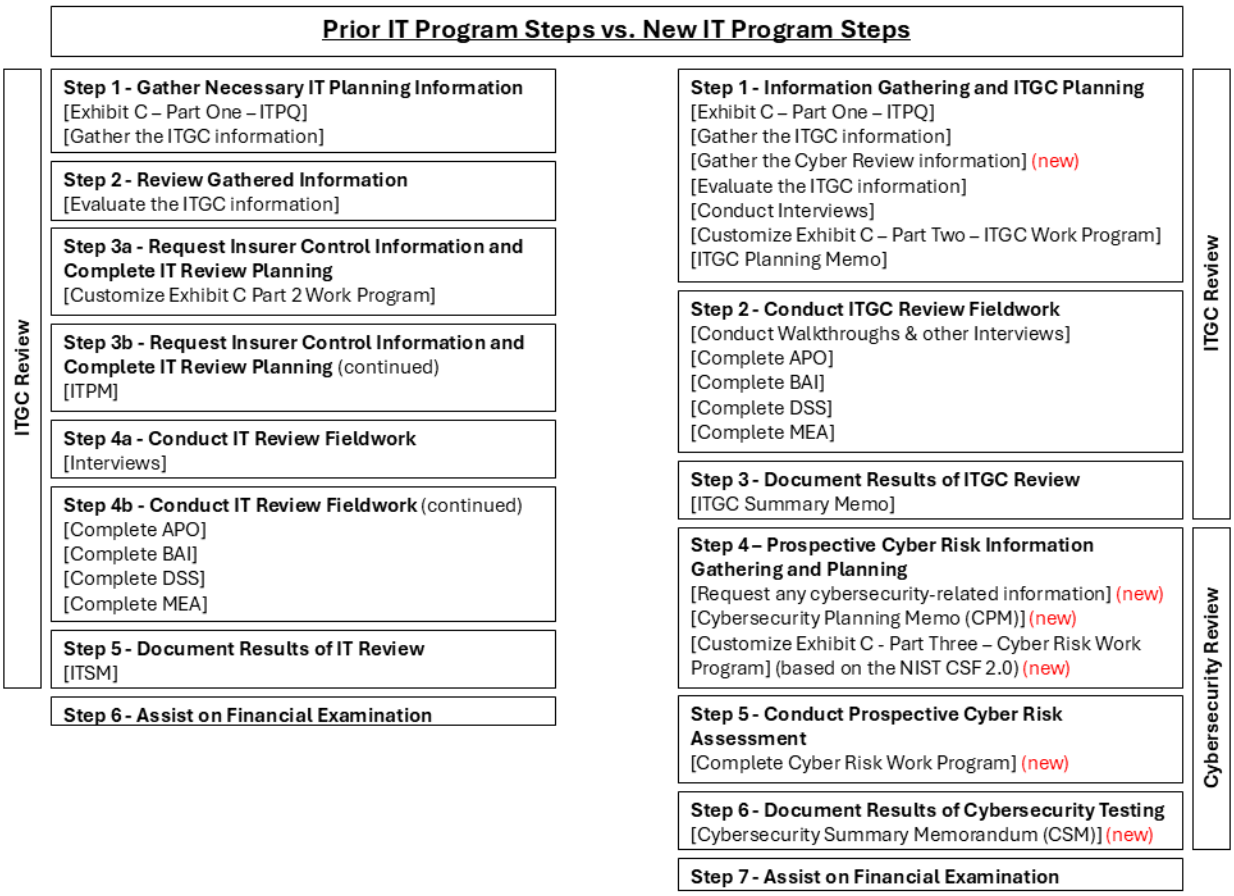
Due to time constraints for incorporating changes into the *Financial Condition Examiners Handbook*, the drafting group chose to take a two-step approach to these changes. In the first step, the drafting group performed a gap analysis of the current Exhibit C procedures versus the NIST CSF 2.0 and modified Exhibit C to address those gaps.

