California Office of Health Information Integrity (CalOHII)

HIPAA Security Rule Toolkit

User Guide

Version 1.0
2/1/2012

Health and Human Services Agency
CalOHII
California Office of Health Information Integrity

Table of Contents

1.0 - HIPAA Security Rule Background 0
2.0 – Purpose 1
3.0 – Intended Audience 1
4.0 – Toolkit Limitations 1
5 – Overview 2
5.1 – Creating an Account and Logging In 2
5.2 – The Dashboard 3
5.3 – Toolkit Introduction Pages 4
5.4 – HIPAA Security Rule Toolkit: Questionnaire 4
5.4.1 Questionnaire Overview 4
5.4.2 Question and Answer Structure 5
5.4.3 Organizational Summary Report 7
5.5 – HIPAA Security Rule Toolkit: Risk Analysis 8

1.0 - HIPAA Security Rule Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

Today, providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management, as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from wherever they are), the rise in the adoption rate of these technologies increases the potential security risks.

A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI.

2.0 – Purpose

The purpose of the CalOHII HIPAA Security Rule Toolkit is to help small organizations in California better understand the requirements of the HIPAA Security Rule, understand their current progress in implementing those requirements, offer suggestions for requirements that have not yet been implemented, and conduct a basic risk assessment of their organizations. The Toolkit is divided into two parts:

- **Questionnaire:** The questionnaire is designed to both introduce the user to the various components of the HIPAA Security Rule as well as capture the user's progress in implementing the Rule in his/her organization. Upon completion of the questionnaire, a report is generated that compares the user's current progress in implementing the Rule versus the requirements contained in the Rule. Further guidance is offered for those areas where a gap is detected.
- **Risk Analysis:** The risk analysis portion of the tool is designed to allow users to conduct a brief analysis of the gaps identified during the questionnaire. This portion of the tool approximates the Annualized Loss Estimate (ALE) and Return on Investment (ROI) for each gap identified. The user can utilize this information to prioritize implementation efforts with respect to remaining gaps (i.e., gaps with higher ROIs should generally be implemented first).

3.0 – Intended Audience

This Toolkit is intended to be used by small organizations within California that wish to augment their understanding and implementation of the HIPAA Security Rule.

4.0 – Toolkit Limitations

It is important to note that the results generated by this toolkit are estimates and should only be used as an approximate guide to evaluate your organization's progress in implementing the HIPAA Security Rule. CalOHII does not and cannot guarantee the accuracy or reliability of the results generated by this toolkit. This toolkit is not intended to make any statement of an organization's compliance with the HIPAA Security Rule. Statements of compliance are the responsibility of the covered entity and the regulatory and enforcement authority (the Department of Health and Human Services, Office for Civil Rights).

This toolkit interactively uses the information you supply to estimate your organization's progress in implementing the HIPAA Security Rule. The general accuracy of this toolkit will depend on how closely the responses provided by you match your actual circumstances; results are not guaranteed.

5 – Overview

A general overview of each main section of the Toolkit is presented below.

