Clearwater

Whitepaper

Bringing Efficiency and Confidence to Your Risk Analysis Processes

Table of Contents

Introduction 3

Risk analysis challenges 4

Why your organization needs risk analysis 5

The costs of failing to do proper risk analysis and management 5

Ensuring compliance 6

The risk analysis and risk management solution for modern healthcare organizations 7

AI and predictive risk ratings 8

How It Works 8

Benefits 9

Introduction

A lot of healthcare entities and business associates say they struggle with conducting risk analysis because they don't think there is a clear definition about what a risk analysis is and what it should entail.

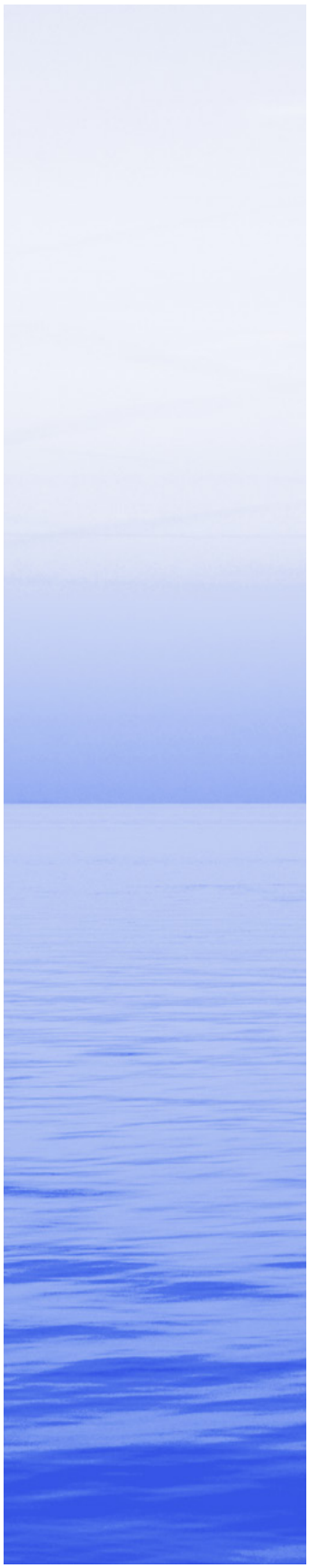
But the reality is, risk analysis guidance has actually been around for more than a decade.

In 2010, the Office for Civil Rights (OCR) published guidance related to the HIPAA Security Rule requirement for risk analysis and risk management.

The guidance includes nine key areas for both healthcare entities and business associates:

1. Ensure comprehensive scope of the analysis
2. Document information asset inventory
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Finalize documentation
9. Periodic review and updates to the risk assessment
10. At Clearwater, we raise the bar further with an additional tenth objective: Meet emerging OCR standard of care.

Think of the OCR risk analysis guidance, which is based off of National Institute of Standards and Technology (NIST) standards, as a framework for your risk analysis program. These guidelines also share commonalities with the ISO 27000 series methodology and workflows. So, while the guidance is specifically for healthcare, it's applicable for all industries, public and private.



In the first half of 2021, the Office for Civil Rights (OCR) has launched more than 250 investigations into HIPAA-related data breaches where 500 or more records may be affected in each breach.

Risk analysis challenges

While OCR created these guidelines to help establish compliant risk analysis and risk management approaches, actually implementing these programs remains a challenge for many healthcare entities and business associates.

Why? Well, when you look at all the guidance for risk analysis, for example, inventorying and assessing all of your assets and media, threat agents, threat actions, vulnerabilities, and security controls, there are millions of combinations for possible approaches.

The ability to do this is a significant shortcoming for many healthcare organizations because most don't understand exactly what they should do. Many organizations also don't have the right tools or resources, and a growing number of organizations don't have the in-house expertise to develop programs that meet all areas of OCR guidance.

Many organizations are resource-constrained and they often lack time and staff to conduct a thorough analysis of risks surrounding all of their electronic protected health information (ePHI) systems and processes.

Documentation, such as creating a risk register for all of your ePHI related systems, is also a stumbling point for many. Far too often, we hear from organizations that don't have clear insight into all the assets they have, where they're at, or how they're used. When you add to that all the threat vectors, potential threat actions, and related vulnerabilities and other security issues, it's challenging to know which areas need your attention first and which controls will work best for your organization's unique and specific needs.

Why your organization needs risk analysis

But as challenging as risk analysis and risk management can be, they're critical parts of your overall cybersecurity and privacy programs that can't be overlooked.

A comprehensive risk analysis helps you meet all of your regulatory and compliance requirements, and it also helps you identify where you have your greatest exposures so you can prioritize how you address them. For example, a risk rating will help you to identify and take action in remediating your greatest risks—risks that are specific to your organization and your threat landscape.

The costs of failing to do proper risk analysis and management

Not only does ineffective risk analysis and risk management put your sensitive data at greater risk for a potential breach, failing to meet OCR expectations can also lead to hefty fines and penalties, and sometimes even legal action.

