Clearwater

From Risk Analysis to Risk Reduction: A Step-by-Step Approach

Table of Contents

Introduction

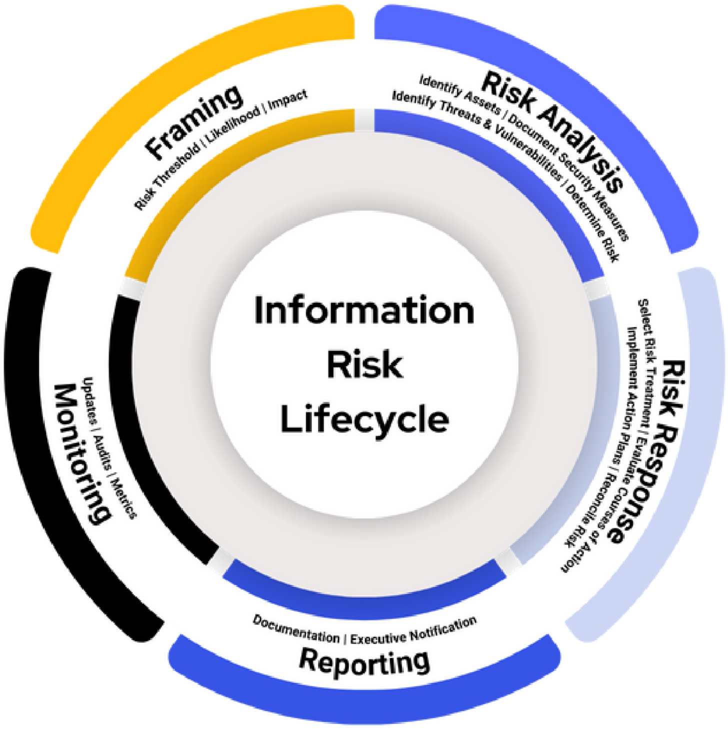
The healthcare landscape has undergone dramatic shifts—a significant portion of the workforce has transitioned to remote work, and telehealth services have surged, breeding new cybersecurity threats and vulnerabilities. Unless strategically countered with proven methodologies, these emerging challenges considerably endanger healthcare organizations' capacity to fulfill their fundamental mission.

Under the HIPAA Security Rule, a comprehensive risk analysis must be conducted regularly on all systems that create, receive, maintain, or transmit electronic protected health information (ePHI) when new technologies are adopted or significant changes in the operational environment occur. These analyses must thoroughly examine how patient data is safeguarded against evolving threats and vulnerabilities, ensuring that the security measures in place are reasonable and appropriate.

A well-developed cybersecurity risk management program transcends the application of the latest controls or responses to trends like ransomware—it demands a deep understanding of an organization's unique threats and vulnerabilities so that resources can be allocated wisely to mitigate these risks over time.

In the event of an investigation by the Office for Civil Rights (OCR), organizations must demonstrate that they have not only identified risks to the confidentiality, availability, and integrity of sensitive data but have also implemented reasonable and appropriate security measures and safeguards scaled to the level of identified threats. OCR looks for demonstrable evidence that an organization's risk management plan is rigorous and effective, focusing on documented proof that security measures have been integrated appropriately to reduce risk.

Compiling such evidence retrospectively, under the pressure of an OCR inquiry, is a daunting challenge, often leaving organizations with limited time to produce the necessary documentation. Clearwater advocates for a proactive, ongoing risk analysis and response process, ensuring that healthcare organizations can readily demonstrate their commitment to comprehensive cybersecurity risk management.