5.1 – Creating an Account and Logging In

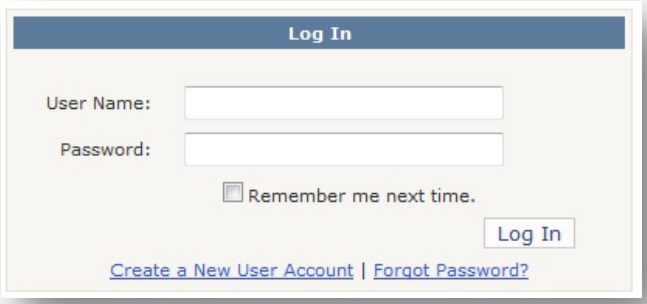

Figure 1: Log In Screen

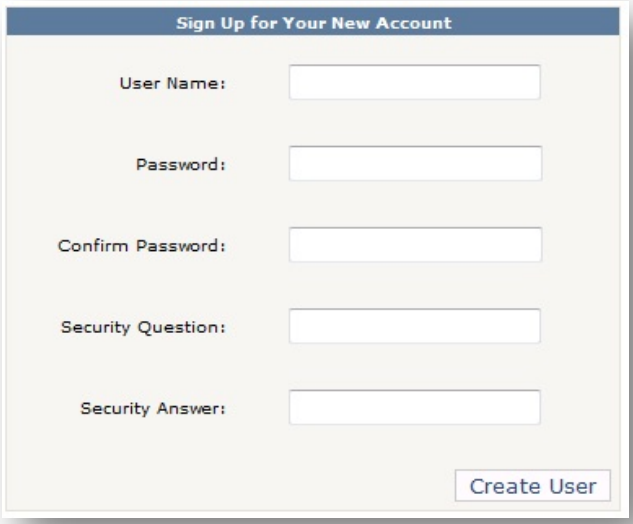

Figure 2: New Account Setup Screen

To create a new user account, click the "Create a New User Account on the Log In screen as shown in Figure 1. This will take you to a page where you can sign up for a new account (as shown in Figure 2.) Enter your desired user name and password (this must be entered twice), as well as a security question and corresponding answer that will be used to allow you to reset your password in the future, should you forget it.

5.2 – The Dashboard

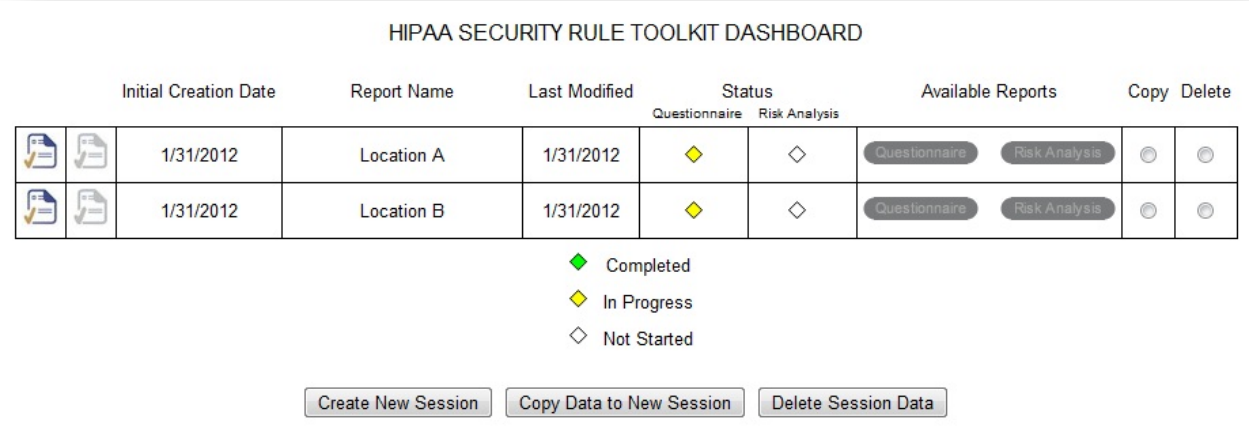

Figure 3: HIPAA Security Rule Toolkit Dashboard Example

Upon creating a user name and successfully logging in, you will be presented with a HIPAA Security Rule Toolkit Dashboard page (an example of which is shown above in Figure 3). For new users, clicking on the "Create New Session" button will begin a new session. Note that you can create multiple sessions for those organizations that have more than one location. A description of each column in the dashboard is provided below:

- **Start or Continue**: To continue a questionnaire or risk analysis in progress, click on the corresponding icon. Note that the risk analysis icon is not active until the questionnaire has been completed.
- **Initial Creation Date**: The initial creation date for this session record.
- **Report Name**: Users can click on the report name to change it as desired. The report name can be the name of the organization, the name of a particular location, etc.
- **Last Modified**: The last date of modification is contained in this column.
- **Status**: The progress status for the questionnaire and risk analysis portions of the toolkit for each record is contained in this column.
- **Available Reports**: Once the questionnaire and/or risk analysis sections of the toolkit are completed, the corresponding reports become available for download in this column. Click on the corresponding button to download either report.