OCR penalties are tiered related to HIPAA violation severity:

- **Tier 1:** Wasn't aware of violation, could not reasonably avoid it, and has taken a reasonable amount of care to abide by HIPAA requirements. Minimum fine $100 up to $50,000 for each violation.
- **Tier 2:** Should have been aware of the violation, but it couldn't be avoided with reasonable amount of care. Minimum fine of $1,000 up to $50,000 per violation.
- **Tier 3:** Demonstrated willful neglect or HIPAA requirements in cases where the entity attempted to correct the deficiency. Minimum fine of $10,000 up to $50,000 per violation.
- **Tier 4:** Demonstrated willful neglect of HIPAA requirements and did not attempt to correct the violation. Minimum fine of $50,000 per violation.

According to the 2016-2017 HIPAA Audits Industry Report, Phase 2 compliance audits uncovered a range of problems for risk analysis and risk management. Based on report findings, of the 166 covered entities audited, 103 were audited on the privacy and breach provisions and 63 were audited on security requirements. An additional 41 business associates were also audited during the same time period.

The report revealed that few of the covered entities, only 14%, and business associates, only 17%, successfully meet requirements to safeguard ePHI through risk analysis.

The report identified common issues including failures to:

- Identify and assess risks for all ePHI
- Develop and implement policies and procedures to conduct a risk analysis
- Identify threats and vulnerabilities, including potential likelihoods and impacts, and risk rating for ePHI.
- Review and periodically update a risk analysis in response changing environments and/or operations, security incidents, or a significant event
- Conduct risk analyses consistent with policies and procedures

Documentation issues plagued many, including a lack of risk analysis for third-party vendors.

In fact, as we're seeing an increase in both OCR enforcement actions and their related penalties, we're also noting large settlements directly related to failing to complete proper risk analysis.

In 2020, we got a closer look at the financial cost of what happens when healthcare organizations fail to meet these risk analysis and risk management requirements, with some of the largest OCR settlements as a result.

Here's a quick look at the top four largest settlements related to risk analysis compliance issues:

Premera Blue Cross
Failure to conduct enterprise risk analysis. Cost: $6.8 million.

CHSPSC LLC
Failure to conduct risk analysis. Cost $2.3 million.

Athens Orthopedic Clinic
Failure to conduct risk analysis. Cost: $1.5 million.

Lifespan Health System
Failure to encrypt and have business associated agreement. Cost: $1.04 million

Ensuring compliance

If you're a healthcare covered entity or business associate and you're confused about how to handle risk analysis or risk management, our first recommendation is to follow OCR published guidelines.

You can read the full text of OCR's Guidance on Risk Analysis Requirements under the HIPAA Security Rule at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

Here are a few other recommendations that may help:

Efficiently and comprehensively assess, manage, monitor, and report on all risks, and all remediation actions

Understand your organization's most significant threats and vulnerabilities

Determine if you have the right controls in place

Review critical risks and produce OCR-ready reports

Plan a course of action to reduce high risks

Initiate risk response and create, assign, and track remediation actions

Automate management of information risk across your entire enterprise

Need more help conducting a risk analysis based on OCR guidance? Check out our HIPAA Security Risk Analysis Self-Review Survey for more tips and information.

The risk analysis and risk management solution for modern healthcare organizations

Even if you have a general understanding of your organization's requirements for risk analysis and risk management, you may still be scratching your head trying to figure out just how to implement everything to meet OCR standards. And you may find it particularly challenging if you have limited staff, time, tools, and resources.

But there is a bright light here for you. You can overcome some of the most pressing risk analysis and risk management challenges simply, all in a single platform, without having to hire more staff or expand a disparate technology stack across your enterprise.

Clearwater's IRM|Analysis is the industry's top-rated risk analysis and risk management solution. Right out of the box, you can quickly get insight into all of your assets and vulnerabilities and get comprehensive visibility (in an easy-to-understand dashboard) into where you have your greatest risks and what you need to do to fix them.

After you enter all the information about your systems and assets into the software (for example, you can enter them manually or import through ServiceNow), IRM|Analysis uses built-in algorithms to determine all of your potential vulnerability and threat scenarios (based off of your specific technology stack and assets) and then automatically suggests which controls you should use to mitigate threats in these specific scenarios.

IRM|Analysis provides a risk rating relevant to both the likelihood of an event (based on controls you have in place or not) and the potential harm that could be caused (based on the importance of the information system or its data to your organization). From there, your organization can prioritize and report on risks across your enterprise in a consolidated manner through integrated reporting tools and dashboards.

AI and predictive risk ratings

IRM|Analysis doesn't just identify risks; it tells you which risks matter most to your organization based on a range of artificial intelligence and machine learning inputs so you know which ones you should focus on fixing first.

IRM|Analysis creates a Predictive Risk Rating to help you more accurately rate risks via system recommendations. It's based on a 25-point scale drawing on the likelihood of an exploit and its potential impact.

IRM|Analysis' AI-driven Predictive Risk Ratings draw upon more than a million risk scenarios that experts across the industry have analyzed, saving you time and effort for risk analysis.

