Cyber Assurance in Healthcare: Insights from HITRUST and Clearwater

May 22, 2024

Clearwater | HITRUST

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- If you’d like to follow along with today’s presentation a link to the deck has been shared in the chat.
- Recording and slides shared via email within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Today’s Speakers

Ryan Patrick

Vice President, Adoption
HITRUST

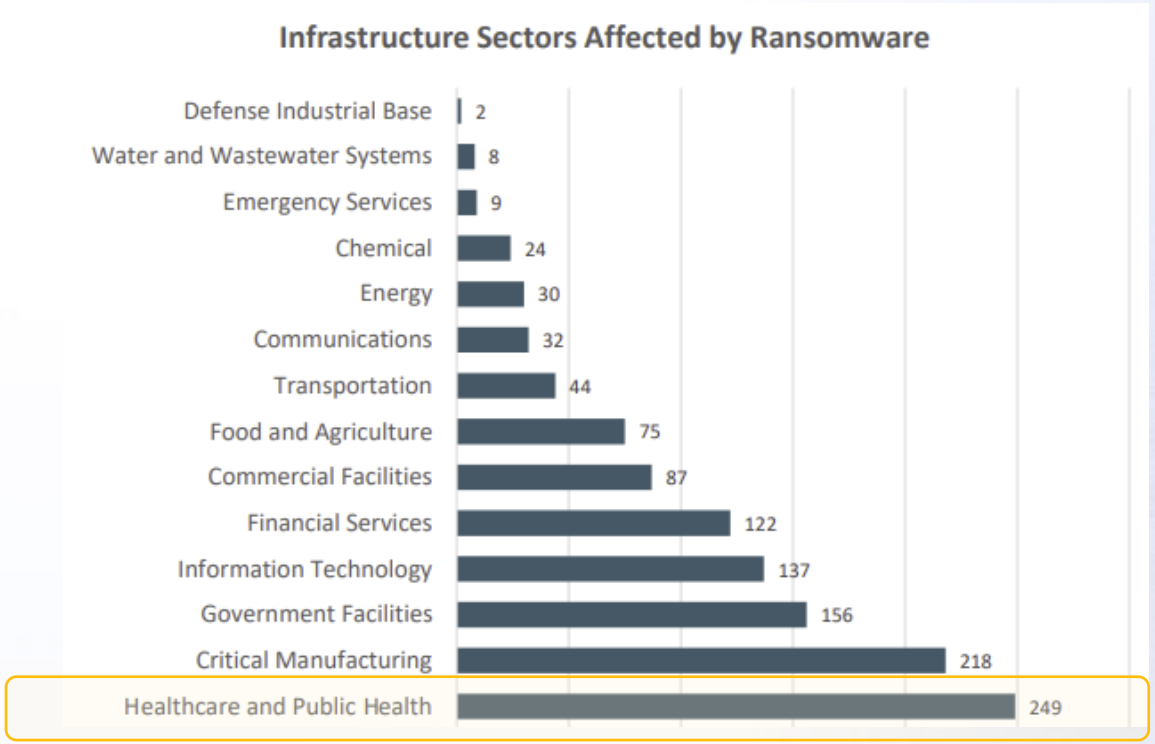
Steve Meyer, CCSP, CHQP

Director, Consulting Services – Auditing & Certification Solutions
Clearwater

Agenda

- The need for greater cyber assurance in healthcare
- How HITRUST helps address that need
  - What's new in HITRUST 11.3
- Why organizations choose to become HITRUST validated/certified
- The HITRUST certification process

