Clearwater

Whitepaper

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

Table of Contents

Introduction

In the wake of the COVID-19 pandemic, healthcare organizations have seen a large percentage of their workforce start working remotely while many providers have begun seeing patients remotely as well. This shift has created new threats and vulnerabilities that potentially can hinder an organization from fulfilling its mission.

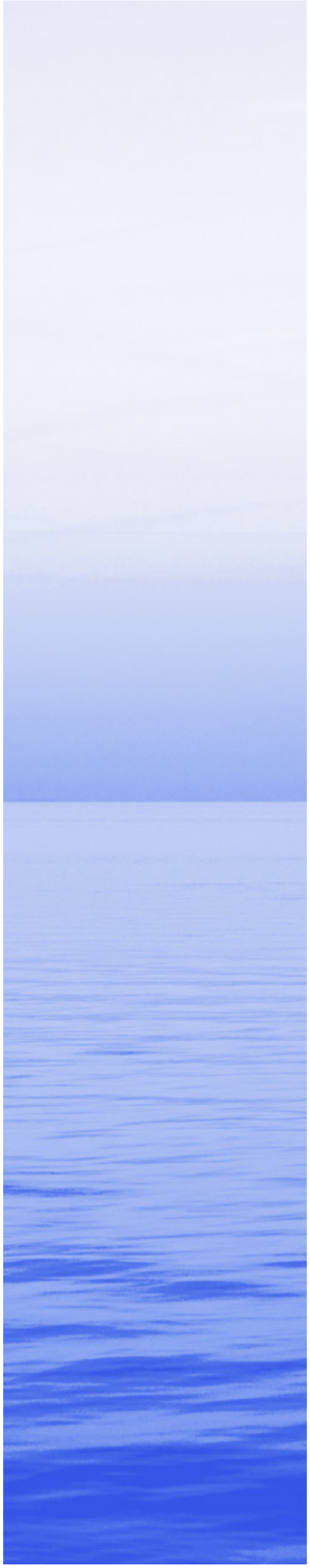
The HIPAA Security Rule maintains that a risk analysis must be performed as new systems and technologies are implemented, or there are any material environmental changes. The new systems and processes should be analyzed to ensure patient data is reasonably and appropriately protected and existing security measures are reasonable and appropriate to protect against the risks associated with evolving threats and vulnerabilities.

But from both a regulatory and a security perspective, it’s not enough to simply perform a risk analysis. The HIPAA Security Rule requires and today’s rapidly evolving threat landscape demands that organizations respond to the risks identified appropriately and effectively.

