Overview of Nonbank Cybersecurity Exam Programs

CSBS and the Nonbank Cybersecurity and IT Work Group developed the Baseline Nonbank Cybersecurity Exam Program (V1.0) and the Enhanced Nonbank Cybersecurity Exam Program (V1.0), released on 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) will allow regulators to harmonize and automate the exam process while streamlining work for institutions. The industry release will 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 (V1.0) is based on the pilot version (previously called Version 1) of the exam program released in December 2020. The new exam program covers the same content as the pilot in a streamlined version, as recommended by testing examiners in 2021.[2] Version 1.0 is redesigned to be easier to use while reducing the overall number of exam questions by nearly half, with no loss of coverage.

Enhanced Nonbank Exam Program

The new 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

[2] The pilot version employed multipart questions with up to six sub-questions, while V2.0 has no multipart questions.

FAQs

General

1. What documents are included in the baseline and enhanced nonbank exam programs?
    - Both exam programs consist of an exam notification letter, a pre-exam document request list, 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. 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, effective January 10, 2022. However, it is important to note that while the effective date has passed, many amendments are not enforceable until December 9, 2022.
    - 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.

Industry

3. Will one of the new cybersecurity exam programs be included in my next exam?
    - Not necessarily. It is up to the state agency (or participating states for multi-state exams) to determine if IT and cybersecurity is included in the exam scope. If it is included in the exam scope, then the lead state must decide if one of the new cybersecurity exam programs will be used.

4. How should an institution use the baseline and enhanced nonbank cybersecurity exam programs?
    - The exam programs are being made available to industry as optional resources. They can be used to assess the institution's cyber preparedness and may be employed during an internal or external review. Companies that use the procedures will also have some advanced understanding of the nature of the state cyber examination process as the procedures are the same as those used by state field examiners.

5. What type of institution should use the baseline exam program? What type of institutions should use the enhanced exam program?
    - The exam programs are a resource for all nonbank institutions. However, the size of the institution, the complexity of the IT environment, the nature of the business, and known past incidents will determine which exam program, and sections of the exam programs, apply to the institution.

6. Who can use the exam programs within an institution?
    - The exam programs can be used by management, IT professionals, auditors, or an entity responsible for a third-party review.

7. What should an institution do with the results of the exam program?
    - The results are for the institution's use and review only.

8. Are the new baseline and enhanced exam programs found in the State Examination System (SES)?
    - The Baseline and Enhanced Nonbank Cybersecurity Exam Programs were added to SES and are available for mortgage origination, mortgage servicing, and consumer finance exams.

Questions

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