Ransomware Threat Continues to Increase



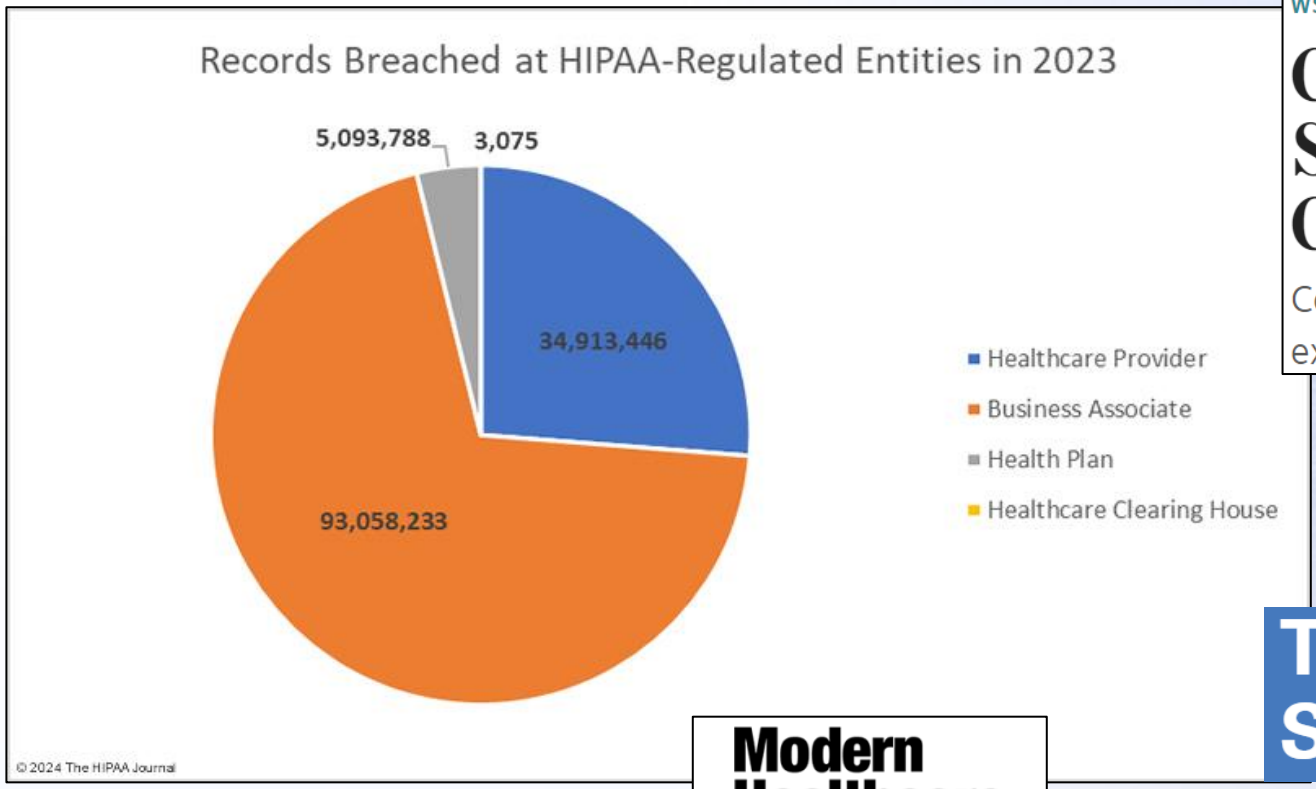
- 95% increase in Ransomware in 2023[1]
- 13% Increase in Insurance Claims – increase primarily driven by ransomware 2023[2]
- Healthcare is the most targeted critical infrastructure industry by ransomware gangs[3]
- Total losses from internet crime increased in the U.S. by 22% in 2023 to $12.5 Billion[3]
- 20% increase in reported victims in Q1 2024 vs Q1 2023[4]

[1] *At Least 141 Were Hospitals Directly Affected by Ransomware Attacks in 2023 (hipaajournal.com)*
[2] *Ransomware triggers cyberinsurance claims increase | SC Media (scmagazine.com)*
[3] *2023 FBI Internet Crime Report.pdf*
[4] *GuidePoint Security Q1 2024 Ransomware Report*

Clearwater

Scrutiny of Vendor Cybersecurity Practices Increasing

"Securing the supply chain is one of the biggest cybersecurity challenges in healthcare."



WSJ PRO

Companies Take a Closer Look at Supply Chains After Recent Cyberattacks

Corporate security executives beef up supplier oversight following extensive supply-chain attacks

American Hospital Association™

Advancing Health in America

Third-Party, Cyber-Risk Skyrockets for Health Systems

Modern Healthcare

Healthcare vendors are the new front of the cybersecurity war

Clearwater

Health3PT Aims to Advance Accountability

Health3PT

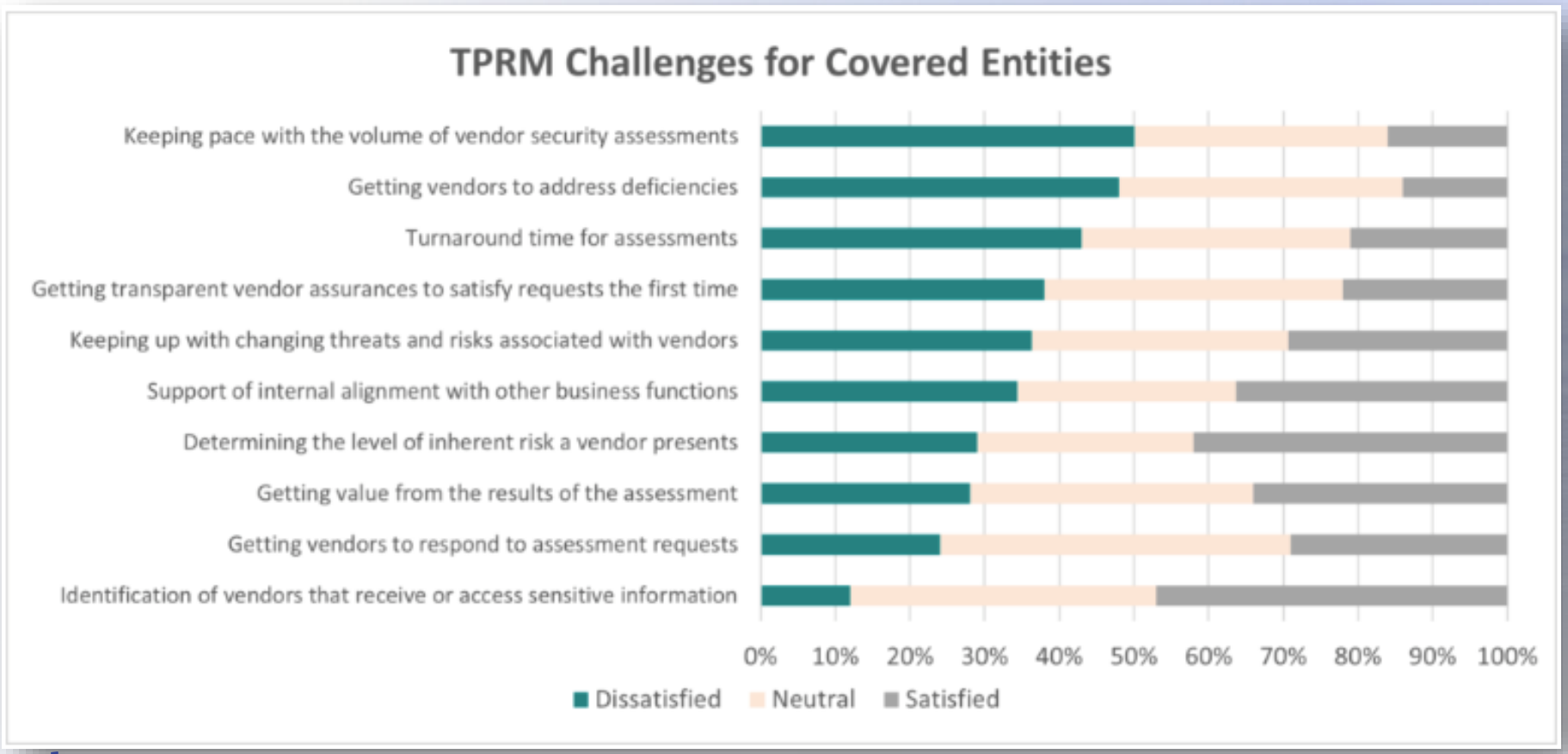
What are the Mission Objectives of the Health3PT Initiative?

- Establish effective, consistent, repeatable programs for managing third-party service providers that require access to Protected Health Information (PHI) or Personally Identifiable Information (PII).
- Share knowledge and resources to further the Council's initiatives, programs, and outcomes.
- Hold our third-party service providers and each other accountable to these commitments to ensure that the shared objectives are met.
- Accept and encourage HITRUST Certification(s) from third-party service providers over other assessments, questionnaires, audits, or certification reports.

Clearwater

Common Third-Party Risk Challenges

- The 2023 Health3PT survey asked 59 covered entities about their top third-party risk management challenges.

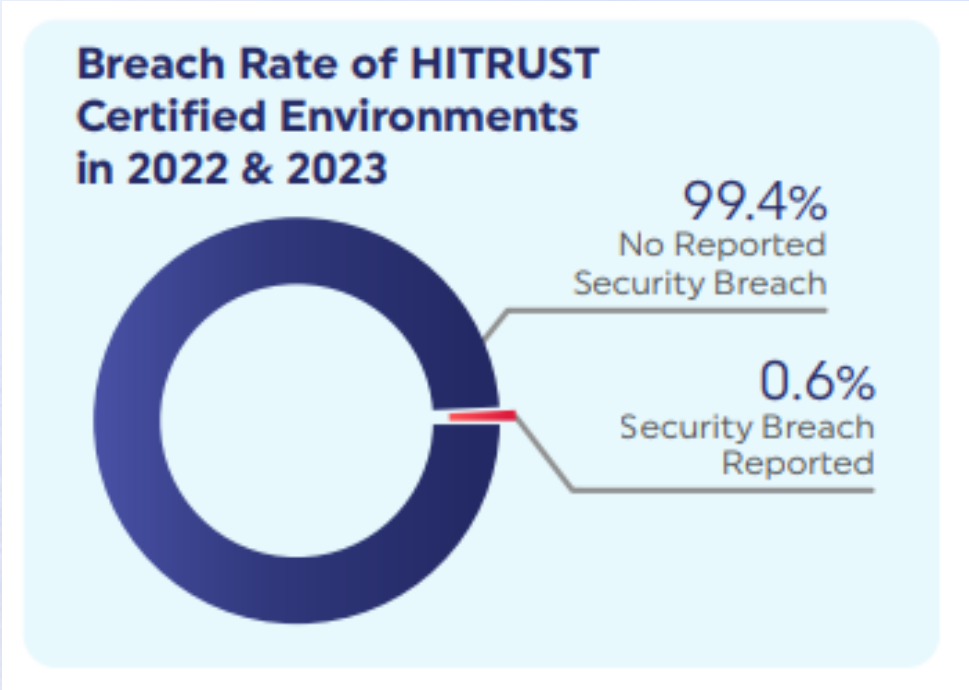


Clearwater

HITRUST: Built to Evolve for Enhanced Cyber Resilience

97%

Of all threat indicators in MITRE ATT&CK are covered in CSF versions 11.2 & 11.3.0



By aligning with HITRUST, organizations demonstrate a proactive and committed approach to privacy and security.

Clearwater

Assurances Over Other Frameworks

1

Start with a core of threat-adaptive controls

Supported by Cloud and AI Shared Responsibility Model

+

2

Optionally Include Other Authoritative Sources

- HIPAA Security Rule
- PHIPA
- GDPR
- NIST
- StateRAMP
- FedRAMP

=

3

HITRUST Issues Many Reports

Clearwater

What's New in CSF v11.30

- Addition of FedRAMP, StateRAMP, and TX-RAMP authoritative sources, which provide a standardized approach to ensure that assessed entities doing business with the government comply with applicable information security requirements.
- Integration of NIST SP 800-172: Enhancing protections for Controlled Unclassified Information (CUI) and supporting organizations with high-risk profiles in their HITRUST r2 Assessment tailoring.
- Foundation for CMMC Level 3 Requirements: Preparing organizations for new compliance needs based on stringent NIST standards.
- Inclusion of MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems (MITRE Atlas) Mitigations: Addressing security requirements crucial for safeguarding AI systems.
- **Streamlined Assessment Process: Reduced redundancy in requirement statements, significantly decreasing the average r2 assessment size without compromising control coverage.**

HITRUST Certification Options

- **HITRUST offers three certification options based on vendor needs, size, risk maturity, and business profile.**
- The HITRUST Essentials (e1) Validated Assessment is ideal for low-risk vendors seeking to establish basic foundational cybersecurity or more complex organizations looking to start their certification journey with plans to move into a more comprehensive certification level.
- The HITRUST Implemented (i1) Validated Assessment offers more coverage than the e1. It is suited for third-party vendors demonstrating leading security practices.
- The HITRUST Risk-Based (r2) Validated Assessment is its most comprehensive assurance. It is considered the gold standard in the industry and is ideal for high-risk vendors.
- **Each level is built on a common framework. This means you can begin with a lower-level assessment and move up to a higher level without losing the invested time, money, and effort.**