Information Risk Lifecycle
Framing
Risk Threshold | Likelihood | Impact
Risk Analysis
Identify Assets / Document Security Measures
Identify Threats & Vulnerabilities / Determine Risk
Risk Response
Select Risk Treatment | Evaluate Courses of Action
Implement Action Plans | Reconcile Risk
Reporting
Documentation | Executive Notification
Monitoring
Updates | Audits | Metrics

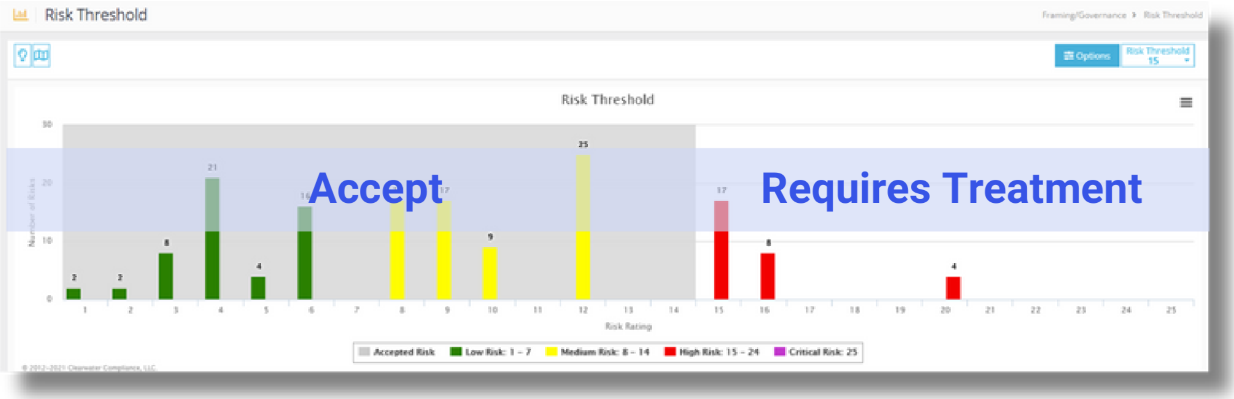
Define Your Risk Threshold

Do all identified risks require the same priority? The answer involves understanding the nature and magnitude of risks within an organization's operational landscape.

Although every risk must be documented and continuously monitored, only a specific set of risks must be treated within a given risk cycle—these are risks at or above your risk threshold. As an example, if you rate risk on a spectrum ranging from 1 (Low) to 25 (Critical), a low risk identified as three (3) is not as concerning when compared to a high risk identified as sixteen (16).

Determining your organization's risk threshold involves understanding two pivotal concepts: your risk appetite and the precision of risk analysis. Crafting a well-defined and accurate risk threshold serves dual purposes: First, it aids in the prudent allocation of cybersecurity investments, and second, it supports the clear definition of acceptable and unacceptable risk levels.

Healthcare organizations, regardless of size, grapple with a multitude of potential security risks that seem to endlessly populate their risk registers, leading to the misconception that every risk demands immediate attention. However, such an approach is not only impractical but also strategically flawed. Effective risk management lies in discerning which threats pose the greatest danger and must receive prioritized attention.



Tailoring Your Risk Analysis: A Tale of Two Covered Entities

To illustrate the process of defining appropriate risk framing and governance values, let's consider two contrasting healthcare scenarios: a small clinic and a large hospital system.

A small clinic, with an annual net patient revenue of $2 million, views financial losses differently when compared to larger organizations. A $500,000 loss could significantly damage its operational stability and long-term viability.

Conversely, a large hospital system, generating $800 million in net patient revenue annually, perceives the same $500,000 loss as a manageable setback, given its more significant financial reserves and operational resilience.

Evaluate Courses of Treatment

After establishing their risk threshold and conducting the risk analysis, organizations have several options to address identified risks: acceptance, avoidance, transfer, and mitigation. Choosing the optimal response hinges on the nature of the risk and its alignment with the organization's overarching risk management strategy.

