List of DOL Audit Questions

July 14, 2021

Below is a list of questions for retirement plan sponsors to consider in the event of a cybersecurity audit. The questions can also be applied to service providers to ensure external compliance.

Please produce all documents relating to any cybersecurity or information security programs that apply to the data of the 401(k) Plan (the Plan), whether those programs are applied by the sponsor of the Plan or by any service provider of the Plan, including:

- All policies, procedures, or guidelines relating to:
  - Data governance, classification and disposal.
  - The implementation of access controls and identity management, including any use of multi-factor authentication.
  - The processes for business continuity, disaster recovery, and incident response.
  - The assessment of security risks.
  - Data privacy.
  - Management of vendors and third-party service providers, including notification protocols for cybersecurity events and the use of data for any purpose other than the direct performance of their duties.
  - Cybersecurity awareness training.
  - Encryption to protect all sensitive information transmitted, stored, or in transit.
- All documents and communications relating to any past cybersecurity incidents.
- All security risk assessment reports.
- All security control audit reports, audit files, penetration test reports and supporting documents, and any other third-party cybersecurity analyses.
- All documents and communications describing security reviews and independent security assessments of the assets or data of the Plan stored in a cloud or managed by service providers.

- All documents describing any secure system development life cycle (SDLC) program, including penetration testing, code review, and architecture analysis.
- All documents describing security technical controls, including firewalls, antivirus software, and data backup.
- All documents and communications from service providers relating to their cybersecurity capabilities and procedures.
- All documents and communications from service providers regarding policies and procedures for collecting, storing, archiving, deleting, anonymizing, warehousing, and sharing data.
- All documents and communications describing the permitted uses of data by the sponsor of the Plan or by any service providers of the Plan, including, but not limited to, all uses of data for the direct or indirect purpose of cross-selling or marketing products and services.

Please note that you may need to consult not only with the sponsor of the Plan but also with the service providers of the Plan to obtain all documents responsive to these requests. If you are unable to produce documents responsive to any of the foregoing, please specify the requests and the reasons for the non-production.

If you have any questions regarding the information in this document, please contact any of our employee benefits attorneys.