- **Copy/Delete**: Occasionally, users may want to copy one session to another record. An example of this would be for an organization with multiple, similar locations. If many of the questionnaire responses apply to each location, the user may want to save time by copying the session, renaming the copy (to match the second location), and revising any responses to match the HIPAA Security Rule implementation status of the second location. Sessions that are no longer needed can be deleted. To copy or delete a session, put a check in the appropriate box and click "Copy Data to New Session" or "Delete Session Data," respectively.

5.3 – Toolkit Introduction Pages

The introductory pages contained in the toolkit consist of the following:

- **Terms and Conditions**: Outlines general terms and conditions that must be accepted prior to use of the toolkit.
- **HIPAA Security Rule**: Contains a summary of the entire HIPAA Security Rule.
- **Required vs. Addressable**: Contains an introduction to the concept of "required" and "addressable" implementation specifications.
- **How to Use This Tool**: Contains a brief summary description of the two main components of this toolkit (the questionnaire and the risk analysis).
- **About This Tool**: Summarizes the four safeguard areas covered in the Questionnaire portion of the toolkit.
- **Directions**: Contains a link to download this user guide.

5.4 – HIPAA Security Rule Toolkit: Questionnaire

5.4.1 Questionnaire Overview

The HIPAA Security Rule Toolkit questionnaire is divided into four distinct sections: administrative safeguards, physical safeguards, technical safeguards, and business continuity safeguards. As mentioned above, the questionnaire is designed to both introduce the user to the various components of the HIPAA Security Rule as well as capture the user's progress in implementing the Rule in his/her organization. Upon completion of the questionnaire, a report is generated that compares the user's current progress in implementing the Rule versus the requirements contained in the Rule. Further guidance is offered for those areas where a gap is detected.

5.4.2 Question and Answer Structure

A sample question from the administrative section of the toolkit is shown in Figure 4. Each component of the question screen is described below.

