INFOLOCK

Data Risk Management Framework

To access the free updated version of

https://www.infolock.com/

this document click here

What is the Framework?

The Data Risk Management Framework (DRMF) is an addendum to, and an extension of, the CIS Controls. It provides a general set of recommended practices for managing and securing data assets and elements, and significantly broader and deeper control guidance than its Control #13 ("Data Protection"). It can be implemented in conjunction with CIS Controls or as a standalone best practices framework.

This structured methodology allows organizations to assess, prioritize, and remediate gaps in their data security, privacy, and operations program. It should be used:

- To assess gaps in an organization's data security, privacy, and operations practices
- To determine and prioritize remediation actions
- To measure effectiveness over time

About the DRMF Workbook

The purpose of the workbook is to provide clear, concise controls language to use when assessing and remediating data risk management.

The DRMF workbook is organized into the major Control Families: **Governance**, **Visibility**, and **Protection**. Each Control Family is comprised of higher-level Controls, and each Control is decomposed into granular Sub-Controls. The varying levels of detail allow an organization to use the Sub-Controls to provide a focused analysis of their security posture, and then to roll-up the analysis to provide simple, meaningful results that resonate with leadership.

Benefits

Organizations that implement the controls in the DRMF can anticipate the following benefits:

- Improved organizational structure & accountability for data protection efforts
- Improved visibility into data leakage & data loss risks
- More consistent & cost-effective application of security controls
- Better utilization of human resources & technology tools

To access the free updated version of this document click here

INFOLOCK

Table of Contents

To access the free updated version of this document click here

Governance: Providing the Ground Rules 1

Organizational Structure	A Governing Body is chartered, authorized, and accountable for Data Risk Management.
Strategy	The Governing Body determines Data Risk Management priorities and publishes policies and relative supporting artifacts.
Assessment	The Governing Body measures the effectiveness of Data Risk Management activities.

Visibility: Informed Decision Making 2

Data at Rest	A Data Inventory of stored assets and elements.
Data in Motion	Continuous Monitoring of your outbound data.
Data Usage	Continuous Monitoring of data access and utilization activity
Data Correlation	Meaningful understanding of the data risk, requiring visibility into the relationship between the data, the user, and the environment.

Protection: Execution of Governance Requirements 3

Enforcement	A Data Security Body (DSB) is chartered to enforce data security requirements, protect data from malicious activity, and recover from negative events.
Security	Protection for the confidentiality, integrity, and availability of data.
Safeguards	Safeguards to support the workforce and prevent predictable errors from becoming violations.
Maintenance	Data maintenance per the Data Life Cycle.
Incident Response (IR)	IR team proficiency in critical aspects of IR with regular, measured practice.

https://www.infolock.com/

Control 1: GOVERNANCE

Governance provides the organizational ground rules for effective data management. This control focuses on the **Governing Body** of the organizational structure, its strategy, and then assesses its effectiveness.

1.1 Organizational Structure – Procedural Domain

Description: A Governing Body (GB) is chartered, authorized, and accountable for Data Risk Management.
Assessment Methodology: Document Review and Attestation

	Description	Order	Key Metrics
a.	GB is a singular entity and representing the entire organization.	Sequential	The scope of Governance authority in relation to the total enterprise.
b.	GB is free from conflicts of interest.	Sequential	The degree that Governance direction is mitigated by competing interests.
c.	GB reports to the highest level of senior leadership (e.g. CEO, COO, and Board of Directors)	Sequential	The level of Governance authority in relation to the corporate structure.
d.	GB has Service Level Agreements (SLAs) with senior leadership regarding Data Risk Management.	Sequential	The degree in which Governance activities comply with defined service deliverables and schedule.
e.	GB has appropriate capacity to meet SLAs (e.g. time, availability, and authority).	Sequential	The degree to which Governance is structured to make informed decisions on a regular basis.
f.	GB meets regularly to provide timely guidance (1.2) and oversight (1.3).	Sequential	• The establishment and execution of GB meetings to address Data Risk. • Assessment of Service Level Agreement compliance with the organization.