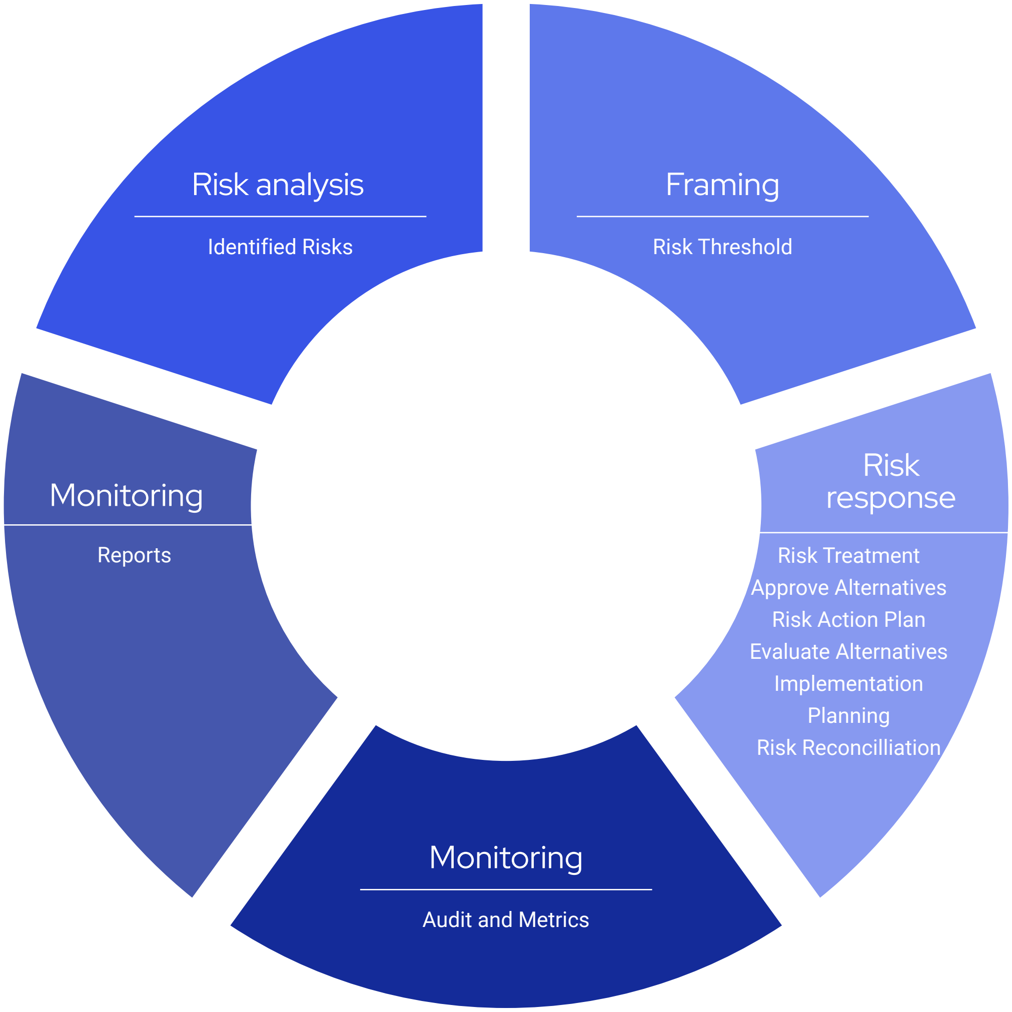
It’s not about throwing some new control – whatever is hot on the Internet, some response to ransomware – at the problem. The problem is broader than that. Cyber risk management involves identifying threats and vulnerabilities and knowing what your risks are so you can invest wisely in responding to them.

And in the unfortunate event of an Office for Civil Rights (OCR) investigation, they will be looking for evidence that the organization has implemented security measures to appropriately respond to the threats and vulnerabilities identified in the risk analysis according to the risk rating, and that such security measures are sufficient to reduce identified risks to an acceptable level.

OCR is going to want to see that there’s rigor applied in your risk management plan, and they’re going to want to see documented evidence of it. It’s very hard to put that together after the fact. We’ve seen that with organizations scrambling to find evidence to document the controls they’ve got in place. So rather than scrambling and having ten days sometimes to respond to an OCR letter, we strongly recommend that you have an ongoing risk response process.



Information risk lifecycle



Determine your risk threshold

Before getting into what constitutes an effective risk response process, let's pause for a moment and ask a question. Do all risks require a response?

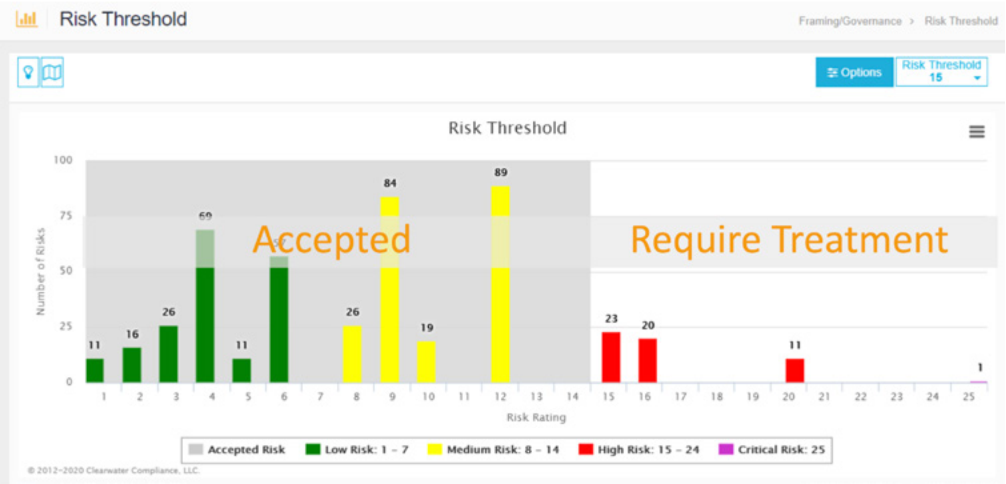
Well, not every risk requires an action. If you rate risk on a scale of 1 to 25, and upon evaluating a risk, you find it has a rating of three, that risk doesn't necessarily need mitigation. That's a less critical risk and you have bigger fish to fry, as they might say. But all risks do need a response.