Assessment Options

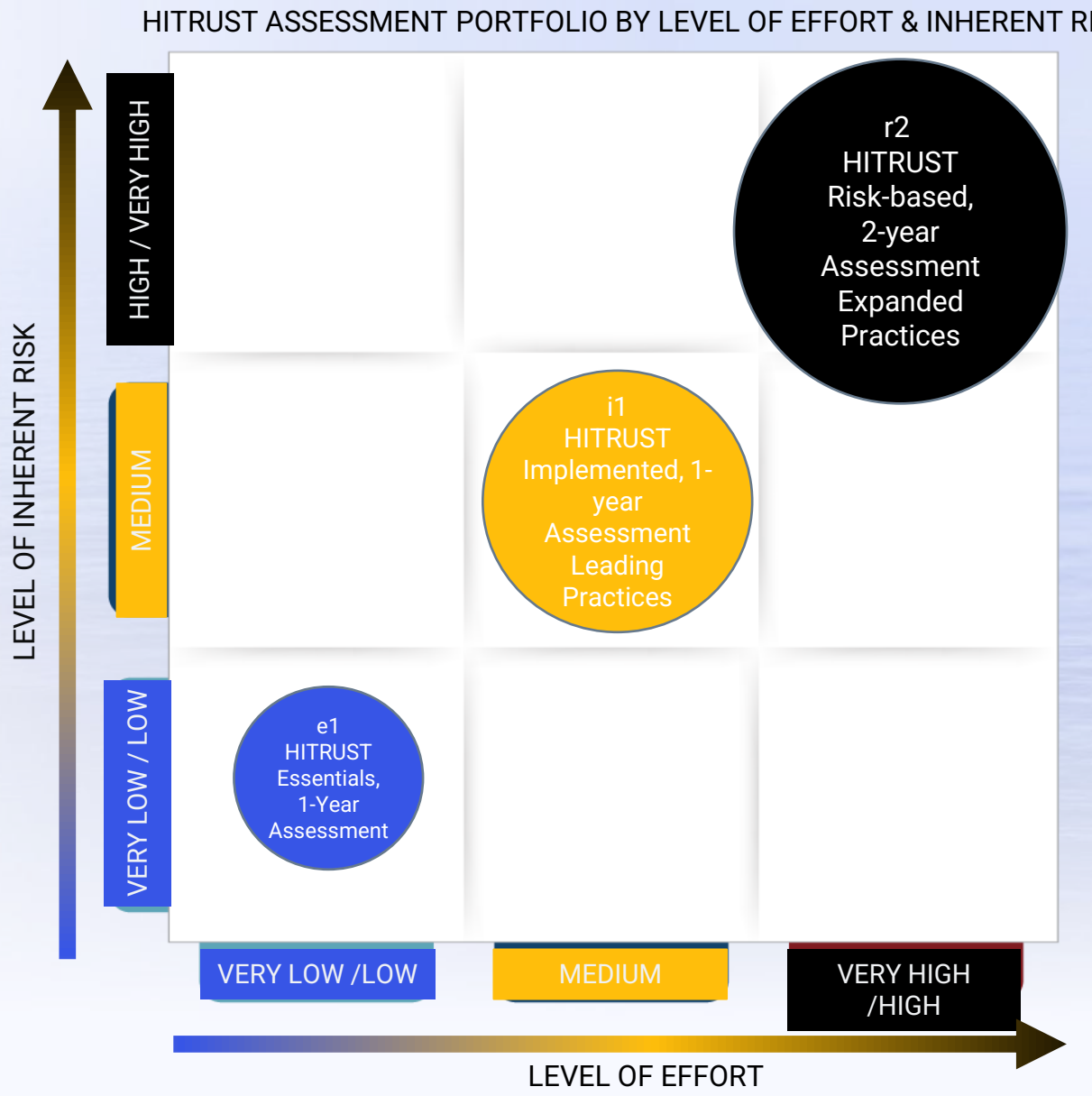
Clearwater

Assessment Options to Meet Every Level of Inherent Risk

Driven By Considerations of Purpose, Time, and Budget

Every HITRUST Assessment Report is Rely-Able™

- Transparency:
  - Leverages a publicly available and widely adopted control framework.
  - Control selection, evaluation, and scoring are clearly understood.
- Consistency:
  - Consistent results regardless of the assessor.
  - Can accurately gauge one organization's security posture with another.
- Accuracy:
  - Formula-driven determination of assessment results
  - Granular scoring and evaluation model
- Integrity:
  - All Validated Assessments receive HITRUST Quality Review.
  - 150 automated quality checks and 5 levels of independent and objective quality assurance reviews ensure transparency, consistency, and accuracy of results.