1.2 Strategy – Procedural Domain

Description: The GB determines Data Risk Management priorities and publishes policies and relative supporting artifacts.
Assessment Methodology: Document Review and Attestation

	Description	Order	Key Metrics
a.	Data Risk Management policies and relative supporting artifacts satisfy internal and external business, regulatory, and legal requirements regarding data.	Sequential	The degree that Corporate Policy defines relevant requirements into formal guidance.
b.	Data Risk Management policies and relative supporting artifacts describe **Data Assets**, **Data Elements**, **Data Lifecycle**, and define corresponding **Data Risk Thresholds**.	Sequential	The degree that Governance is translated into actionable direction in terms of defining assets by attribute, risk, severity and state.
c.	Data Risk Management policies and relative supporting artifacts provide guidance for the collection, discovery, visibility, acceptable use, classification, availability, protection, and destruction of data.	Sequential	The degree that Corporate Policy generated by Governance defines technical and procedural requirements.
d.	Data Risk Management policies and relative supporting artifacts are reviewed on a regular basis and updated to ensure guidance is relevant and current.	Sequential	The rate at which guidance is reconciled with current risk.

https://www.infolock.com/

1.3 Assessment – Procedural Domain

Description: The Governing Body (GB) measures the effectiveness of Data Risk Management activities.
Assessment Methodology: Document Review, Attestation, and Sampling

	Description	Order	Key Metrics
a.	GB works with senior leadership to establish **Data Risk Reduction** goals aligned with the Data Risk Management priorities.	Sequential	The degree that data risk reduction is prioritized by corporate leadership. The occurrence of compliance assessment in relation to the rate of environment change and the effectiveness of reporting of results.
b.	GB collects and analyzes evidence regarding performance against Data Risk Reduction goals.	Sequential	The level of totality that assessments in 1.4b reflect requirements from Governance.
c.	GB reports Data Risk Reduction findings to senior leadership.	Sequential	The degree that which results from assessments are translated into risk reduction activities.
d.	GB works with senior leadership to utilize Data Risk Management reporting to establish Data Risk Reduction goals.	Sequential	The articulation data risk management goals and the corresponding impact on data risk.

To access the free updated version of this document click here

Control 2: VISIBILITY

This control focuses on the **Informed Decision-Making** capability of the organization.

2.1 Data at Rest – Technical Domain

Description: An organization has a Data Inventory of its stored Data Assets and Data Elements (1.2b, 1.2c)
Assessment Methodology: Technical Review, Attestation, and Sampling

	Description	Order	Key Metrics (Percentages of)
a.	Network - Unstructured	Unique	• Visible Data Stores • Attributes Detected
b.	Network - Structured	Unique	
c.	Host	Unique	
d.	Cloud	Unique	
e.	Mobile	Unique	

2.2 Data in Motion – Technical Domain

Description: An organization performs Continuous Monitoring of outbound data (1.2b, 1.2c)
Assessment Methodology: Technical Review, Attestation, and Sampling

	Description	Order	Key Metrics (Percentages of)
a.	Network (encrypted and unencrypted data)	Unique	• Visible Data Transmissions • Attributes Detected
b.	Mail	Unique	• Mail Inspected • Attachments Inspected • Attributes Detected
c.	Web	Unique	• Messaging Inspected • Content/Attachments Inspected • Attributes Detected
d.	Messaging	Unique	• Visible Host-Based Transmissions per Three (3) Vectors • Attributes Detected
e.	Cloud	Unique	• Visible Cloud-Based Transmissions • Attributes Detected
f.	Host	Unique	• Detected Host-Based Transmissions to Removable Media • Attributes Detected

https://www.infolock.com/

2.3 Data Usage – Technical Domain

Description: An organization performs Continuous Monitoring of data access and utilization activity (1.2b,1.2c)
Assessment Methodology: Technical Review, Attestation, and Sampling

	Description	Order	Key Metrics
a.	Access - Monitoring who is accessing protected data and through what method/authority	Sequential	• (% of) Users Accessing Monitored Data • (% of) Access Attributes Detected
b.	Activity - Monitoring the change to protected data	Sequential	• (% of) Data Monitored for Manipulation • (% of) Activity Attributes
c.	Anomaly - The deviation from baseline data access and activity	Sequential	The ability to detect unusual behavior as compared to standard activity.

2.4 Data Correlation – Technical Domain

Description: Meaningful understanding of the data risk requires visibility into the relationship between the data, the user, and the environment (1.2b,1.2c)
Assessment Methodology: Technical Review, Document Review, and Sampling

	Description	Order	Key Metrics
a.	Actor - Identification of the person(s) both logically and physically responsible for the action	Unique	The ability to correlate the Actor with Action and Asset.
b.	Action - The manipulation of the asset	Unique	The ability to correlate the Action with the Actor and Asset.
c.	Asset - The data and associated attributes	Unique	The ability to correlate the Asset with Action and Actor.