Risk response requires setting your risk threshold and understanding your risk appetite. It requires real risk analysis as a foundation. Risk response is about informed decision making.

Having a thoughtful process of documenting what your risk threshold is, is very useful for two reasons. One, it shows that you're using your security dollars thoughtfully, on the basis of a real analytical process. Number two, it shows that you have a governance process in place and you are giving thought to what is the right level of risk for your organization.

We have often talked to organizations, and they say, "We've got the risk register. We've got all these risks. There's no way we can possibly address all these." You don't address all of them. That's really not a thoughtful, wise approach. But documenting what is the level you're going to accept risk at and what is the level of risk you're going to require treatment at is setting your risk threshold. That's a thoughtful governance and cyber risk management approach.

It's not a decision that should be made by an engineer in the bowels of the IT organization. It should be made by those who have ownership of security and privacy for the organization.



Sample data from Clearwater's IRM|Analysis® software

Understand your response options

Once the risk threshold is determined and risks are analyzed, what are the options for effective risk response? As we just described, risk acceptance is the appropriate risk response when the identified risk is within the organization's risk tolerance. But you shouldn't just accept the risk and not document it. Documenting that you've accepted a risk and it's within your tolerance is the complete and effective response.

Risk avoidance is a very valid option, and it involves taking specific actions to eliminate the activities or technologies that are the basis for the risk. If a particular laptop, for example, is a source of risk because it's out of date, the recommended risk response would be to decommission the laptop and get some new ones.

With transfer, it shifts the risk liability from one organization to another, for example, using insurance. But keep in mind that while insurance offsets the financial impact of a risk, it does not offset all of the impacts of a risk and it's only a partial way of treating risk. Responses can be done in combination. You might decide to mitigate and transfer at the same time. That's not unusual.

Risk mitigation is the response we typically think of when discussing how to manage risk. If you can't accept the risk and you can't avoid it and you can't transfer it, then you need to take some action to mitigate the risk by applying appropriate controls.

Evaluate the alternatives

Having defined our risk response options, let's turn our attention to evaluating alternatives and consider what that means. When you look at the NIST standards, they outline two key ways of evaluating alternatives.

The first is in terms of effectiveness, the expected effectiveness in achieving the desired risk response. It may include building in additional controls beyond what you currently have or increasing the strength of an existing control, enhancing what you've got rather than adding new.

You balance effectiveness with feasibility, the anticipated feasibility of the implementation.Cost is the obvious thing that comes to mind when you're looking at a new control or an enhanced control, but don't forget the mission, legal, technical and operational considerations. Undoubtedly, for those of us in healthcare, we're all very aware of the fact that sometimes new controls can affect the clinical workflow, and those impacts on the clinical workflow – doctors, nurses, and the work they're doing – are an important consideration. But it can't be the only consideration.

Organizations used to say we can't share passwords, so we have to tape the password to the laptop on the screen of the laptop so whomever walks up knows the password and can use the laptop. We've all begun to realize that that's no longer a viable way of maintaining and safeguarding sensitive data. It was really easy from an operational perspective, but not very effective from a security standpoint.

