Overview of Nonbank Cybersecurity Exam Programs

CSBS and the Nonbank Cybersecurity and IT Work Group developed the Baseline Nonbank Cybersecurity Exam Program (V1.1, released March 21, 2023) and the Enhanced Nonbank Cybersecurity Exam Program (V1.0, released May 09, 2022). 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 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 in August 2022 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) was released in March 2023. Version 1.0 was updated to streamline the flow of similar questions, combine like questions, ensure the accuracy of the FTC Safeguards Rule citations, and further align questions with the Safeguards Rule.

Enhanced Nonbank Exam Program

The Enhanced Nonbank Exam Program (V1.0) 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 exist for new exam program (Version 1)?
   - 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 (V1.0) 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 (V1.0) 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 updated FTC Safeguards Rule?
   - Yes. All citations are from the final rule amending the Standards for Safeguarding Customer Information. However, it is important to note that while the effective date has passed, many amendments will not be enforceable until June 9, 2023.
   - The sections with a delayed effective date include: § 314.4(a), related to the appointment of a Qualified Individual; § 314.4(b)(1), relating to conducting a written risk assessment; § 314.4(c)(1) through (8), setting forth the new elements of the information security program; § 314.4(d)(2), requiring continuous monitoring or annual penetration testing and biannual vulnerability assessment; § 314.4(e), requiring training for personnel; § 314.4(f)(3), requiring periodic assessment of service providers; § 314.4(h), requiring a written incident response plan; and § 314.4(i), requiring annual written reports from the Qualified Individual.
   - Even though many of the amendments to the FTC Safeguards Rule cannot be enforced until 6/9/2023, examiners can begin having conversations with management today about these amendments and the need for their implementation. Many of the requirements noted above will take time and effort to implement. It will only benefit the company to begin thinking about these changes now.

7. Where can I find the exam programs on the CSBS website?
   - At this release, the exam programs can be found in the password protected portion of the CSBS website. After log-in, go to the “My CSBS” drop down in the upper right and select → Examiner Tools → Nonbank Cyber Exam Programs. Future releases of the exam programs for industry use will not be password protected.

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

9. 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).

10. 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.

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