Risk Response Defined by NIST SP 800-39:

Risk Response	Definition	Example
Mitigate	Implementing mitigating controls is typically the preferred starting point in lowering risks at or above threshold. Organizations should prioritize implementation of safeguards and controls that are reasonable, feasible, and likely to have the greatest impact.	Installation of air gapped storage to reduce impact of ransomware infection and increase the likelihood of successful restoration.
Transfer	Organizations may wish to shift liability or responsibility to other parties or entities, typically through contracts or agreements.	Purchase of a cyber insurance policy to transfer financial risk due to a breach.
Avoid	Organizations may decided to eliminate or reduce risk by discontinuing activities or decommissioning and replacing systems. Keep in mind that through risk avoidance, it is possible to introduce new risks (i.e. loss of critical functionality).	Decommissioning of unsupported or outdated systems, environments, or technologies.
Accept	Organizations may determine that certain risks are not feasible or possible to treat through mitigation, avoidance, or transference. Instead, they may wish to document and acknowledge the risk but take no action outside of performing continuous monitoring and frequent review. Keep in mind that some risks, typically operational in nature, are unavoidable, no matter the controls or safeguards in place.	Organizations may choose to accept the risk of minor power or internet service disruptions, especially if the clinical impact is low.

Balancing Effectiveness and Feasibility

After outlining possible risk responses, the next critical step is carefully evaluating the alternatives. The process, well-documented in NIST standards, revolves around two principle considerations: effectiveness and feasibility.

Effectiveness: Prioritizing Impactful Responses

Effectiveness concerns how well the proposed risk response strategy or control achieves the desired outcome in mitigating the risk. The goal is not merely to add more layers of security but to strengthen the resilience of the organization's defenses meaningfully. Considering the depth and breadth of controls ensures that enhancements contribute genuinely to the organization's risk posture.

Feasibility: Reasonable & Practical Application

Feasibility is a subjective measurement of how practical and achievable the implementation of a response is, given the organization's unique constraints and context. For healthcare organizations, any change or introduction of new security measures must be conscientiously weighed against potential disruptions to patient care and clinical operations. It's crucial to find a balance that maintains security without hindering care delivery.

There was a time when operational convenience might trump security considerations, illustrated by practices such as sharing passwords for ease of access. The healthcare industry, among others, has evolved to recognize the critical importance of securing sensitive information far beyond such rudimentary measures. What once seemed operationally efficient is now considered fundamentally flawed in safeguarding data security and patient privacy.

Holistic Decision-Making

Evaluating alternatives demands a holistic approach. Decision makers must balance the scales between the effectiveness of risk response and its feasibility across various dimensions, always optimizing security while maximizing essential clinical workflows. Balancing security and ongoing operations requires a nuanced understanding of the technological landscape and the healthcare environment on which these decisions have the greatest impact.

Managing cybersecurity risks requires a careful evaluation of risk treatment options. Organizations should consider the treatment's effectiveness in mitigating threats, the associated costs, and its feasibility for implementation.

A treatment's effectiveness is paramount. Highly effective and impactful treatments (controls) offer strong protection against potential threats and vulnerabilities, while ineffective controls may leave your organization exposed to additional risk or waste resources.

Cost is another factor. Organizations must consider the financial impact of implementing, maintaining, and updating controls. Organizations must strike a balance between effectiveness and affordability.

Finally, the feasibility of risk treatments should be considered. Controls must be reasonably deployed with a manageable level of disruption to existing systems and workflows. In other words, highly feasible controls can be readily integrated.

Clearwater's IRM|Analysis® software leverages a five-point scale to assess control effectiveness and feasibility. The tool allows organizations to make informed decisions based on their specific needs and constraints.

Evaluating Risk Treatment Options

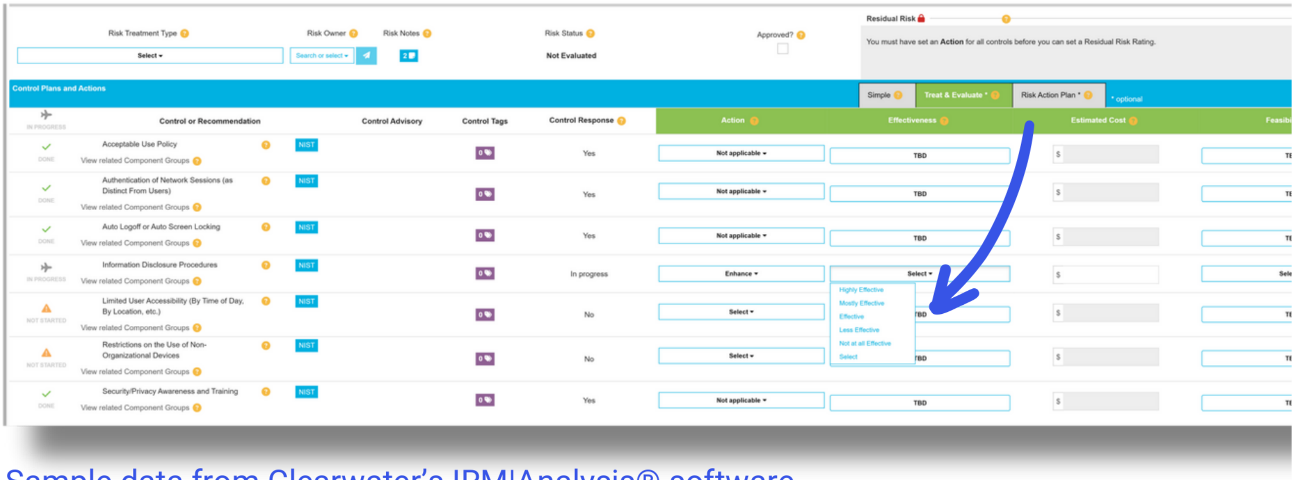
Once all feasible risk treatment options have been evaluated, the next step is to approve the most effective course of action. During this step, it is essential to determine and document a residual risk rating, representing the anticipated risk level present after implementing the chosen controls and risk response strategies. For example, if the initial risk rating is 16 out of 25, business owner(s), information security, and other relevant stakeholders should determine what the risk should be once the proposed controls are implemented. Ultimately, the goal is to bring the residual risk rating within the organization's risk appetite and below its risk threshold.

Business owners should participate in the decision-making process as they need to be acutely aware of the risks relevant to their respective information systems and business processes. For example, the Director of Health Information Management should be aware of the risks associated with the coding and billing platforms.

Organizations often lack proper communication channels between information technology and business operations, leading to a perception that information risk is solely an IT and Information Security Responsibility. Information risk management is a business function at its core, as the business must provide products and services to its customers, even in the event of technical disruptions. Consequently, the business must participate and take ownership of the risks associated with their respective areas and be actively involved in the risk management process. By ensuring business owners are informed about the risks and are involved in the decision-making process for addressing those risks, organizations can foster a culture of shared responsibility and accountability.

> Risk Mitigation is typically the preferred starting point for lowering risks at or above threshold. Organizations should prioritize implementing safeguards and controls that are reasonable, feasible, and likely to have the greatest impact.

Evaluating Alternatives: Risk Mitigation Example



Risk Treatment Type: Select ▾

Risk Owner: Search or select ▾

Risk Notes: 2

Risk Status: Not Evaluated

Approved? □

Residual Risk

You must have set an **Action** for all controls before you can set a Residual Risk Rating.

Control Plans and Actions

Simple | Treat & Evaluate * | Risk Action Plan * | * optional

	Control or Recommendation	Control Advisory	Control Tags	Control Response	Action	Effectiveness	Estimated Cost	Feasibi
✓ DONE	Acceptable Use Policy View related Component Groups	NIST	0	Yes	Not applicable ▾	TBD	$	T
✓ DONE	Authentication of Network Sessions (as Distinct From Users) View related Component Groups	NIST	0	Yes	Not applicable ▾	TBD	$	T
✓ DONE	Auto Logoff or Auto Screen Locking View related Component Groups	NIST	0	Yes	Not applicable ▾	TBD	$	T
IN PROGRESS	Information Disclosure Procedures View related Component Groups	NIST	0	In progress	Enhance ▾	Select ▾	$	Sele
NOT STARTED	Limited User Accessibility (By Time of Day, By Location, etc.) View related Component Groups	NIST	0	No	Select ▾	TBD	$	T
NOT STARTED	Restrictions on the Use of Non-Organizational Devices View related Component Groups	NIST	0	No	Select ▾	TBD	$	T
✓ DONE	Security/Privacy Awareness and Training View related Component Groups	NIST	0	Yes	Not applicable ▾	TBD	$	T

Sample data from Clearwater's IRM|Analysis® software

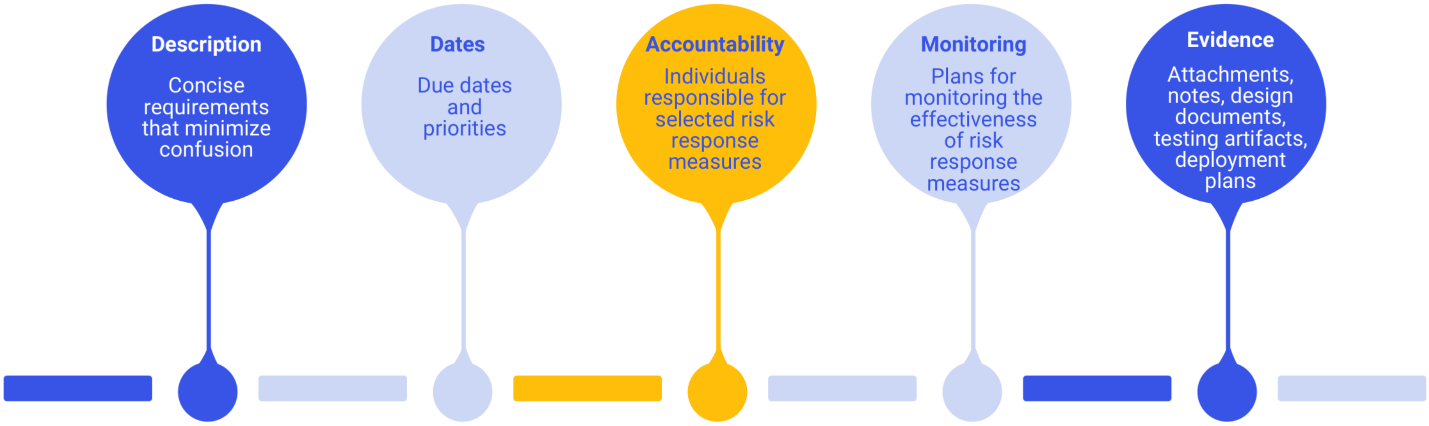
Implementing Risk Response: A Plan for Action

To be successful, risk management requires robust governance. Comprehensive implementation plans are vital and include clearly understood requirements, measurable outcomes, and defined accountability to maximize risk reduction.

As a general rule of thumb, well-documented implementation plans should contain:

- Specific details of controls to be added or enhanced
- Mechanisms for monitoring the effectiveness of the risk response
- Clear timelines and priorities
- Assigned roles and responsibilities
- Risk and issues tracking

Implementation Planning



Description
Concise requirements that minimize confusion

Dates
Due dates and priorities

Accountability
Individuals responsible for selected risk response measures

Monitoring
Plans for monitoring the effectiveness of risk response measures

Evidence
Attachments, notes, design documents, testing artifacts, deployment plans

Example: Untrained Staff

Consider the following risk scenario:

- Threat Source: System Cracker
- Threat Event: Social Engineering
- Vulnerability: Untrained/Untested Staff

To mitigate this risk, we may consider implementing a plan with the following structure:

Risk Owner: Human Resources
Project Manager: John Doe
Open Risks or Issues: Nothing Significant to Report

Priority 1: Improve or update security and awareness training

- Control: Security/Privacy Awareness Training
- Action: Enhance
- Implementation Manager: Information Security & Talent Management
- Due Date: 03/31/2024 (Q1)

Priority 2: Deploy targeted phishing campaigns

- Control: Targeted phishing campaigns
- Action: Add
- Implementation Manager: Information Security
- Due: 06/30/2024 (Q2)

Priority 3: Improve audit trail collections and review cadences

- Control: Audit trail collections and cadences
- Action: Enhance
- Implementation Manager: Application Analysts
- Due: 09/30/2024 (Q3)

Priority 4: Validate, refine, and update information disclosure procedures and sanctions policies

- Control: Information disclosure procedures and sanctions policies
- Action: Enhance
- Implementation Manager: Legal, Privacy, and Compliance
- Due: 12/31/2024 (Q4)

Organizations can systematically address vulnerabilities over time by treating risk response actions as distinct projects with clearly defined outcomes.