Make an informed decision

Let's now go into a little more detailed example on risk mitigation. We're going to look at a risk for laptops again. Laptops are the gateway to your claim payment system, your electronic health record system, and other systems that contain protected health information. There's a looming threat of system crackers and social engineering, and there's a potential vulnerability around untrained, untested staff.

What are we going to do from a risk response perspective about this risk? At a significant risk rating in our risk register, there are a whole number of options we could look at. You could think about things like access logging, information disclosure procedures, log aggregation analysis, security and privacy awareness training, and social engineering testing – all are really good safeguards for this particular vulnerability.

We did a risk analysis. We looked at those controls and we determined that a number of them, in this case for this particular asset, were not in place. Access logging was not in place. Log aggregation analysis was not in place. The next steps are to look at the various controls and consider should I be adding these, should I be enhancing these? Which of these things should I be doing?

Risk response identification

Risk acceptance

Risk acceptance is the appropriate risk response when the identified risk is within the organizational risk tolerance.

NIST SP 800-39, pg. 42

Risk mitigation

Risk mitigation, or risk reduction, is the appropriate risk response for that portion of risk that cannot be accepted, avoided, shared, or transferred, (e.g., adding or enhancing controls or safeguards).

NIST SP 800-39, pg. 42

Risk avoidance

Risk avoidance involves taking specific actions to eliminate the activities or technologies that are the basis for the risk … to avoid the potential for unacceptable risk.

NIST SP 800-39, pg. 42

Risk transfer

Risk transfer shifts the risk liability from one organization to another organization (e.g., using insurance to transfer risk from particular organizations to insurance companies).

NIST SP 800-39, pg. 43

For each of the controls, you want to think about effectiveness, cost, and feasibility. Within our IRM|Analysis® software, we use a five-point scale rating the control from highly effective all the way through not at all effective. We evaluate feasibility on a five-point scale as well. It's also important to document the costs for each of the controls.

All of these things help you determine what is a good course of action for reducing this risk. Something might be rather expensive and you can't do it this year, but there are some things you can do. You're not forced into the response of, "I've got to do all of them." Doing all of them is not very practical in most cases. Doing none of them shows a lack of diligence. But selecting from these alternatives based on an informed understanding of effectiveness and feasibility and cost, that's a thoughtful approach that anyone reviewing your risk management program most certainly will appreciate.

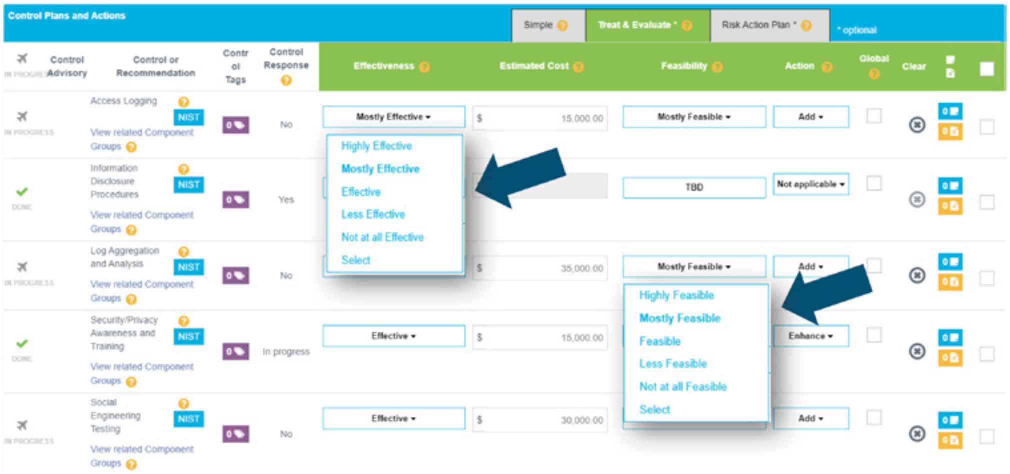
Approve the alternatives

Once you've selected a risk treatment type, the next step is approving the alternatives. What does this mean? This hearkens back to the key elements of the net risk response process we reviewed earlier. You need to document a residual risk rating. Say, the risk rating was at 16. What's it going to be now once I've put these controls in place? What's my residual risk rating likely to be? Again, the goal is to get it within the organization's risk tolerance, within the risk threshold.

