Overview of Nonbank Cybersecurity Exam Programs

Nonbank Cybersecurity and IT Work Group developed the Baseline Nonbank Cybersecurity Exam Program (V1.1) and the Enhanced Nonbank Cybersecurity Exam Program (V1.1). These comprehensive exam programs provide state regulators and industry the tools needed to conduct a review of a nonbank institution's information technology (IT) and cybersecurity risks. The exam programs consist of an exam notification letter, document request list, and exam procedures. The most recent versions (V1.1) of each exam program were released on 10/21/2024.

The exam programs are part of the CSBS Networked Supervision initiative[1] aiding in common supervisory practices while advancing the level of state IT and cybersecurity supervision. Their addition to the State Examination System (SES) allows regulators to harmonize and automate the exam process, while streamlining work for institutions. They were released to industry to foster institution internal review using the same tools as regulators.

Exam Program Details

The two exam programs were created by the Nonbank Cybersecurity and IT Work Group, comprised of state regulator IT and cybersecurity subject matter experts. The companion exam programs build off one another with the enhanced exam program containing the baseline exam program questions, plus review areas for more complex institutions or IT situations. This allows examiners to transfer easily from one exam program to the other based on the size, complexity, and risk profile of the institution. Both exam programs use the same document request list which also contributes to the ease of transferring between exam programs.

The exam program questions are categorized according to the Uniform Rating System for Information Technology (URSIT) component ratings of Audit, Management, Development and Acquisition, and Support and Delivery. Each question contains the applicable Gramm-Leach-Bliley Act (GLBA) Safeguards Rule citation and document request list reference.

Baseline Nonbank Exam Program

The Baseline Nonbank Exam Program (V1.1) is a program created to evaluate the cybersecurity practices of nonbank financial institutions. This program is designed to ensure that nonbank institutions maintain adequate cybersecurity measures to protect consumer data and prevent cyber threats.

Enhanced Nonbank Exam Program

The Enhanced Nonbank Exam Program (V1.1) is a comprehensive program created for larger and more complex nonbank institutions. It contains all the questions in the Baseline Nonbank Exam Program with additional exam questions in areas where a deeper dive may be required.

[1] https://www.csbs.org/advanced-site-search?search_api_fulltext=network+supervision

FAQs

1. What documents are included in the baseline and enhanced nonbank exam programs?
   - Both exam programs consist of an exam notification letter and pre-exam document request list for regulator use, and the exam program. The exam notification letter and pre-exam document request list are the same for both the baseline and enhanced exam programs.

2. The pilot of the Baseline Nonbank Exam Program contained a Pre-Exam IT Officer's Questionnaire. Does this still exist?
   - No. There is not a Pre-Exam IT Officer's Questionnaire for either of the new exam programs. The questionnaire was discontinued as the questions were either incorporated directly into the new exam programs or deemed unnecessary.

3. What skill level is needed for an examiner to use the baseline exam program?
   - While a basic understanding of information technology and cybersecurity will benefit use of the program, the Baseline Nonbank Exam Program is designed to be used by all examiners regardless of information technology skills or expertise.

4. What skill level is needed for an examiner to use the enhanced exam program?
   - Examiners using the Enhanced Nonbank Exam Program should possess a comprehensive understanding of information technology, cybersecurity practices and procedures, and the ability to accurately assess risks associated with those practices and procedures.

5. When should an examiner use the baseline exam program vs the enhanced exam program?
   - The primary decision factor for which exam program is used should be based on the complexity of the IT environment. However, secondary decision factors should include time to complete the exam and the examiner skill set.

6. Do the exam programs contain citations to the FTC Safeguards Rule?
   - Yes. The exam program contains the applicable FTC Safeguards Rule citations.

7. Are the exam programs being released to industry?
   - The exam programs are public and available to industry.

8. Are the new baseline and enhanced exam programs found in the State Examination System (SES)?
   - The exam programs are available in SES for all nonbank industry types. They can be found under the CSBS Nonbank Cybersecurity & IT Area for Review (AFR).

9. How will these exam programs be used by state regulators – as a part of a multi-state exam or as an independent exam?
   - The exam programs are flexible in that they can be used as part of a multistate exam, independent exam, or in response to a security event at an institution.

10. Who can I contact with more questions?
    - Please reach out to Mike Bray (MBray@csbs.org) with any questions.

Released 10/21/2024