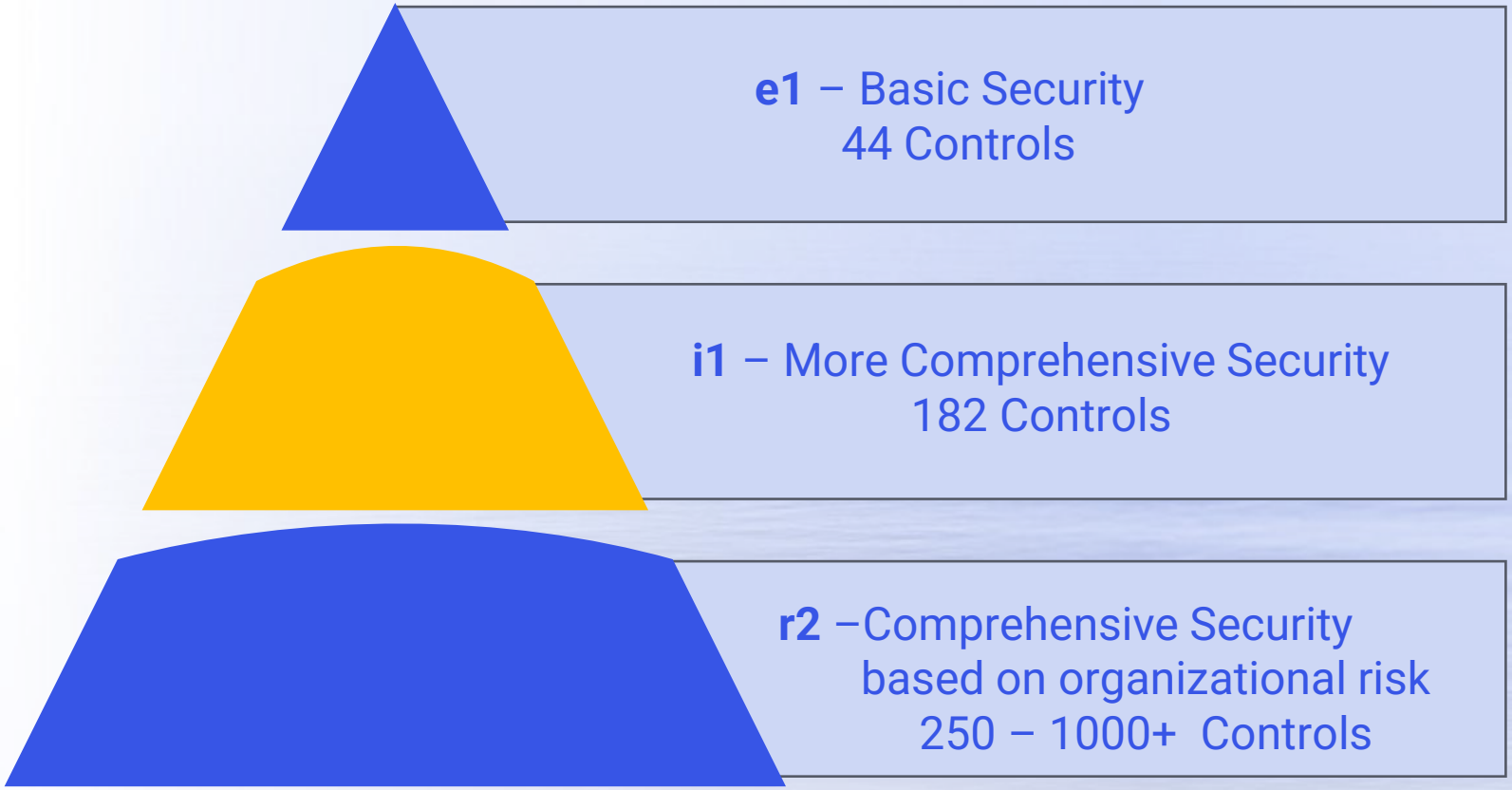


Clearwater

Assurance That Builds Based on Assessment

Maturity Level	Weight
Implemented	100%

Maturity Level	Weight
Policy	15%
Procedure	20%
Implemented	40%
Measured	10%
Managed	15%



	7 Levels of Assurance
1	Organization
2	Assessor
3	Assessor Organization QA
4	Assessment Check-in QA

	7 Levels of Assurance
5	HITRUST Assurance Team Review
6	HITRUST Quality Team Review
7	Board Level Quality Subcommittee (sampled)