If we go back to the example for laptops and clinical laptops and for untrained, untested staff, we talked about the fact that we were going to add various actions. We were going to enhance various actions, where you may make some investments. Somebody needs to approve those steps that are being taken.

> Risk mitigation is the response we typically think of when discussing how to manage risk. If you can't accept the risk and you can't avoid it and you can't transfer it, then you need to take some action to mitigate the risk by applying appropriate controls.

Evaluate alternatives: risk mitigation example



Control Advisory	Control or Recommendation	Control Tags	Control Response	Effectiveness	Estimated Cost	Feasibility	Action	Global	Clear
IN PROGRESS	Access Logging NIST View related Component Groups	0	No	Mostly Effective	$ 15,000.00	Mostly Feasible	Add	□	⊗
✓ DONE	Information Disclosure Procedures NIST View related Component Groups	0	Yes			TBD	Not applicable	□	⊗
IN PROGRESS	Log Aggregation and Analysis NIST View related Component Groups	0	No		$ 35,000.00	Mostly Feasible	Add	□	⊗
✓ DONE	Security/Privacy Awareness and Training NIST View related Component Groups	0	In progress	Effective	$ 15,000.00		Enhance	□	⊗
IN PROGRESS	Social Engineering Testing NIST View related Component Groups	0	No	Effective	$ 30,000.00		Add	□	⊗

Sample data from Clearwater's IRM|Analysis® software

Theoretically, this approval should be done by the business owner who owns the risk. They should be informed of the risks that are in the risk register like your director of health information management and your EHR, for example, would be informed about the risk on the risk register that is relevant to that information system.

Often times, organizations don't have this type of communication between technology and business owners, and information risk is seen as strictly an IT problem. But from day one, the message needs to be that information risk management is a business problem. When something goes wrong, it's the business that's actually providing the products and services to customers, not IT, and the business needs to own the risk.

Implement the risk response

Information risk management requires strong governance, as we've discussed, but it's also a project management activity that demands strong implementation planning to ensure risks are treated as intended. It has the characteristics of any good project management plan, concise and well-described requirements that minimize confusion describing what's going to be done if you're adding or enhancing a control. Plans for monitoring the effectiveness of risk response measures are also critically important. Good planning involves establishing due dates and setting priority as well as defining accountability for implementing the selected risk response measures. Documenting the implementation plan on paper is very helpful in the event of an investigation but it also helps keep everyone on the project team on the same page.

Let’s examine implementation planning for untrained, untested staff, a risk that we spoke about earlier. How do we put together a proper plan for this vulnerability, for this particular system? We want to initiate risk response activities as projects. Three different controls or recommendations are going to be taken – access logging, information disclosure procedures, and log aggregation and analysis. We’ll review one of those, access logging, to show the type of information you’re going to want to document in your project plan.

First, we want to describe your action here. What are you actually implementing? What do we mean by access logging? In security, these words can mean different things to different people, so you want a description. A detailed business requirement around this control is even better, but at a minimum, describe what we mean by access logging. You’ll need a plan for monitoring effectiveness. This is the hook into the next step of the information risk management lifecycle. Any time you document a control and what’s going to be implemented, it should have control objectives that ensure it is being effective. If it fails, we know why it’s failing and when it’s failing. Attaching a due date and a responsible party are important to this effort as well.