To access the free updated version of this document click here

Control 3: PROTECTION

This control focuses on the **Data Security Body** of the organizational structure, its ability to enforce rules, provide security, safeguards, maintenance, and incident response.

3.1 Enforcement – Procedural Domain

Description: A Data Security Body (DSB) is chartered to enforce data security requirements as defined by Controls 1.2 and 1.3, or a documented business requirement/request. The DSB is responsible for protecting data from malicious activity and recovering from negative events as efficiently as possible. The DSB must be designed to ensure integrity, efficiency, and effectiveness.
Assessment Methodology: Document Review and Attestation

	Description	Order	Key Metrics
a.	The DSB is a singular organization in purpose and authority.	Sequential	The scope of the DSB's authority in relation to the total enterprise.
b.	DSB reports to senior management.	Sequential	The level of the Data Security Body's authority in relation to the corporate structure.
c.	The reporting structure is free of conflict of interest.	Sequential	The degree that the Data Security Body's direction is mitigated by competing interests.
d.	The DSB is resourced appropriately.	Sequential	The degree to which Data Security Body is inhibited by personal and technology limitations.
e.	Security requirements are articulated by the Security Organization and regularly to Governance and Business leadership.	Sequential	The degree of participation that the Data Security Body has in the formulation of corporate standards and policy.

3.2 Security – Technical Domain

Description: The confidentiality, integrity and availability of data will be protected from malicious internal and external activity as defined by Controls 1.2 and 1.3 or a documented business requirement/request. The Data Control Framework leverages the Center for Internet Security's (CIS) 20 Critical Controls for Security methodology.
Assessment Methodology: Technical Review, Document Review, and Sampling

	Description	Order	Key Metrics
a.	Network Storage (Unstructured) - Departmental Shares, User Directories, Collaboration Sites	Unique	Refer to the **CIS 20 Critical Controls for Security Assessment Methodology** in relation to infrastructure assets.
b.	Network Storage (Structured) - Database, SharePoint	Unique	
c.	Application - Internal or Hosted	Unique	
d.	Host - Local Storage, Memory, and Removable Media	Unique	
e.	Cloud - Sanctioned and Unsanctioned	Unique	

https://www.infolock.com/

3.3 Safeguards – Technical Domain

Description: Safeguards must be in place to support the workforce and ensure predictable errors do not result in violation of data protection requirements as defined by Controls 1.2 and 1.3 or a documented business requirement/request.
Assessment Methodology: Technical Review, Document Review, and Sampling

	Description	Order	Key Metrics
a.	Network – All ports, encrypted and unencrypted	Unique	The degree users are prevented from transmitting protected data through common network protocols.
b.	Mail – Message body and attachment inspection	Unique	The degree users are prevented from emailing protected data in text, attachment, or imbedded document through email.
c.	Messaging – Text, video, and audio	Unique	The degree in which sanctioned messaging applications prevent disclosure of protected data.
d.	Cloud – Sanctioned and Unsanctioned	Unique	The degree users are protected from accidently sharing or transmitting protected data in a cloud environment.
e.	Host – Local storage, and removable media	Unique	The degree users are protected from accidently transmitting protected data to removable media.

3.4 Maintenance – Technical Domain

Description: Data is maintained per Data Life Cycle defined by Controls 1.2 and 1.3 or documented business requirement\request.
Assessment Methodology: Technical Review, Document Review, and Sampling

	Description	Order	Key Metrics
a.	Archiving – Data is moved to the appropriate environment based upon data classification and disposition	Unique	The functionality to automatically move data to a designated area based upon disposition in the data life cycle and response requirements.
b.	Destruction – The irrecoverable obliteration of information	Unique	The ability to render data unreadable and irrecoverable per sub control 3.5f.
c.	Restoration – Returning data to a previous point in time	Unique	The functionality to return data to a previous point in time based up data classification and sub control 3.5e.
d.	Auditing – Maintaining access and system information	Unique	The ability to capture and record user and system activities per defined requirements in Sub Controls 1.3a and 2.3a.

https://www.infolock.com/

3.5 Incident Response – Technical and Procedural Domain

Description: The organization will have Incident Response (IR) functionality as defined by corporate policy. The Incident Response team will be proficient in critical aspects of IR and respond to all data related incidents. Further, IR will be practiced regularly with the results measured for improvement.
Assessment Methodology: Technical Review, Document Review, and Attestation

	Description	Order	Key Metrics
a.	Preparation - Adaption from previous lessons, proactive remedies, and practiced response	Sequential	The maturity of the Incident Response Plan in combination with the effectiveness of IR staff to execute tasks.
b.	Detection - The ability to detect a threat regardless of vector	Sequential	The ability to detect malicious activity through the inspection of encrypted\ unencrypted network traffic and user behavior.
c.	Containment - Limiting the scope of impact in a timely fashion	Sequential	The speed at which threats are prevented from propagating or intensifying.
d.	Eradication - Removing all aspects of a negative event	Sequential	The ability to remove all aspects of malware or malicious user impact.
e.	Recovery - Returning to state prior to the negative event	Sequential	The degree to which critical systems can be returned to a production state with the least impact to the business.
f.	Response - Litigation Hold, Data Breach, Audit Response, Data Discovery, Preservation and Sanitization	Unique	The ability of the organization to respond to the most likely request for information or performing a specific action.

To access the free updated version of this document click here

2900 S QUINCY ST #330
ARLINGTON, VA 22206
+1 (877) 610-5625
https://www.infolock.com/

Copyright © 2018 Infolock. All rights reserved.

PRECIPICE HEALTHCARE DATA LOSS PREVENTION PROGRAM SCORECARDS

OVERVIEW– The DLP Program scorecards deconstruct the DLP Program into three logical control families: Governance, Visibility, and Protection. This report provides an overall assessment of the DLP Program followed by a detailed breakdown of each Control Family. The Control Family definitions are as follows:

Governance– The organizational structure and function to support the DLP Program in goal setting, defining risk thresholds, and the adjudication of Data Loss Prevention findings.

Visibility- The ability to make informed risk decisions based up the technical assessment of data in motion, data at rest, and the effective correlation of that data.

Protection – The technical and operational enforcement of the organizational risk tolerance.

SCORING DEFINITIONS

Effective – All aspects of the control or sub control are fully implemented

Partially Effective – Gaps exist in the control or sub control resulting in partial coverage

Ineffective – Critical gaps exist in the control or sub control, rendering it valueless

SCORECARD NAVIGATION

TITLE – The title provides the description of the scorecard. For Sub Control score cards the parent Control is identified in the upper left corner.

SCORE – The assessment assigned to that individual scorecard.

SUMMARY – A brief synopsis of the scorecards findings.

IMPACT – The upstream and downstream benefits or issues arising from the assessed area.

NEXT LEVEL BREAKDOWN – A description and summary of the constituent elements of that Control or Sub-Control.

EVIDENCE AND ANALYSIS – A listing of the material analyzed to produce the scorecard findings.

PRECIPICE HEALTHCARE

DATA RISK MANAGEMENT SCORECARD
A best practice for managing data risk

INEFFECTIVE

PHC does not have the ability to effectively manage data risk.

IMPACT

UPSTREAM IMPACT
PHC leadership lacks the ability to make informed risk management decisions.

DOWNSTREAM IMPACT
Uninformed information technology spend. Workforce confusion and apathy regarding data security.

SUMMARY

PHC has not clearly defined what data is important to the organization. Organizational guidance on data management does not contain the level of detail needed to be effective. PHC information security and infrastructure teams are critically impacted by the lack of direction.

NEXT LEVEL BREAKDOWN

The three components of data risk management

NAME	DESCRIPTION	SUMMARY
GOVERNANCE INEFFECTIVE	Organizational guidance on data risk management	Guidance is fragmented and incomplete Policy does not address current risk
VISIBILITY EFFECTIVE	The ability to measure data risk	PHC possesses the tools and technology to measure data risk with the exception of email
PROTECTION PARTIALLY EFFECTIVE	Enforcement of the organizational risk posture	Data-safe guards have been purchased, but only partially implemented Unprepared for data incidents

EVIDENCE AND ANALYSIS
PHC 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

GOVERNANCE
PRECIPICE HEALTHCARE

CONTROL FAMILY SCORECARD

The ability to formally express guidelines for managing data risk.

INEFFECTIVE

PHC does not provide effective guidance for data risk management.

IMPACT

UPSTREAM IMPACT

Leadership cannot measure and manage data risk, only HIPPA compliance.

DOWNSTREAM IMPACT

Technical and organizational guidance for protecting important data is critically incomplete.

SUMMARY

PHC provides detailed guidance for protecting patient information in compliance with HIPPA but, does not provide guidance on financial, legal, or business confidential data risk management. Corporate policy is out of date and does not account for current risk. PHC assesses for HIPPA compliance annually, but does not address any other data concerns.

NEXT LEVEL BREAKDOWN

The three components of data risk governance

NAME	DESCRIPTION	SUMMARY
ORGANIZATION MOSTLY EFFECTIVE	The corporate structure and resourcing of the governing body.	PHC's IS governance department is a fully chartered and resourced governing body. Governance reports to senior leadership.
STRATEGY PARTIALLY EFFECTIVE	Defining data risk. Risk reduction.	PII is the only data asset identified. The plan for data risk reduction is ineffective.
ASSESSMENT PARTIALLY EFFECTIVE	Understanding the current state vs. the ideal state.	Governance has access to the appropriate reporting audience. Reporting needs to be tied to actual metrics.

EVIDENCE AND ANALYSIS

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

VISIBILITY
PRECIPICE HEALTHCARE

CONTROL FAMILY SCORECARD

The ability to measure data risk.

EFFECTIVE

PHC can effectively measure risk defined by governance.

IMPACT

UPSTREAM IMPACT

Governance can Measure data risk f or PIII. Technical expenditures are not being leveraged to measure complete organizational data risk.

DOWNSTREAM IMPACT

Protection measures can only be enforced only on what is monitored. Incidents are detected near real time.

SUMMARY

PHC is able to measure data risk across endpoint, server, web and cloud. Email is not being monitored completely due to technical limitations. PHC's DLP platform provides the required correlation of data to effectively measure risk.

NEXT LEVEL BREAKDOWN

The four components that make up visibility.

NAME	DESCRIPTION	SUMMARY
DATA AT REST MOSTLY EFFECTIVE	Data in storage, local and cloud.	DLP program is used to assess data risk in storage on a scheduled basis.
DATA IN MOTION PARTIALLY EFFECTIVE	Data transmitted through email, web and cloud.	PHC does not have the ability to inspect email at the Ohio facilities.
DATA USAGE MOSTLY EFFECTIVE	The acceptable use of data.	PHC effectively monitors for the acceptable use of data.
CORRELATION MOSTLY EFFECTIVE	The ability to organize data by attribute.	Data insight and DLP provide robust correlation functionality.

EVIDENCE AND ANALYSIS

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

PROTECTION
PRECIPICE HEALTHCARE

CONTROL FAMILY SCORECARD

Enforcing organizational risk posture

PARTIALLY EFFECTIVE

PHC is only partially protected from the abuse and misuse of data

IMPACT

UPSTREAM IMPACT

PHC security spending is not effectively reducing data risk. Decentralized data protection responsibilities are not producing enterprise level results.

DOWNSTREAM IMPACT

Conflicting requirements from multiple bodies creates increased errors and gaps in critical data protection. Data incidents will consume unaccounted for time, people and resources.

SUMMARY

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

NEXT LEVEL BREAKDOWN

The five components that make up protection.

NAME	DESCRIPTION	SUMMARY
ENFORCEMENT PARTIALLY EFFECTIVE	The corporate structure and resourcing of the protection body.	Threat based security teams report to infrastructure creating a conflict of interest. Data security is fragmented and decentralized.
SECURITY PARTIALLY EFFECTIVE	Ensuring the confidentiality, integrity, and availability of data.	Foundational threat-based tools are implemented. Threat protections do not account for the value of data.
SAFEGUARDS PARTIALLY EFFECTIVE	Ensuring predictable errors do not result in data loss.	Data loss prevention tools are fully installed. A formal data loss prevention program does not exist.
MAINTENANCE MOSTLY EFFECTIVE	Managing the data life cycle.	PHC enforces a complete data life. Cycle for patient information.
INCIDENT RESPONSE PARTIALLY EFFECTIVE	Managing the impact of data driven events	PHC's incident response program is based only on threat response. Data incidents are handled informally.

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