CLIENT CORPORATION

Data Advisory Scorecards

2900 S Quincy St #330 · Arlington VA 22209

CLIENT CORPORATION

Data Risk Management Program Scorecards Overview

About This Report

These scorecards provide an overall assessment of CLIENT NAME's (referred to as CLIENT within the scoring tables) Data Risk Management Program, deconstructed into three (3) logical control families, defined to the right.

Methodology & Scorecard Elements

Each aspect of the program and its controls/sub-controls undergoes a detailed breakdown and is given a score based on the findings:

- Effective – All aspects are fully implemented.
- Partially Effective – Gaps exist, resulting in partial coverage.
- Ineffective – Critical gaps exist, rendering it valueless.

Each control and sub-control receives its own scorecard, divided into sections for reference. Each scorecard also contains the following elements:

- Description – the description of the scorecard. For sub-control scorecards, the parent control is identified beneath the name.
- Score – the assessment assigned to that individual scorecard.
- Summary – a brief synopsis of the scorecard findings
- Impact and Breakdown – the upstream/downstream benefits or issues arising from the assessed area, and a description/summary of its constituent elements.

Control 1: GOVERNANCE

The organizational structure and function supporting the program.

This includes goal setting, defining risk thresholds, and the adjudication of Data Risk findings.

Control 2: VISIBILITY

The ability to make informed risk decisions.

This is based upon the technical assessment of data in motion, data at rest, and the effective correlation of both.

Control 3: PROTECTION

The technical and operational enforcement of the organization's risk tolerance.

⚠

CLIENT CORPORATION

Overall Rating: PARTIALLY EFFECTIVE

Summary

CLIENT has not clearly defined what data is important to the organization, and organizational guidance on data management does not contain the level of detail required to be effective. This lack of direction is a critical impact on CLIENT information security. As such, CLIENT does not have the ability to effectively manage data risk.

EVIDENCE AND ANALYSIS

- CLIENT Corporate Policy
- Interviews with CIO, CIS, and CPO
- Technical Review
- User Education Program Review
- Audit results from 2016-2018
- Corporate Data Risk Management Goals 2016-2018

Impact and Breakdown

Upstream Effects

CLIENT leadership lacks the ability to make informed risk management decisions.

Downstream Effects

Uninformed information technology spending.

Workforce confusion and apathy regarding data security.

X GOVERNANCE
INEFFECTIVE

Description

Organizational guidance on data risk management.

Summary Findings

Guidance is fragmented and incomplete. Reporting and metrics are not provided to leadership.

✓ VISIBILITY
EFFECTIVE

Description

The ability to measure data risk.

Summary Findings

CLIENT possesses the tools and technology to measure data risk – except for email.

⚠ PROTECTION
PARTIALLY EFFECTIVE

Description

Enforcement of the organizational risk posture.

Summary Findings

Data safeguards have been purchased, but only partially implemented. CLIENT is unprepared for data incidents.

X

CLIENT CORPORATION

Governance Rating: INEFFECTIVE

Description

Organizational structure and guidance on data risk management.

Summary

CLIENT has not chartered or authorized a governing body to establish data risk objectives and set risk reduction strategies. While corporate policy does identify PII as a sensitive data type, no other type of legal, compliance, or business critical information is outlined within. CLIENT is gathering metrics from a DLP solution - however these reports are not shared outside of the technical operations team.

EVIDENCE AND ANALYSIS

- CLIENT Corporate Policy
- Acceptable use guide
- Interviews with HR, CPO, Internal Audit
- Industry best practice(s)
- April 2017 CLIENT Breach Report

Impact and Breakdown

Upstream Effects

The ability to measure compliance with organizational requirements is limited by organizational gaps.

Downstream Effects

The inefficiency of informal processes are impacting the Data Risk Management Program's ability to address incidents effectively.

X ORGANIZATION G1

Description

The corporate structure and resourcing of the governing body.

Summary Findings

CLIENT does not have a chartered governance body that oversees data risk reduction and strategy.

⚠ STRATEGY G2

Description

Defining data risk and risk reduction activities.

Summary Findings

PII is the only data asset identified by corporate policy. The plan for data risk reduction is ineffective.

X ASSESSMENT G3

Description

Understanding the current state vs. the ideal state.

Summary Findings

Metrics and reporting are not used outside of the operational team for the DLP solution.

✓ CLIENT CORPORATION

Visibility Rating: EFFECTIVE

Description

The ability to make informed data risk decisions based on evidence.

Summary

CLIENT can measure data risk across endpoints, servers, web, and cloud. Email is not being monitored completely due to technical limitations. CLIENT's DLP and UBA platforms provide the required correlation of data to measure risk effectively.

EVIDENCE AND ANALYSIS

- Network diagram review
- Interviews with ISO, IS Manager
- Architecture assessment
- IS tool review

Impact and Breakdown

Upstream Effects

Governance can measure data risk for PII.

Technical expenditures are not being leveraged to measure complete organizational data risk.

Downstream Effects

Protection measures can only be enforced on what is monitored.

Incidents are detected in near real-time.

✓ DATA-AT-REST V1

Description

Data in storage, both local and cloud.

Summary Findings

A DLP solution is used to assess data risk in storage on a scheduled basis.

⚠ DATA-IN-MOTION V1

Description

Data transmitted through email, web, and cloud.

Summary Findings

CLIENT does not have the ability to inspect email at the Ohio facilities.

✓ DATA USAGE V1

Description

The acceptable use of data.

Summary Findings

CLIENT effectively monitors for the acceptable use of data.

✓ CORRELATION V1

Description

The ability to organize data by attribute.

Summary Findings

The DLP Solution and a UBA solution provide robust correlation functionality.

⚠ CLIENT CORPORATION

Protection Rating: PARTIALLY EFFECTIVE

Description

Enforcing organizational risk posture.

Summary

CLIENT does not have a centralized body responsible for the protection of data. Security teams are focused solely on cyber threat activities. CLIENT cannot respond effectively to a data loss or abuse event.

EVIDENCE AND ANALYSIS

- CIS20 Assessment
- Interviews with CPO, IR Team, CISO
- External and internal 2017 findings
- Security Program Plan review
- Incident Response Policy and Plan

Impact and Breakdown

Upstream Effects

CLIENT security spending is not effectively reducing data risk.

Decentralized data protection responsibilities are not producing enterprise-level results.

Downstream Effects

Conflicting requirements from multiple bodies creates increased errors and gaps in critical data protection.

Data incidents will consume unaccounted time, people, and resources.

⚠ ENFORCEMENT P1

Description

The corporate structure and resourcing of the protection body.

Summary Findings

Threat-based security teams report to infrastructure, creating a conflict of interest. Data security is fragmented and decentralized.

⚠ SECURITY P1

Description

Ensuring the confidentiality, integrity, and availability of data.

Summary Findings

Foundational threat-based tools are implemented. Threat protections do not account for the value of data.

⚠ SAFEGUARDS P1

Description

Ensuring predictable errors do not result in data loss.

Summary Findings

Data protection tools are fully installed. A formal Data Risk Management Program does not exist.

✓ MAINTENANCE P1

Description

Data is managed per the Data Lifecycle defined by Governance and Visibility.

Summary Findings

CLIENT enforces a complete data lifecycle.

⚠ INCIDENT RESPONSE P1

Description

Managing the impact of data-driven events.

Summary Findings

CLIENT's incident response program is based only on threat response. Data incidents are handled informally.