Implementation planning

Description Concise and well described requirements that minimize confusion

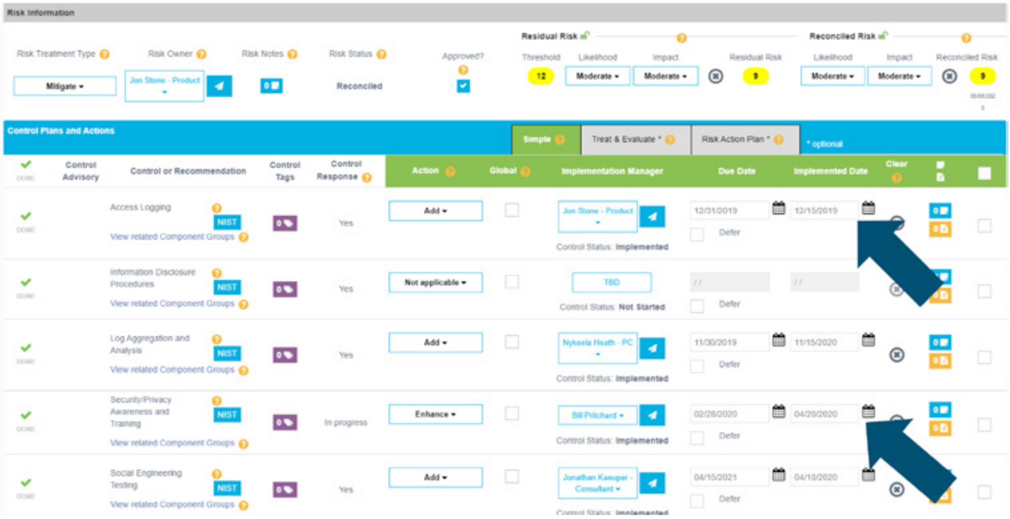
Dates Due dates and priority

Accountability Individuals responsible for the selected risk response measures

Monitoring Plans for monitoring the effectiveness of risk response measures

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

Risk reconciliation



Risk Information

					Residual Risk				Reconciled Risk		
Risk Treatment Type	Risk Owner	Risk Notes	Risk Status	Approved?	Threshold	Likelihood	Impact	Residual Risk	Likelihood	Impact	Reconciled Risk
Mitigate ▾	Jon Stone - Product ▾	0	Reconciled	☑	12	Moderate ▾	Moderate ▾	9	Moderate ▾	Moderate ▾	9

Control Plans and Actions

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

✓ DONE	Control Advisory	Control or Recommendation	Control Tags	Control Response	Action	Global	Implementation Manager	Due Date	Implemented Date	Clear		□
✓ DONE		Access Logging NIST View related Component Groups	0	Yes	Add ▾	□	Jon Stone - Product ▾ Control Status: Implemented	12/31/2019 □ Defer	12/15/2019		0 0	□
✓ DONE		Information Disclosure Procedures NIST View related Component Groups	0	Yes	Not applicable ▾	□	TBD Control Status: Not Started	/ / □ Defer	/ /			□
✓ DONE		Log Aggregation and Analysis NIST View related Component Groups	0	Yes	Add ▾	□	Nykeela Heath - PC ▾ Control Status: Implemented	11/30/2019 □ Defer	11/15/2020		0 0	□
✓ DONE		Security/Privacy Awareness and Training NIST View related Component Groups	0	In progress	Enhance ▾	□	Bill Pritchard ▾ Control Status: Implemented	02/28/2020 □ Defer	04/20/2020		0 0	□
✓ DONE		Social Engineering Testing NIST View related Component Groups	0	Yes	Add ▾	□	Jonathan Kaeuper - Consultant ▾ Control Status: Implemented	04/15/2021 □ Defer	04/10/2020			□

We need to monitor the plan which we like to call the risk action plan. Where possible, we want to take notes. What do we mean by taking notes about those things? There's an awful lot you can do just by documenting on a certain day who did what. The Agile Scrum approach is to document your accomplishments and your next steps. For each of your items, each of the controls that you're implementing, we recommend you document accomplishments, next steps, and date-time stamp that note. That way, any time you get back to that plan – say the plan got put down for three or four days or someone leaves and the next person comes along – if you have accomplishments and next steps, you're a long way to getting oriented back to that item that's being worked on. You can really drive a project forward with those minimal data elements.

Reconcile your risks

After you've completed your risk action plan, your risk response for the risk in question, comes the important step of risk reconciliation.

