Minimum Baseline Information Technology Security Standards

Item 21 – Group Insurance Board

David Maradiaga, Chief Information Security Officer

Ruth Ballard, Security Analyst

Bureau of Information Security Management

Action Needed

The Department of Employee Trust Funds (ETF) staff request the Group Insurance Board (Board) approval to add requirements to vendor contracts that clarify that alternatives to System and Organization Controls (SOC) 2 submissions must provide to ETF detailed visibility into the health plans security controls — scope, description, evaluation criteria, and results.

Value of a SOC 2 Report

A SOC 2 Type 2 Report is a third-party audit that provides assurance about a company's security controls and their operating effectiveness over a period of time. It is designed to help users of the report assess the risks arising from interactions with the company's system, particularly the risks to the security, availability, processing integrity, confidentiality, and privacy of their information.

- **Security** - the security of information during its entire life cycle from creation, use, processing, and transmission to storage
- **Availability** - ensuring that the system is available for operation and use as agreed upon
- **Processing Integrity** - ensuring that system processing is complete, accurate, timely, and authorized
- **Confidentiality** - protecting confidential information from unauthorized access, disclosure, or use
- **Privacy** - protecting personal information from unauthorized collection, use, retention, disclosure, and disposal

Assessment Scope and Criteria

BISM Security Analyst evaluated various aspects found within the SOC 2 report to draw conclusions on the amount of residual risk to member information.

1. Service Auditors Report
2. Management Assertion
3. Trust Service Principles
4. Reporting Period
5. Control Descriptions
6. End User Controls passed to ETF
7. Subservice Organizations
8. Evaluation and Results
9. Management Response to Exceptions

Assessment Scope and Criteria

BISM Security Analyst evaluated various aspects found within the SOC 2 report to draw conclusions on the amount of residual risk to member information.

1. Service Auditors Report
2. Management Assertion
3. Trust Service Principles - the risks to the security, availability, processing integrity, confidentiality, and privacy of their information.
4. Reporting Period
5. Control Descriptions
6. End User Controls passed to ETF
7. Subservice Organizations - How they oversee and mitigate risk of subservice providers
8. Evaluation and Results - evaluation scope, testing criteria and audit findings
9. Management Response to Exceptions - managements response to findings

Recommendations

The Department of Employee Trust Funds (ETF) staff request the Group Insurance Board (Board) approval to add requirements to vendor contracts that clarify that alternatives to System and Organization Controls (SOC) 2. Contracts should minimally include:

- If a health plan fails to submit a SOC 2 Type 2 report (submission of a HITRUST certificate) as they pursue compliance, the health plan must allow further examination of their security practices
- This examination would allow ETF to assess the independent auditor's detailed testing approach; the testing results; and follow-up on their policies, standards, and procedures, including full disclosure and oversight of their subservice organizations
- A deadline for compliance

Action Needed

The Department of Employee Trust Funds (ETF) staff request the Group Insurance Board (Board) approval to add requirements to vendor contracts that clarify that alternatives to System and Organization Controls (SOC) 2 submissions must provide to ETF detailed visibility into the health plans security controls — scope, description, evaluation criteria, and results.

Questions?