In the next step, a new drafting group will separate procedures needed to establish the reliability of IT General Controls (ITGC) from those needed to examine cybersecurity preparedness on a prospective basis. The drafting group will take care to ensure findings and conclusions concerning ITGC can be made before the end of examination planning (i.e., Phase 2), whereas work in assessing prospective cyber risk may take place later in the examination process.

Due to the expansion of cybersecurity testing, some current ITGC review procedures in Exhibit C will need to be streamlined or eliminated during this process, to avoid redundancy and ensure that the overall time budget allocated to the IT review of a financial examination

is not significantly expanded. It is important that the resulting ITGC and cybersecurity reviews remain right sized for examination purposes.

Updated Process



Given the goal to separate the ITGC review from the prospective cyber risk assessment, the updated IT review process is proposed to consist of the following 7 distinct steps:

1. **Information Gathering and ITGC Planning**

   This step combines several of the previous steps.

   Changes to the Information Technology Planning Questionnaire (ITPQ), included in Exhibit C - Part One, will need to address the split of work into ITGC reliability and prospective cyber risk assessment. Some additional questions concerning cybersecurity will be needed, while other questions may be found to be redundant. Third-party assessments (e.g., SOC reports or external audit testing) will also be requested as needed so that they may be leveraged by the IT examiner.

Following receipt of the completed ITPQ and any third-party results, responses will be analyzed for completeness and used to develop a preliminary risk assessment. Third-party work will be leveraged to enhance efficiency when appropriate.

Following this analysis, more targeted information aligned with and specific to the scope of the current financial examination will be requested. This can include interviews with company staff, as needed.

At the end of this step, the ITGC risk assessment and planning documentation will be completed in preparation for fieldwork, including customizations to the ITGC Evaluation of Controls Work Program (Exhibit C - Part Two) based on this risk assessment and determined reliance on third-party work as well as the ITGC Planning Memo.

2. Conduct ITGC Review Fieldwork

Step 2 will focus specifically on the reliability of ITGC risks, with only focused work (just that needed for ITGC determination) concerning cyber risk. Most prospective cyber risk work previously conducted during fieldwork will now take place during Step 4, below. IT examiners will conduct any remaining necessary interviews, walk-throughs, and control testing, as well as other work needed in the scope of the ITGC review.

3. Document Results of ITGC Review

An ITGC Summary Memo (ITSM) will be created to provide clear findings and recommendations related to ITGC reliability to the financial examination staff. The ITSM will be delivered to the financial examiners before the end of Phase 2 of the financial examination.

The ITGC reliability determination should conform to the “Effective”, “Ineffective”, or “Effective except for…” (e.g., limitations or concerns regarding IT General Controls for a specific system) language outlined in the current *Financial Condition Examiners Handbook* and best practices documents. ITGC reliability determination will use a COBIT 2019 framework as the baseline for inquiries and testing.

IT examiners will also develop management letter comments related to ITGC findings, as needed.

4. **Prospective Cyber Risk Information Gathering and Planning**

Any additional cybersecurity-related information will be requested during this step. For some examinations, all information required might have already been collected in Step 1.

This information will be used to develop a risk-focused testing plan based on the NIST CSF 2.0 framework by customizing the Prospective Cyber Risk Evaluation of Controls Work Program (Exhibit C - Part Three). Previous work for ITGC reliability determination and third-party work (penetration tests, security reviews, internal audit work, CPA work, etc.) will be leveraged to the extent possible. The scope of this assessment should be carefully tailored to the examination and according to the insurer's nature, size, complexity, and risk profile as well as consideration of the materiality of potential risks.

At the end of this step, the cyber risk assessment planning documentation will be completed in preparation for fieldwork, including a targeted Cybersecurity Planning Memo.

5. Conduct Prospective Cyber Risk Assessment

The prospective cyber risk assessment should be completed prior to the conclusion of Phase 5 and should result in an assessment of prospective cyber risk exposure being provided to the financial examination team and analyst in accordance with the current prospective risk assessment guidance outlined in Exhibit V of the *Financial Condition Examiners Handbook*.