Through a data mining approach, the technology automatically gathers analytics to "match" similar information systems across risk analyses and suggests a risk rating based on ratings from existing risk analyses. You can automatically accept the risk rating or use it as guidance.

How It Works

- Risk analysts input their analysis
  - Thousands of risk analysts from hundreds of healthcare organizations
  - Clearwater experts contributing their insight

- Risk ratings sent to IRM|Analysis database
  - 1.6 million+ controls analyzed
  - 1 million + risk scenarios
- Clearwater's proprietary algorithm determines risk scenarios
  - 34 categories of information systems
  - 177 control types
  - Aligned with NIST
- AI/Machine-Learning Engine digests and outputs threat and vulnerability information, including suggested likelihood and impact
- Delivers unique Predictive Risk Ratings specific to your organization's environment and threat landscape

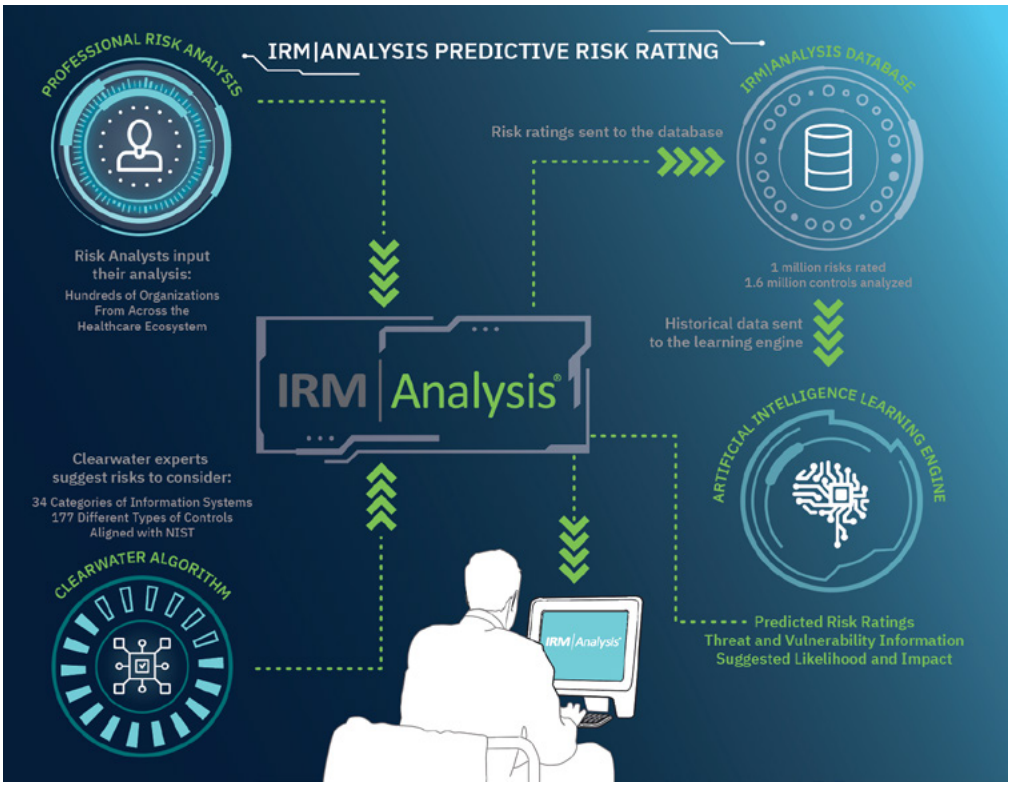
Benefits

IRM|Analysis automates and simplifies many of the more complicated and tedious parts of risk analysis and risk management practices to meet OCR requirements. Among some of the many benefits your organization can reap from using the software for all of your risk analysis and risk management needs are:

- Improved efficiency (save time and resources)
- More risk analysis confidence without having to hire more staff (tap into the knowledge of industry experts who have analyzed the same scenario)
- You can manage your risk analysis and risk management frameworks and all related governance components
- Perform risk analysis within the software. There's even a risk questionnaire list that enables you to manage workflows for your risk analysis activities.
- Insight into your asset inventory, including associated threats and vulnerabilities
- Insight into all risk scenarios that need addressing, including your organization's progress on mitigating or remediating risks
- Get accurate, reliable Predictive Risk Ratings based likelihood and impact
- Conduct risk response or risk management, with recommendations
- Maintain all proper documentation
- Get insight into risk magnitude against industry peers with easy-to-understand benchmarking dashboards

- Be consistent with implementing all OCR requirements for a risk analysis, including creating reports that detail all OCR requirements such as your risk analysis, event impact likelihood, vulnerability types and severity, controls, and remediation plans and activities

In addition to helping ensure OCR compliance for risk analysis and risk management, Clearwater's IRM|Analysis is a great resource to help you quantify your program success, identify gaps, and communicate with your executives and key stakeholders about why your program may need additional resources and financial support and what the potential risks would be if you don't effectively remediate these issues for your organization.



Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact