Risk Response

Develop a repeatable, sustainable process to manage your cyber risk

Risk response is part of an ongoing process of managing risks identified during risk analysis and a key step in the overall NIST Risk Management Process. Responding to risks in a methodological manner with adequate identification of owners, alternatives considered, documented decisions, and implementation planning is required under the HIPAA Security Rule.

Promoting Interoperability (formerly Meaningful Use) attestation also requires providers to implement security updates, as necessary, and correct identified security deficiencies as part of a risk management process.

Preparation

Our experts will help you form your Project Team, provide them with education materials and detail the entire Risk Response process. We will work with your team to train them to use the Risk Response module in our IRM|Analysis™ software.

Onsite Response

During the onsite Risk Response WorkShop we facilitate a detailed response plan for each risk in scope of the engagement.

Reports

Our software will dynamically create a compliance dashboard, detailed list of all compliance gaps, and full remediation plan. In addition, we will prepare a Risk Response Summary Report to help you prioritize your next steps.

Ongoing Support

As part of our community of software customers, you can enjoy excellent concierge customer support, monthly Customer Council meetings and a dedicated help center.

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Risk Response

Be Clear
De-mystify a complex process by using a by-the-book approach and obtain management approval of a risk response process and procedure

Be Confident
Utilize a proven approach and methodology used by thousands of organizations

Be Thorough
For all risks exceeding your risk threshold, evaluate alternatives, associated costs and, effectiveness

Be an Informed Decision Maker
Readily identify security investments providing the highest ROI by reducing high-ranked and/or multiple risks

Be On-Record
Document alternatives considered and decisions made to provide evidence of good faith effort

Become Self-Sufficient
Your team will learn a repeatable, sustainable process to manage your information security risks

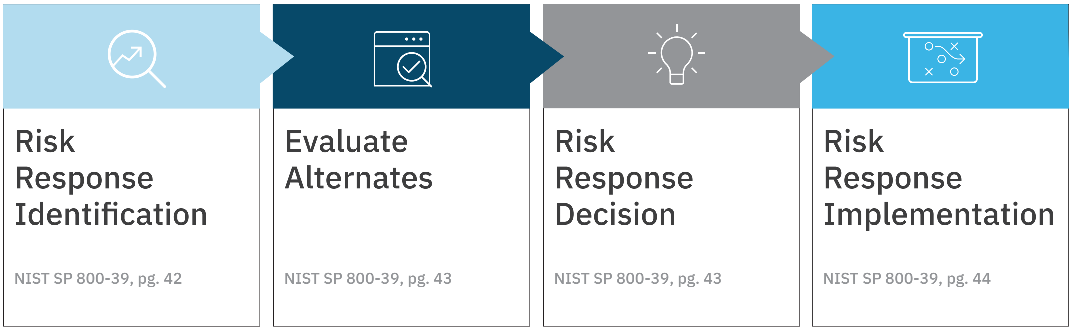
BEST IN KLAS CYBERSECURITY ADVISORY SERVICES 2018

2018 Best in KLAS designation
Cybersecurity Advisory Services

BLACK BOOK 2019

2017, 2018 and 2019 Black Book Marketing Research Awards
Compliance and Risk Management

The Risk Response Process Begins With Understanding Your Risk Threshold



Risk Response Identification
NIST SP 800-39, pg. 42

Evaluate Alternates
NIST SP 800-39, pg. 43

Risk Response Decision
NIST SP 800-39, pg. 43

Risk Response Implementation
NIST SP 800-39, pg. 44

Go beyond risk analysis and take action to address risks

> *"Clearwater understood our needs and our challenges, and, in addition to ensuring the completion of our risk analysis, trained our team to be self-sufficient in conducting our next risk analysis and how to approach our risk treatment priorities."*
>
> — Andrea Thomas-Lloyd
> MBA, RHIA, CISSP, CHPS
> Information Protection & Assurance,
> Lancaster General Health
> (now part of Penn Medicine)

Clearwater's software and consulting services enable organizations to make more informed risk treatment decisions (i.e., accept, avoid, mitigate or transfer), respond to risks faster and to mitigate them more efficiently. Once risk levels have been established, customers can review each of the risks rated above their risk appetite and respond accordingly with action plans to implement mitigating controls. This may entail using the software's workflow and collaboration tools to create action plans and assign them to stakeholders along with implementation dates.

See what Clearwater can do for you.

800-704-3394
clearwatercompliance.com

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT