Session I of V | August 12, 2026 @ 11am CT

Risk Analysis Fundamentals: OCR Expectations, Enforcement Trends, and Introduction to IRM|Analysis

Central Time	Instructional Module	Learning Objectives Attendees Will Be Able To:	Clearwater Presenter	Supplemental Material (in addition to presentation slides)
11:00am	Risk Analysis Fundamentals	• Explain the purpose of the Working Lab Series • Explain what a Risk Analysis is, and what it is not • Describe fundamental problem we are trying to solve and Risk Analysis Dilemma	**Nykeeia Heath**| Senior Principal Consultant **Marie Lange** | Client Technology & Training Specialist	1.1 Guidance on Risk Analysis Requirements under the HIPAA Security Rule 1.2 NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments 1.3 NIST SP800-39-final_Managing Information Security Risk 1.4 NIST SP800-37_rev.2, Risk Management Framework for Information Security and Organizations: A System Life Cycle Approach for Security & Privacy 1.5 Blog: Steps Every Healthcare Organization Can Take to Ensure an OCR-Compliant Risk Analysis 1.6 Blog: HIPAA Security Rule Enforcement: Where Things Stand in 2026
11:20am	Introduction to IRM|Analysis	• View Initial Demonstration of IRM|Analysis software • Identify key features and benefits of IRM|Analysis and understand how the use of IRM|Analysis helps to ensure the completion of an OCR-Quality® Risk Analysis (Clearwater Risk Algorithm, CES, 9-Key Components)		
11:40am	Course Participation Requirements	• Explain attendee responsibilities and objectives of each session		
11:45am	Your IRM|Analysis Account	• Describe the features and functionality available on all Clearwater Software screens.		

After Session Self-Study: Each attendee will be given access to the IRM|Analysis software and encouraged to explore features and functions, view the support areas such as Notifications, Risk Management Map and Healthcare Entity.

Session II of V | August 19, 2026 @ 11am CT

IRM|Analysis Workflow Phase 1: Building a Complete ePHI Information Asset Inventory

Central Time	Instructional Module	Learning Objectives Attendees Will Be Able To:	Clearwater Presenter	Supplemental Material (in addition to presentation slides)
11:00am 11:10am	Self-Study Review Physical Locations & Information Systems/Assets	• Clarify why and how Physical Locations are used • Create New Physical Locations within IRM|Analysis • Explain what an Information System is, and what it is not • Add New Information Assets within IRM|Analysis • Discuss Asset Import Tool	**Nykeeia Heath**| Senior Principal Consultant **Marie Lange**	Client Technology & Training Specialist	2.1 The Clearwater Definition of an Information Asset
11:35am	Introduction to Components	• Define Components • Describe different Component types (e.g., Software, Hardware, Networks, etc.) and add appropriate Components to an Information Asset • Demonstrate how different Component types affect the Clearwater Risk Algorithm		

After Session Self-Study: After this meeting, each attendee will be tasked with creating two Physical Locations and producing an asset inventory (with a minimum of 2 assets using the Application Component type).

Session III of V | August 26, 2026 @ 11am CT

IRM|Analysis Workflow Phase 1: Identifying Current Threats, Vulnerabilities, and Component-Level Risks

Central Time	Instructional Module	Learning Objectives Attendees Will Be Able To:	Clearwater Presenter	Supplemental Material (in addition to presentation slides)
11:00am 11:15am	Self-Study Review Component Expert System	• Explain benefits of grouping systems by threat surface • Demonstrate how new Component Groups can be created in the Component Groups page • Show how different Component Groups can be created using the Asset Grouping Expert • Describe the pros and cons of using a "Master Infrastructure" Asset for common Components versus selecting every relevant Component for each Asset • Copying Risk Determination Information	**Nykeeia Heath**| Senior Principal Consultant **Marie Lange** | Client Technology & Training Specialist	

After Session Self-Study: After this meeting, each attendee will be tasked with creating at least two different Application Component groups and selecting appropriate Properties for each group.

Session IV of V | September 2, 2026 @ 11am CT

IRM|Analysis Workflow Phase 2: Defensible Risk Determination — Likelihood, Impact, and Risk Scoring

Central Time	Instructional Module	Learning Objectives Attendees Will Be Able To:	Clearwater Presenter	Supplemental Material (in addition to presentation slides)
11:00am 11:15am	Self-Study Review Controls/Global	• Explain how NIST Methodology is used to create Clearwater safeguards • Respond to Clearwater Controls, both globally (default) and at the Component Group level – understanding the difference and use case • Realize the importance of documentation during a Risk Analysis (Control Notes) and uploading supporting Documents • Demonstrate the use of Quick Filters and the Filter Dialog	**Nykeeia Heath**| Senior Principal Consultant **Marie Lange** | Client Technology & Training Specialist	4.1 NIST: Updated Security & Privacy Controls Guidance for Information Systems & Organizations
11:30am	Risk Questionnaire List / Form Pages	• View Risk Scenarios / Threat & Vulnerability Combinations associated with Component Groups • Understand how Control Responses and notes can affect Risk Rating • Define difference in Risk Likelihood and Risk Impact • Calculate Risk Ratings and value the importance of Risk Notes • Introduction to Predictive Risk Rating		

After Session Self-Study: After this meeting, each attendee will be tasked with completing a Risk Analysis for one Component Group.

Session V of V | September 9, 2026 @ 11am CT

IRM|Analysis Workflow Phase 3: Reports, Dashboards, Risk Register Outputs, and Risk Response Planning

Central Time	Instructional Module	Learning Objectives Attendees Will Be Able To:	Clearwater Presenter	Supplemental Material (in addition to presentation slides)
11:00am 11:15am 11:30am 11:40am 11:50am	Self-Study Review Reports Version History Dashboards Introduction to OneView	• View Reports and Enterprise Extracts within IRM|Analysis and discuss importance of each • Understand the importance of routine re-assessments • View Cyber-Security Intelligence Dashboards within IRM|Analysis and discuss importance of each • What is a Finding? • Comprehend how to create and import new findings • Discuss the steps of assigning activities to findings and using Activities Manager to track progress of issues	**Nykeeia Heath**| Senior Principal Consultant **Marie Lange**	Client Technology & Training Specialist	5.1 White Paper: From Risk Analysis To Risk Reduction: A Step-By-Step Approach 5.2 Article: Driving Real Cyber Risk Reduction in Healthcare 5.3 Self Review: Clearwater HIPAA Security Risk Analysis Self-Review