ERISA Advisory Council

Data Protection Considerations for Benefit Plans

June 7th, 2016

Scott Esposito
Director
PricewaterhouseCoopers

pwc

Data Protection Considerations
Current state

- As reiterated in a recent AICPA Employee Benefit Plan Audit Quality Alert (EBPAQC Alert #365), plan administrators (also known as the plan sponsor) have a responsibility to implement processes and controls to restrict access to a plan's systems, applications and data, including third party records and other sensitive information.
- In situations where plans choose to outsource key functions to third parties, their responsibility extends to include the control environment of the service provider(s).
- In some instances where there are numerous third party service providers, it may not be well documented or understood by the plan administrators where and how data is being transmitted, stored or used by each of the third-party service providers. An example of this would be if a plan outsourced payroll to one service provider, recordkeeping to another, benefit payments to a third, etc.

Data Protection Considerations
Current state

- This creates challenges for the plan in effectively meeting data protection requirements.
- Additionally, in instances where known third-parties are transmitting, storing and using plan and participant data, plan administrators vary in their approach to managing the associated information security risks at the service providers (e.g., some administrators have a more robust approach than others).

Data Protection Considerations
Current state

- A critical step for plan administrators in evaluating the risks associated with information security is understanding the flow of data between the plan administrator and third parties.
- At a minimum, plans should understand and document an inventory of all sensitive data being shared with third party service providers, including where it is stored, who has access to it, and its use.
- Understanding how plans are sharing data with third parties will help them to better assess the associated information security risks and determine the appropriate risk mitigation procedures.

Service Provider 3rd Party Reporting
Current state

- Most service providers currently issue SOC 1 reports at least annually covering their relevant internal controls over financial reporting (ICFR).
- SOC 1 reports are considered the industry standard for ICFR, and accordingly there has been widespread adoption by service providers and acceptance by benefit plans and their auditors.
- In many instances, there are now contractual obligations between the plans and the service providers requiring SOC 1s because plan administrators rely on these reports in order to properly evaluate the plan's ICFR.
- SOC1 reports are not permitted to extend beyond ICFR, and therefore do not address broader operational and compliance control needs by user organizations.

Service Provider 3rd Party Reporting
Current state

- Plan sponsors are not consistently considering and evaluating the risks associated with information security considerations (e.g., some administrators have a more robust approach than others), and as a result there is not a consistent approach and methodology to mitigating these risks.
- Service providers are often receiving multiple and varied questionnaires regarding information security measures from a significant number (hundreds, in some cases) of plan administrators, at unpredictable times, which can significantly strain resources and may result in an inconsistent level of quality in their responses.
- To meet the demand, vendors are finding themselves investing additional time and resources. The costs to respond to the various questionnaires and inquiries from customers can be extensive, while also taking core resources away from delivering on the core competency of the company.

Service Provider 3rd Party Reporting
SOC 2 Reporting

- One of the options that service providers may leverage to provide additional information to plan administrators is a SOC 2 report.
- While SOC 2 is currently a voluntary exercise (i.e. not required per any specific rules / regulations), these reports can be a useful vehicle for service providers to convey additional information about their controls around the trust principles.
- Currently, the trust principles do not provide a comprehensive cybersecurity assessment, however they do cover some key elements of an information security program that would be helpful for user organizations to understand.
- Specifically, SOC 2 reports provide an assessment of the controls in place at a service organization around the trust principles, which can serve as an important input to the user organization's cybersecurity risk management strategy.
- There is not currently a commonly accepted, industry-wide attestation reporting standard that provides a comprehensive cybersecurity framework assessment over service providers.

Service Provider 3rd Party Reporting
SOC reporting comparison

Intended Subject Matter and Applicable Scope:

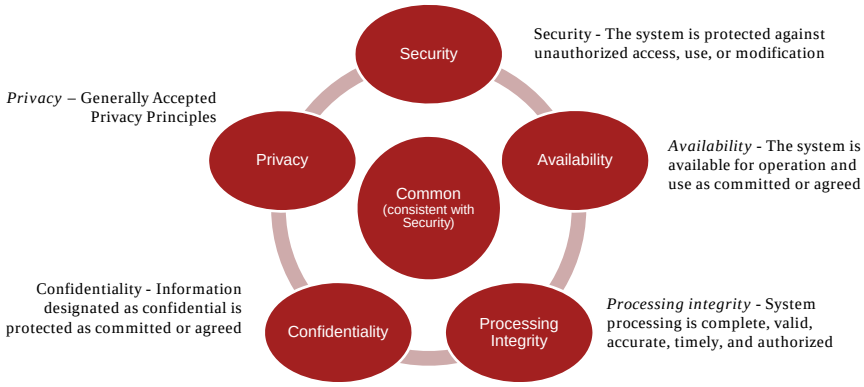
- SOC 1: Internal controls over financial reporting (ICFR)
- SOC 2/3: Report on controls at a service organization that are relevant to the Trust Services principles: Security and/or Availability, Processing Integrity, Confidentiality and Privacy

Intended Users of Each Report:

- SOC 1: External user organization's auditors, management of the organization, and management of the service organization
- SOC 2: Specified parties who have sufficient knowledge and understanding of the services provided by the service organization and its internal controls - this generally includes current user entities and management of the service organization.
- SOC 3: Unrestricted distribution

Service Provider 3rd Party Reporting
Trust Principles

SOC 2 and SOC 3 reports provide companies with an option to obtain the assurance they need over compliance and operational controls for functions they outsource to third parties.



Security - The system is protected against unauthorized access, use, or modification

Privacy – Generally Accepted Privacy Principles

Availability - The system is available for operation and use as committed or agreed

Confidentiality - Information designated as confidential is protected as committed or agreed

Processing integrity - System processing is complete, valid, accurate, timely, and authorized

Thank you

pwc