There is an interesting nuance that's not in the standards very clearly. If we implement our defined controls, we believe we're going to bring the risk to a 9 on a scale of 1 to 25. That's our residual risk rating. Our threshold was at a 12. Now, things happen. Maybe all of the controls we said we were going to implement, for example, when we set our residual risk rating, they didn't all get implemented. Maybe something got deferred, or all sorts of other changes can happen between the decision or the prediction of what the residual risk rating is going to be and how it'll actually affect the risk in the real world. That's why we recommend the idea of a reconciled risk.

Once we've made a predicted residual risk rating and done all the things we said we were going to do, what is the actual reconciled risk? We're going to go back to our risk register and say, "This risk was a 16 before. We said we were going to get it to a 9, and we actually got it to a 9." You'll select your reconciled risk on the same scale that we described earlier. Likelihood times impact equals reconciled risk.

Key points to remember

That gives us the full process, from risk analysis to risk reduction. Some key points to remember as you embark on your risk management journey:

1. All risks require a response. Sometimes acceptance is a very valid response depending on the organization's appetite for risk. It's not something to be embarrassed about if it's well documented.

2. Not all risks must be mitigated. Some can be avoided, some can be transferred. Avoidance is a really good risk response if you remember to think of it. Sometimes it gets forgotten in the risk response process.

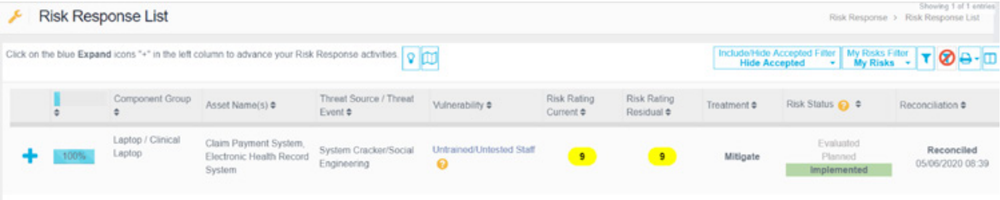
3. Risk response should be based on risk analysis and not checklists. There are a lot of risk checklists out there. Some of those can be very useful. But a checklist is not a risk analysis. It's missing those key elements of threats and vulnerabilities that help us calculate a risk rating. And what that risk rating does is it helps us focus our attention. It helps us focus our attention from the perspective of where we're going to invest this year. It helps show investigators if they knock on the door that we've been thoughtful and analytical in our process. If you do risk analysis at the level of the information system and you look at threats and vulnerabilities and controls, that's a good amount of rigor that can really stand the test.

4. A thoughtful evaluation of alternatives is a critical part of the process. You know what your high-risk rating is, but typically, there's more than one control that might mitigate the risk, that might reduce the risk rating. And you can document them. You can go as detailed as you want.

5. At a minimum, you want to think about effectiveness, feasibility, and cost to guide your decision-making process. It may even help you change your initial idea about how to respond to the risk.

Thoughtful and disciplined risk management often can be a challenge for organizations to implement. Strong project management to make sure your plans get implemented is key. A purpose-built software system like Clearwater's IRM|Analysis® can guide you through the process, helping you understand your risks and take the appropriate the steps to manage them.

From day one, the message needs to be that information risk management is a business problem. When something goes wrong, it's the business that's actually providing the products and services to customers, not IT, and the business needs to own the risk. Information risk management requires strong governance.


Risk Response List

Showing 1 of 1 entries

Risk Response > Risk Response List

Click on the blue **Expand** icons "+" in the left column to advance your Risk Response activities

		Component Group	Asset Name(s)	Threat Source / Threat Event	Vulnerability	Risk Rating Current	Risk Rating Residual	Treatment	Risk Status	Reconciliation
+	100%	Laptop / Clinical Laptop	Claim Payment System, Electronic Health Record System	System Cracker/Social Engineering	Untrained/Untested Staff	9	9	Mitigate	Evaluated Planned Implemented	Reconciled 05/06/2020 08:39

Sample data from Clearwater's IRM|Analysis® software

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