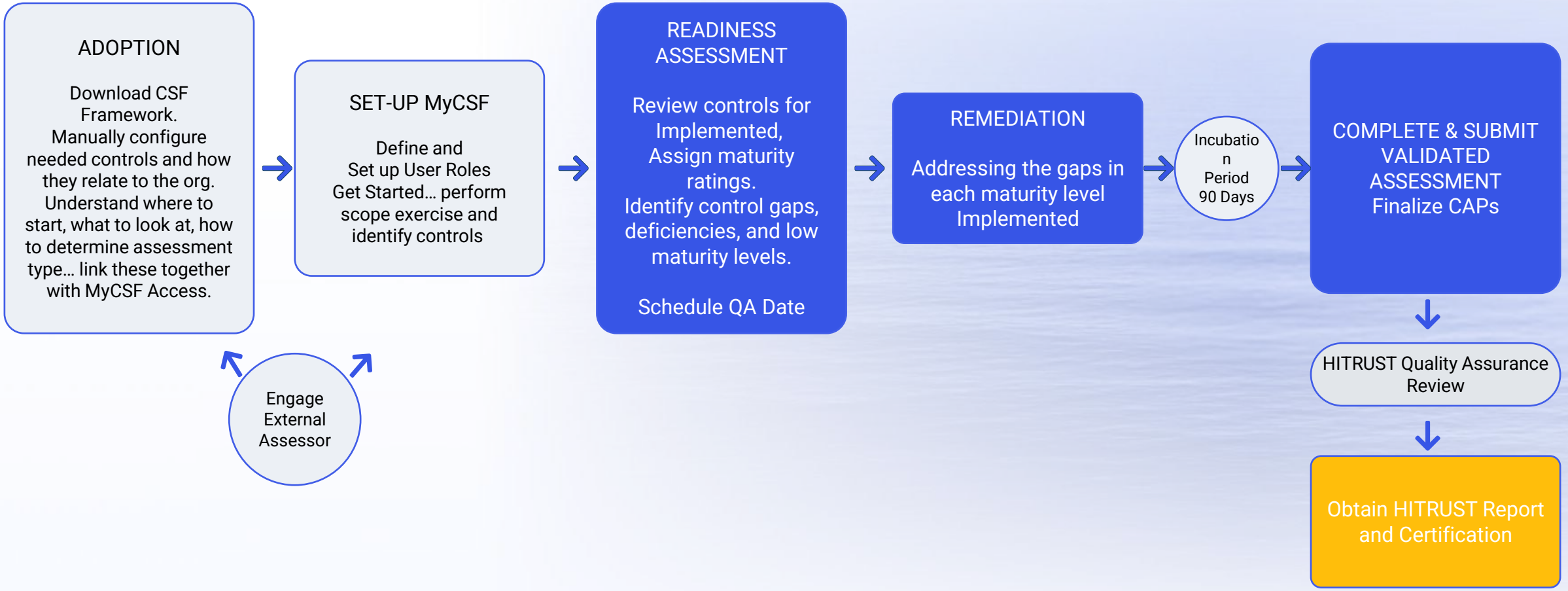
Clearwater

Top 5 HITRUST Needs

HITRUST®

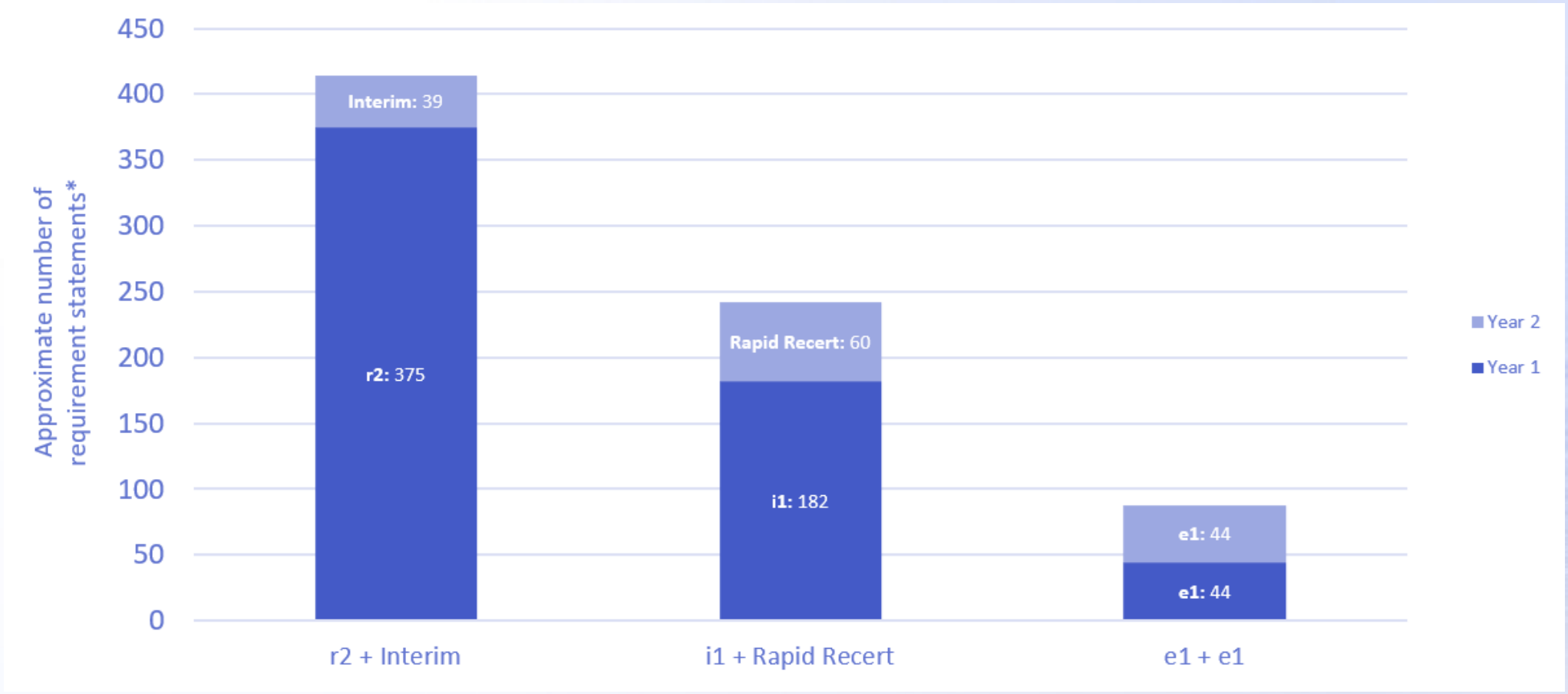
Clearwater

HITRUST Certification Journey



Clearwater

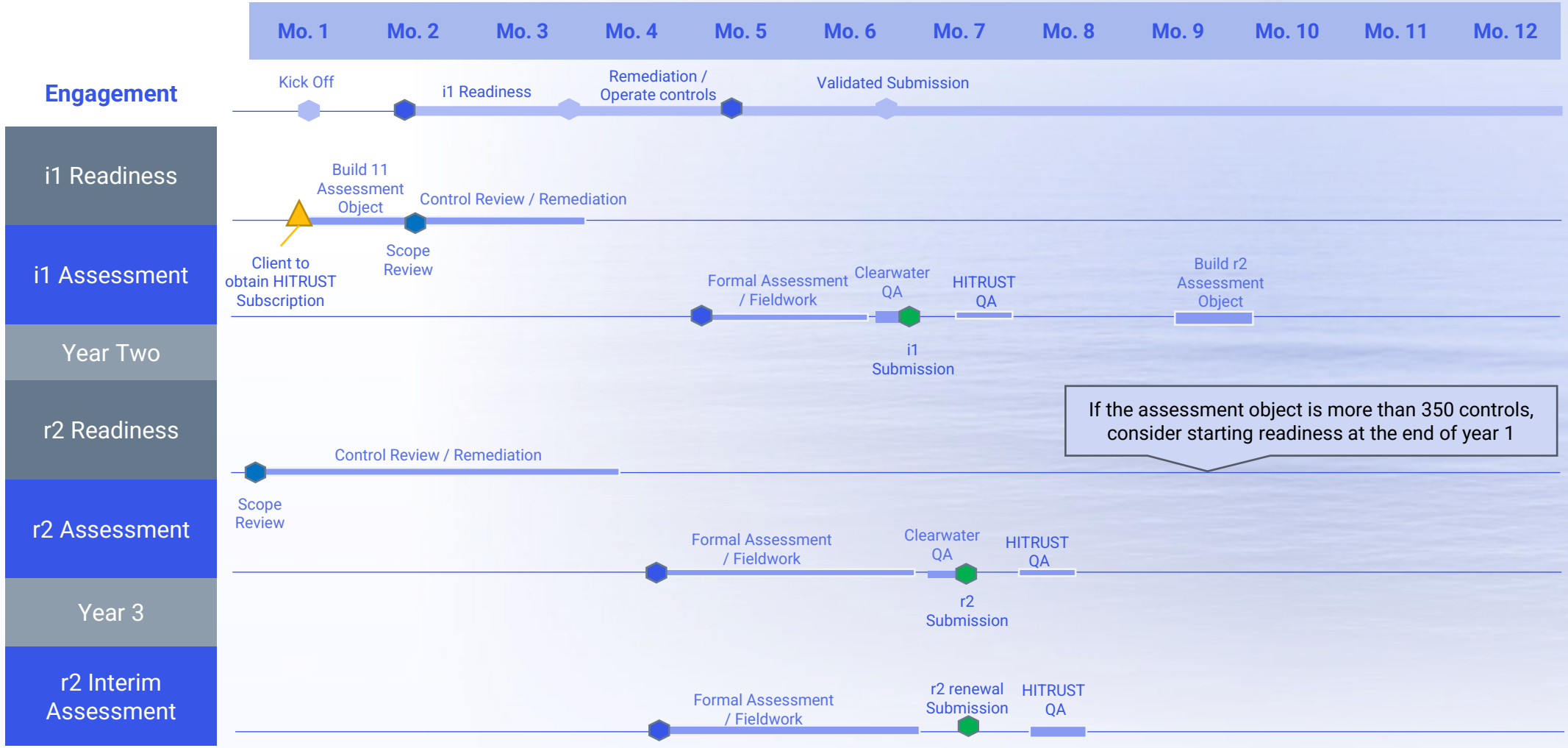
Illustrative Examples of Two-Year Count of Requirement Statements



*r2: Average number of requirement statements based on data for v9.1 – 9.6 r2 Assessments submitted to HITRUST; Interim: Average number of requirement statements based on data for v9.1 – 9.6 r2 Assessments submitted to HITRUST; i1: Number of requirement statements within the i1 Assessment using v11; Rapid Recert: Projected number of requirement statement within the i1 Rapid Recertification Assessment

Clearwater

Sample Engagement Timeline (i1 → r2)



Clearwater

Engagement Process

Pre-Kickoff | Kickoff | Working Sessions | Deployment | Validation | Assessments | Final Reports

- **Pre-Assessment Working sessions** – Control Review Client and Assessor Firm
- **Deployment** – Client Operates Controls and puts changes in place.
- **Validation** – Answer any final questions and review new items implemented from the pre-assessment working sessions.
- **Assessment** – Formal HITRUST Validated Assessment
- **Final Reports** – Results of formal assessment

To Learn More

Clearwater

Blog

A Look at HITRUST Version 11: Everything You Need to Know

Blog

Preparing for HITRUST Certification: The How and Why for Healthcare Service Providers

Q&A

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Upcoming Events

June Cyber Briefing | June 6

Register here: Monthly Cyber Briefing - Clearwater (clearwatersecurity.com)

Digital Health Innovation Summit | June 5-6 - Boston

- Clearwater Digital Health team members are attending

Incident Response Webinar | June 20

- Partnering with 1st Responder and Jarrad Communications

Register here: Breach to Resolution: A Live Cyber Incident Response Tabletop for Healthcare Executives | June 20 @ 12:00 CST - Clearwater (clearwatersecurity.com)

Clearwater

Clearwater

Healthcare–Secure, Compliant, Resilient

www.clearwatersecurity.com

800.704.3394

info@clearwatersecurity.com

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.