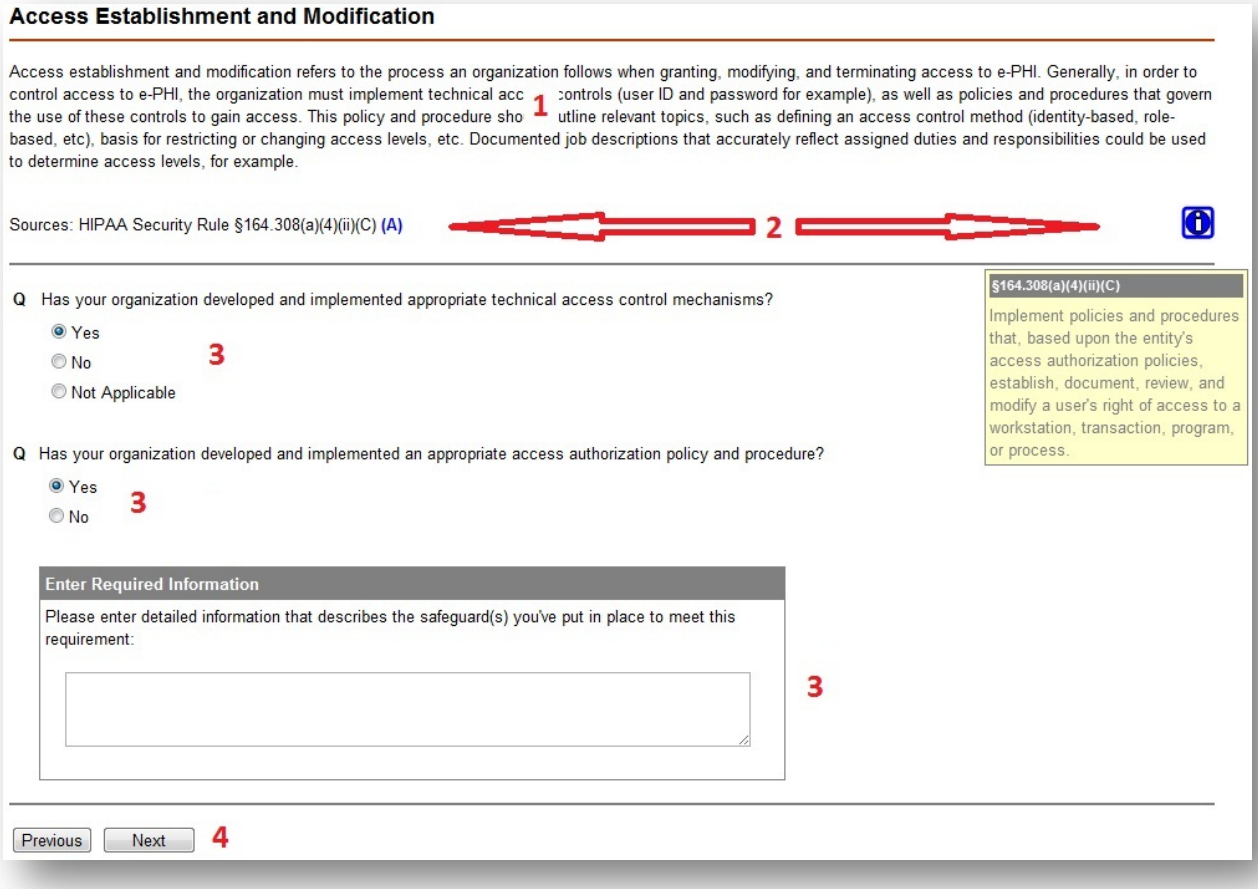

Figure 4: Typical Questionnaire Question

1. **Question Background Information**: Each question in the questionnaire contains a brief background discussion on the question being asked. This background information is provided to aid the user in understanding the scope of the following question(s).

2. **Source(s)**: The portion(s) of the HIPAA Security Rule covered by each question are cited in this area. The left side of the page contains the citation(s), including whether or not the citation(s) is/are addressable (A) or required (R).[1] The right

[1] A discussion of the importance of the difference between addressable safeguards and required safeguards is offered in the introduction section of the toolkit.

side of the page contains one or more information boxes, denoted by a "" icon. When the user points to these icons, the actual regulation text for each source cited appears in a floating box. This information is provided so that the user can easily compare the actual HIPAA Security Rule regulation text with the background information provided in formulating a response to each question.

3. **Initial Question/Follow On Question**: All topics in the questionnaire have at least one question. Users generally have up to three choices in responding:

    a. **Yes**: If the user answers "Yes" to the initial question, one of two options will occur:

        i. **Enter Required Information Box**: If the topic only contains one question, the user will be prompted to enter detailed information that describes the safeguard(s) they've put in place to meet this requirement. This often happens when the topic requires only the implementation of a policy and procedure.

        ii. **Follow On Question**: For topics with more than one question, the user will be presented with a follow on question that requests more information. This often happens when the topic typically requires a technical implementation in addition to the implementation of a policy and procedure (as in Figure 4).

    b. **No**: If the user answers "No" to the initial question, no further action is required. This indicates a gap between the requirements of the HIPAA Security Rule and the organization's implementation progress with that topic.

    c. **Not Applicable**: If the user answers "Not Applicable" to the initial question, the toolkit will prompt the user to enter detailed information that describes the *alternate* safeguard(s) they've put in place to meet this requirement. All questions whose source citations are addressable (A) contain this answer option. As outlined in the "Required" vs. Addressable page in the toolkit, users may elect to meet a given standard through alternative measures. If alternative measures are chosen, the user must document the decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard.

4. **Previous/Next Navigation**: Users may navigate to the previous/next question by clicking the appropriate button or using the navigation pane to the left (not shown in Figure 4).

5.4.3 Organizational Summary Report

The organizational summary report contains the organization's status in implementing each component of the HIPAA Security Rule. This report gives the user a brief overview of its progress in implementing the HIPAA Security Rule. With this report, the user can easily compare each component of the HIPAA Security Rule with the organization's progress in implementing that component. Guidance documents containing more information for implementing each component are also included. A brief description of each column in the report is below:

- **HIPAA Security Rule Component**: Each component of the HIPAA Security Rule is listed in this column, organized by Administrative, Physical, Technical, and Business Continuity subject areas.