This work should apply the NIST CSF 2.0 framework to evaluate the forward-looking cybersecurity posture using the IT examiner's professional judgement. Testing should be conducted for controls specifically related to cyber risk and should be used to help assess the effectiveness of the insurer's govern, identify, protect, detect, respond, and recover capabilities. Other work could include evaluation of emerging technology risks and their impact on the insurer's near-future operations.

6. Document Results of Cybersecurity Assessment

A Cybersecurity Summary Memorandum (CSM) will be prepared to document the results of the fieldwork. After considering the insurer's inherent exposure to prospective cyber risks (e.g., nature of operations or sensitivity of data), as well as the controls and mitigating strategies in place, the IT examiner will determine whether the residual risk assessment level of Cybersecurity to the insurer is minimal, moderate, or significant and whether the trend of that risk is decreasing, static, or increasing. The drafting group will be tasked with developing additional guidance to assist the IT examiner in reaching this determination, as well as in identifying any significant findings or recommendations to be provided to the insurer based on the cyber risk assessment work performed.

The CSM will include specific recommendations concerning identified weaknesses. The memorandum will also provide insights to the financial examination staff and financial regulators concerning prospective cyber risks and the insurer's

preparedness in each area, as well as information to financial regulators concerning these threats that may be useful to monitor until the next examination (e.g., results of an annual third-party penetration test).

IT examiners should help translate specific findings and recommendations from the CSM to the Exhibit AA - Summary Review Memorandum and will develop management letter comments related to cyber risks as needed.

7. **Assist in Financial Examination**

   This step is otherwise unchanged from the previous Step 6. IT examiners will support financial examiners in addressing both ITGC and prospective cyber risks, translate technical findings into business impacts, provide guidance on the relevance of identified issues to overall solvency concerns, and assist in developing comprehensive recommendations for regulatory action.

Impact of the New Approach

This effort should allow the IT examiner to provide more effective conclusions and assessments to financial examiners and financial analysts for an amount of time and effort comparable to the current approach. This separation of procedures should result in comparable to faster determination of the reliability of ITGC, potentially enabling the examination process to move forward at a quicker pace.

The total time and effort needed to complete the new seven-step process of an IT Review should be comparable to the current amount allocated for the six-step process. Deliverables will continue to include a finding of the reliability of ITGC (via an IT Summary Memorandum) before the end of Phase 2 and comments to the insurer via a management letter as needed. Additionally, IT examiners will provide information of use to the financial regulators via a Cybersecurity Summary Memorandum similar to the current IT Summary Memorandum, Exhibit AA - Summary Review Memorandum, or similar vehicle concerning the insurer's cyber risk profile.

Timeline

Following a period of public exposure for this document, and with the approval of the ITEWG, a new drafting group will be formed to develop proposed revisions to Exhibit C and related sections of the *Financial Condition Examiners Handbook*. All revisions will be exposed for public comment before being considered for adoption. The NAIC anticipates that due to the nature and scope of the revisions to be developed that the updated guidance will be incorporated into the 2027 edition of the *Financial Condition Examiners Handbook*.

Separating ITGC from Cybersecurity

A new drafting group composed of those with experience conducting IT reviews will be formed to carefully consider the controls and possible test procedures found in the current Exhibit C - Part Two. In most cases, separation between procedures needed for ITGC

assessment (Exhibit C - Part Two) and prospective cyber risk assessment (Exhibit C - Part Three) will be conducted to avoid duplication of work between the two. In some limited cases, possible test procedures might be moved from ITGC assessment to the cyber risk assessment if they are not needed for determination of ITGC reliability and pertain to cybersecurity.

Examples

- Some risks and controls will be moved to the new Exhibit C - Part Three. An example of this is APO 14, which was added during the gap analysis work conducted last year.

- Some risks and controls will be split, with some possible test procedures remaining as part of ITGC reliability determination while others are moved to the prospective cyber risk assessment. An example of this is DSS 04.01 – DSS 04.02 and DSS 04.05, which include possible test procedures related to continuity management in the event of several potential issues, including cyber risks.