The Final Stage: Risk Reconciliation

Following the execution of your risk action plans, risk reconciliation is the final critical step in the risk management lifecycle. It involves a nuanced assessment, often not explicitly detailed in standards but crucial for effective risk management.

After implementing the selected controls, you might expect to reduce the risk to a residual level, say a 9 on a scale from 1 to 25, comfortably below your threshold of 12. However, the unpredictable nature of the implementation process and external factors means the anticipated outcome might not always align with reality. Not all planned controls may be deployed as expected, leading to deviations between projected and actual risk levels.

Risk reconciliation addresses this gap between prediction and reality. It involves revisiting the risk register to update and evaluate the residual risk based on the effectiveness of the implemented controls.

For example, if a risk analyst initially assessed a risk at 16 (on a scale from 1 to 25), predicted it would reduce to 9 after a series of implemented controls, and, upon implementation, verified that the risk should actually decrease to a 6.

Risk Reconciliation supports an accurate, current view of the organization’s risk profile, allowing you to:

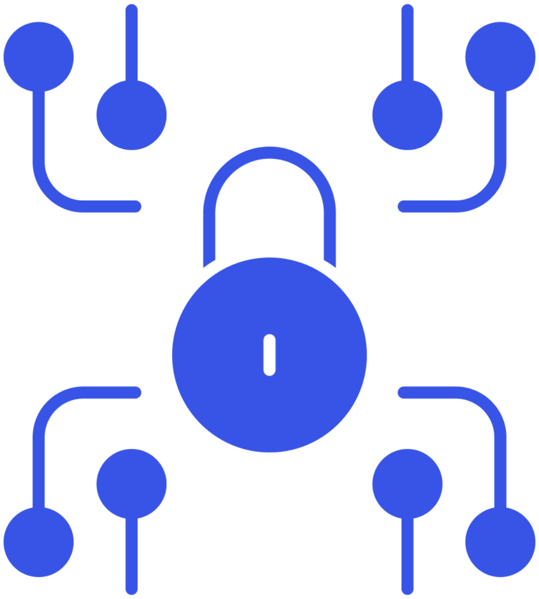
- Confirm that implemented controls have effectively reduced the risk to the intended level.
- Adjust your risk management strategies based on the actual outcomes observed.
- Account for changing threats and vulnerabilities

The process of reconciliation is essential for maintaining the integrity and accuracy of your risk management efforts, ensuring that your organization's risk posture accurately reflects the current state of affairs.

Conclusion: Navigating Your Risk Management Journey

As we conclude our exploration from risk analysis to risk reduction, here are pivotal insights to guide your risk management endeavors:

- Respond to All Risks Above Threshold: Every risk warrants a response; acceptance is a strategic choice when aligned with your organization's risk appetite and overall strategy.
- Diversify Risk Strategies: Beyond mitigation, consider risk avoidance and transfer as potent responses. Remember, avoiding a risk can often be as effective as confronting it directly. Also, consider that risk treatment options can be combined.



- Analysis Over Checklists: Effective risk management is grounded in thorough risk analysis, not merely adhering to checklists or compliance requirements. An in-depth analysis reveals specific threats and vulnerabilities and informs targeted responses.
- Guided Decision Making: Understanding your high-risk scenarios is just the start. Assess multiple treatment options, considering the balance between effectiveness, feasibility, cost, and labor requirements. Let effectiveness, feasibility, and cost principles influence your risk response decisions.

Implementing a disciplined risk management process is a complex but crucial endeavor that requires diligent project management and oversight. Specialized software, like Clearwater's IRM|Analysis®, can provide structured and automated guidance, enhancing your understanding of risk and facilitating appropriate management action.