- **Regulation Text**: The regulation text for each component of the HIPAA Security Rule is listed in this column. Note that there may be more than one citation for each HIPAA Security Component.

- **Compliance Status**: Your organization's indicated compliance status (responses to each question) with each of the HIPAA Security Rule Components is listed in this column.

- **Gap (Policy and Procedure)**: For those components of the HIPAA Security Rule that require the implementation of a policy and/or procedure, your implementation status will be indicated in this column. If a gap is indicated, your organization may want to review the guidance documentation (described below) for guidance in closing these gaps.

- **Gap (Technical)**: For those components of the HIPAA Security Rule that require the (specified or implied) implementation of a technical safeguard, your implementation status will be indicated in this column.

- **Guidance**: Guidance documentation for each component of the HIPAA Security Rule is listed in this column. For portions of the Security Rule that require the creation of a policy and/or procedure, a customizable policy/procedure document is provided. Other guidance documents include more detailed information on the component it was written for and may include further information such as an overview of the component area, links to external sources of information, etc.

5.5 – HIPAA Security Rule Toolkit: Risk Analysis

Per section 164.308(a)(1)(ii)(A) of the HIPAA Security Rule, organizations must periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. The risk analysis tool can assist you in this task.

Performing a basic risk analysis can aid your organization in focusing its compliance efforts where they're needed most. In order to rank the relative importance of closing identified gaps in implementing the HIPAA Security Rule, this tool utilizes a quantitative risk assessment process which allows for quantifying impacts to information assets due to the successful exploitation (attack) of a vulnerability (lack of safeguard). The process allows for these impacts to be quantified in dollars. Safeguards can then be employed to remediate a vulnerability and the cost of these safeguards can also be expressed in dollars. This common unit of measurement is used to rank the suggested and approximate order of safeguard implementation based on the relative risk to the organization (measured by calculating an Annualized Loss Estimate, or ALE) as well as the return on investment.

The major components and required information you will need to complete each step in the risk analysis are outlined in the following sections.

5.5.1 Asset Inventory and Valuation

In order to effectively protect e-PHI, organizations must have an accurate understanding of where the data resides and how it is transmitted or transported. Building an accurate, up to date asset inventory is a critical first step in conducting a risk analysis and lays the foundation for the rest of the tool. After all assets that contain or transmit e-PHI have been inventoried, an approximate valuation for each asset type can be derived.

As shown in Figure 5 below, a variety of pre-defined asset types are provided, as well as the option to add specific asset types (each “Other” field in the Asset Type column can be renamed as needed). For the purposes of this risk analysis tool, asset values are calculated based on the approximate number of e-PHI records each asset contains or transmits. Asset values for each category are calculated based on the product of average e-PHI records stored or transmitted and the approximate cost of one compromised e-PHI record (this value can be changed or left at the default value of $294).

Asset Type	# of e-PHI Records (stored, or trasmitted per day, on average)	Quantity
Laptop	6800	5
Desktop	0	0
USB Flash Key	0	0
E-Mail	0	0
LAN/WAN	0	0
Servers	0	0
CD/DVD	0	0
Magnetic Tape	0	0
Portable Hard Drive	0	0
Cell Phone	0	0
Other	0	0
Other	0	0

Figure 5: Asset Inventory Table

It is critical that each asset type is inventoried and classified as predominately storing or transmitting e-PHI.

- **Assets That Predominantly STORE e-PHI Data**: Assets such as laptops, desktops, USB flash keys, servers, CD/DVD media, magnetic tapes, and portable hard drives are used to store e-PHI data. For these assets, estimate how many e-PHI records are stored on each asset, on average for a typical day.
- **Assets That Predominantly TRANSMIT e-PHI Data**: Assets such as e-mail systems, LAN/WAN, and cell phones are used to transmit e-PHI data. For these assets, estimate how many e-PHI records are transmitted by/across each asset, on average for a typical day.

To complete the table, you must approximate how many e-PHI records each category of assets stores or transmits. For example, let's assume your organization

has 5 laptops. After examining each one, you've estimated each contain the following amounts of e-PHI records:

Laptop Number	Approximate Quantity of e-PHI records
1	1,000
2	20,000
3	5,000
4	8,000
5	0

Based on this scenario, the average number of e-PHI records stored on your laptops would be 6,800 (the sum of all records stored divided by the number of laptops). This value (6,800) should be entered as shown in Figure 5.

5.5.2 Vulnerability Frequency Determination

In this section, each identified gap in implementing the HIPAA Security Rule is listed along with a selectable range of "vulnerability frequencies." The vulnerability frequency represents the likelihood a lack of safeguard may result in unauthorized disclosure of e-PHI. For example, if your organization has not implemented appropriate policies, procedures, and technical measures (antivirus software, for example) to prevent, detect, and correct instances of malicious software, how often do you estimate your organization may suffer a breach of confidentiality of e-PHI as a result? In this example, it is very likely that your organization may suffer a breach of confidentiality so choosing a higher vulnerability frequency would be appropriate.

5.5.3 Safeguard Cost Determination

In this section, each identified gap in implementing the HIPAA Security Rule is listed along with a corresponding safeguard cost field. The safeguard cost represents your best estimate of the cost of implementing safeguards to close identified gaps with the HIPAA Security Rule. For this section of the toolkit, estimate the total cost of implementing administrative, physical, and/or technical safeguards to close each identified gap.

5.5.4 Annualized Loss Estimate (ALE)

In this section, tables used to derive the ALE are shown. The ALE is defined as the asset value multiplied by the number of breach occurrences in one year. For example, if a class of assets (say laptops) is valued at $100,000 (rating index 5) and has an estimated vulnerability frequency value of once in three years (rating index

3), the ALE would be calculated as $30,000 (when rounded down). This figure should be interpreted as the amount the organization could be expected to spend in any given year as a result of non-compliance with any given part of the HIPAA Security Rule.

5.5.5 Return on Investment (ROI) Table

Now that the toolkit has the required asset value, frequency and cost data for identified gaps, a return on investment (ROI) value can be calculated for each gap. In this toolkit, the ROI value is calculated as the sum of ALEs across each asset class divided by the safeguard cost for that portion of the Security Rule.

The toolkit creates a table containing the ALE value for each asset class and HIPAA Security Rule component. The middle of the table contains the individual ALE values for each asset type (column) and frequency rating for each HIPAA Security Rule standard/implementation specification (row) that you have indicated non-compliance with. The sum of these individual ALEs is contained in the "Full ALE" column. This value represents the total estimated Annualized Loss Estimate should a vulnerability due to non-compliance be exploited. The "Full Safeguard Cost" column represents the organization's estimate of cost to remediate the compliance gap for this standard/implementation specification. The Return on Investment (ROI) column represents the organization's approximate ROI to remediate each compliance gap.

Note that an ROI greater than 1.0 indicates that, on average, it would cost less to remediate an identified gap than the expected losses the organization will incur if the gap is not remediated.

5.5.6 Safeguard ROI Rankings

In this section, the ALE for each identified gap is plotted along with its corresponding safeguard cost[2]. As discussed in 5.5, the ROI is the quotient of these two values and can be interpreted visually as the difference in heights between the two bars for each gap. As discussed in the toolkit, this sorted bar chart allows for the delineation of "action groups" organized by those safeguards with the greatest potential impact if actions are taken to bring them into compliance. The end user can use this chart to move or aggregate safeguards into practical implementation groups based on similar implementation methods or any other implementation consideration.

[2] The plot utilizes the logarithm of each value. This is done to reduce wide-ranging quantities to smaller scopes.

5.5.7 Risk Analysis Report

In this final section, the risk analysis results are added to the organizational summary report. This report gives the user a brief overview of its progress in implementing the HIPAA Security Rule, as well as the ROI for each identified gap in implementing the HIPAA Security Rule.