Clearwater

Healthcare – Secure, Compliant, Resilient

Monthly Cyber Briefing

October 2023

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Cyber Briefings are eligible for HIMSS & CHIME CE credit
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Clearwater

Agenda

- Cyber update
- AI Risk Management Framework

Steve Cagle, MBA, HCISSP
CEO, Clearwater

David Bailey, EMBA, CISSP
VP, Consulting Services, Security

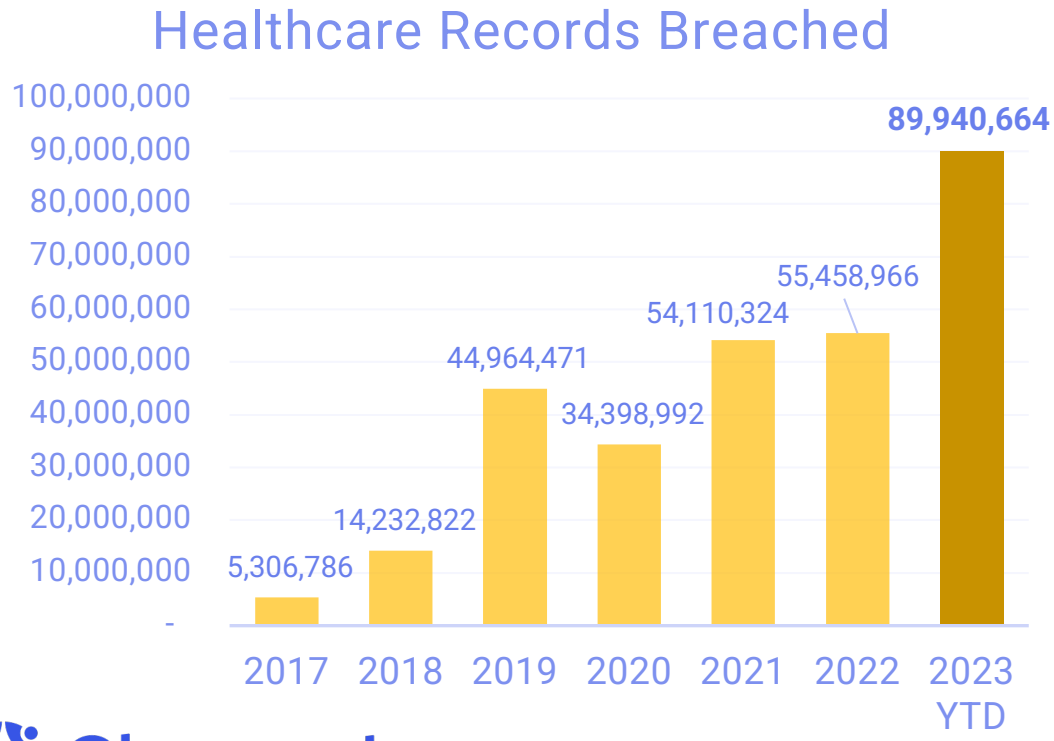
Clearwater

Cyber Update

Steve Cagle

Healthcare Breaches Increasing in Total Due to Size

~100 Million records reported breached in the Last 12 months Ending 9/30/23



- 21.5m records reported breached in July 2023
- 10.5m records reported breached in August 2023
- 3.6m records reported breached in September

2 Large Healthcare Breaches Reported in September 2023

Nuance Communications Notifies 1.2M Individuals of Data Breach

Stemming from the MOVEit vulnerability

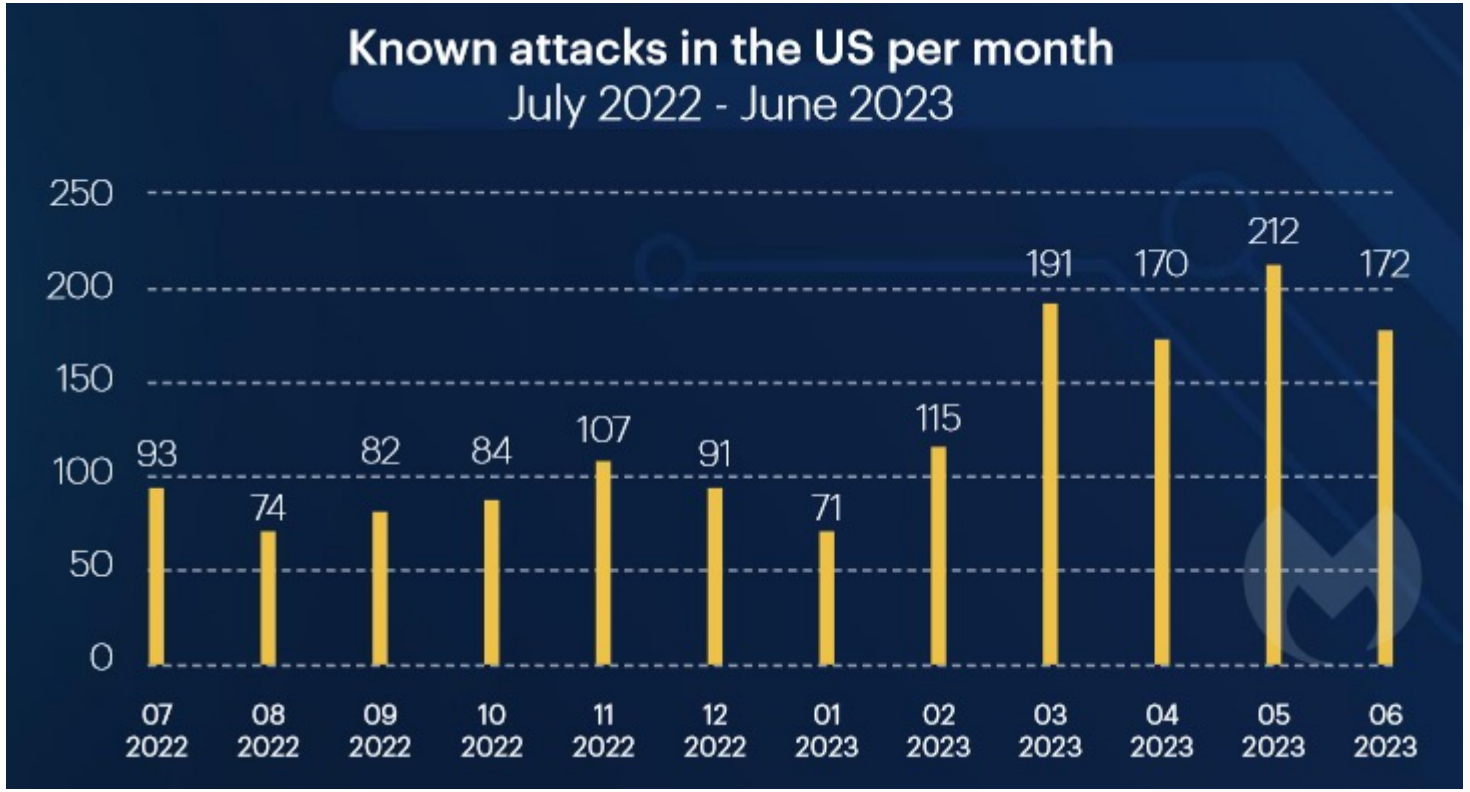
Virginia Department of Medical Assistance Services Files Another Notice of Data Breach with the Federal Government

Hacking / Network Server Incident

Clearwater

Source: HHS Breach Portal

State of Ransomware



Across all sectors

"Over the last 12 months, education and healthcare were the most beleaguered sectors in the US outside of services. They received so many attacks that if they were countries, they would be the fourth and sixth most attacked in the world."

Clearwater

2023 State of Ransomware Report - Malwarebytes

Recent Ransomware Attacks – BlackCat/ALPHV

MGM cyberattack claimed by ALPHV/BlackCat ransom gang

Caesars Entertainment Reportedly Pays Ransom to Attackers

Half of $30 Million Demand Paid to Same Group That Hit MGM Resorts, Reports Say

- Caesars – social engineering used to gain access via a third-party IT Services company
- MGM - vishing used to trick help desk employee into providing access
- Caesars paid ransom, though to be $30m
- MGM did not, down for 10 days

Large Michigan healthcare provider confirms ransomware attack

- Suspicious activity led to investigation and partial IT shutdown of 14 locations
- Claims to have stolen 6TB of data – 2.5m records

Previous notable healthcare victims include NextGen and Lehigh Valley, and Sun Pharmaceuticals

Clearwater

FBI Notification

[Link to FBI Notification]

Two or More Ransomware Variants Impacting the Same Victims and Data Destruction Trends

Summary

The Federal Bureau of Investigation (FBI) is releasing this Private Industry Notification to highlight emerging ransomware trends and encourage organizations to implement the recommendations in the “Mitigations” section to reduce the likelihood and impact of ransomware incidents.

Threat

As of July 2023, the FBI noted two trends emerging across the ransomware environment and is releasing this notification for industry awareness. These new trends included multiple ransomware attacks on the same victim in close date proximity and new data destruction tactics in ransomware attacks.

Clearwater

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Adopted in July of 2023 the Final Rule became effective on September 5, 2023.

Applies to SEC registered organizations.

Incident Reporting

- Beginning 12/18/23
- Disclosure of material cyber incidents on 8-K
- 4 days from determining a material incident
- “Materiality” must be determined “without delay”

Annual Reporting

- All fiscal year periods ending on or after 12/15/23
- Disclose risk management and governance information in relation to cybersecurity, including board proficiency and oversight of cybersecurity risks on 10-K

Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

New Threat Brief from HSC3

- Overview of Cybercrime, including different motivators
- Chinese Cyber Power strategy with deep dive into APT 41
- North Korea Cyber Power Strategy with deep Dive into APT 43 and APT 38 (Lazarus)
- Defenses & Mitigations

Clearwater

OCR Enforcement of HIPAA Security Rule Violations

HHS Office for Civil Rights Settles with L.A. Care Health Plan Over Potential HIPAA Security Rule Violations

The largest publicly operated health plan in the country paid $1,300,000 to settle

- Failure to Conduct Risk Analysis
- Failure to reduce risks to an acceptable level
- Failure to implement procedures to review of system activity
- Failure to conduct technical evaluations
- Failure to conduct nontechnical evaluations
- Failure to implement tools to review system activity

Link to OCR-LA County Resolution Agreement

This enforcement action follows other 2023 breach related settlements: Banner Health, MedEvolve, Yakima Valley

Clearwater

Recommendations Based on Current Threat Environment

- Perform vulnerability scans on an on-going basis. Remediate high and critical vulnerabilities rapidly. Employ virtual patching in the case that a patch is not available, or not practical to implement
- Update security awareness training to account for more sophisticated attack techniques including smishing and vishing
- Test your employees, contractors on their ability to detect a social engineering attack
- Conducting on-going risk analysis, technical testing and non-technical evaluations when changes occur
- Mitigate risk of third parties, by reducing access, minimizing data exposure, and assessing and responding to service provider and supply chain risks
- Ensure on-going monitoring of end-points and correlate data with logs and other sources, with automated escalation and disciplined process related to escalation and investigation
- Test your security controls through security controls validation assessment
- Develop and test incident response plans, including at the executive level

Resources

BlackCat/ALPHV

Also refer to Clearwater's June 2023 Cyber Briefing, where we discussed this threat actor

- Health Sector Cybersecurity Coordination Center Threat Briefing: Royal & BlackCat
- HHS "Indicators of Compromise" BlackCat/ALPHV 4/26/23
- Mandiant MITRE Brief, including IOCs, Detection Opportunities and MITRE ATT&CK Technique References

Social Engineering

- Health Sector Cybersecurity Coordination Center Analyst Note: Vishing Attacks on the Rise
- Health Sector Cybersecurity Coordination Center Threat Briefing: The Impact of Social Engineering on Healthcare 8/18/22
- Health Sector Cybersecurity Coordination Center Threat Brief: MFA & Smishing 8/10/23

AI Risk Management Framework (RMF)

Dave Bailey

Healthcare Organizations are Rushing to Adopt AI

98%

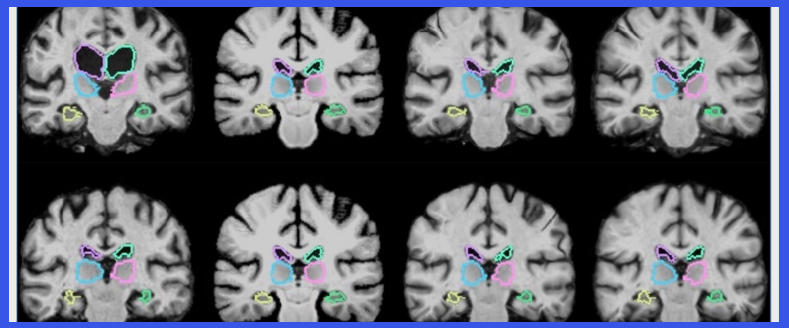
Of 500 surveyed healthcare leaders say their organization either has or is planning to implement an AI strategy, including 48% who implemented already – Optum

Reasons for AI Adoption:

- Easing administrative burden
- Improve patient outcomes with virtual care
- Reach equity goals
- Reduce Costs

Clearwater

Artificial intelligence (AI) technologies have significant potential to transform society and people's lives . . . However, [they] also pose risks that can negatively impact individuals, groups, organizations, communities, society, the environment and the planet. - NIST



- The GOOD

Medical Imaging Analysis and Machine Learning

- MIT researchers describe a machine-learning algorithm that can register brain scans and other 3-D images more than 1,000 more quickly using novel learning techniques.

The Impacts of Artificial Intelligence and Cybersecurity

- How AI is impacting Cyberthreats: Threat Actors are using AI for both designing and executing attacks
  - Development of phishing emails
  - Impersonation attacks
  - Rapid exploitation of vulnerabilities
  - Development of complex malware code
  - Deeper target reconnaissance
  - Automation of attacks
  - Overwhelming human defenses
  - Ransomware; wider spread and more evasive

Problem Domain

AI Risk Appetite

- Is there a reluctance or concern on the introduction of AI within the healthcare ecosystem?
- Does your organization have any guidance or boundaries around AI, i.e., ChatGPT?

AI Managed

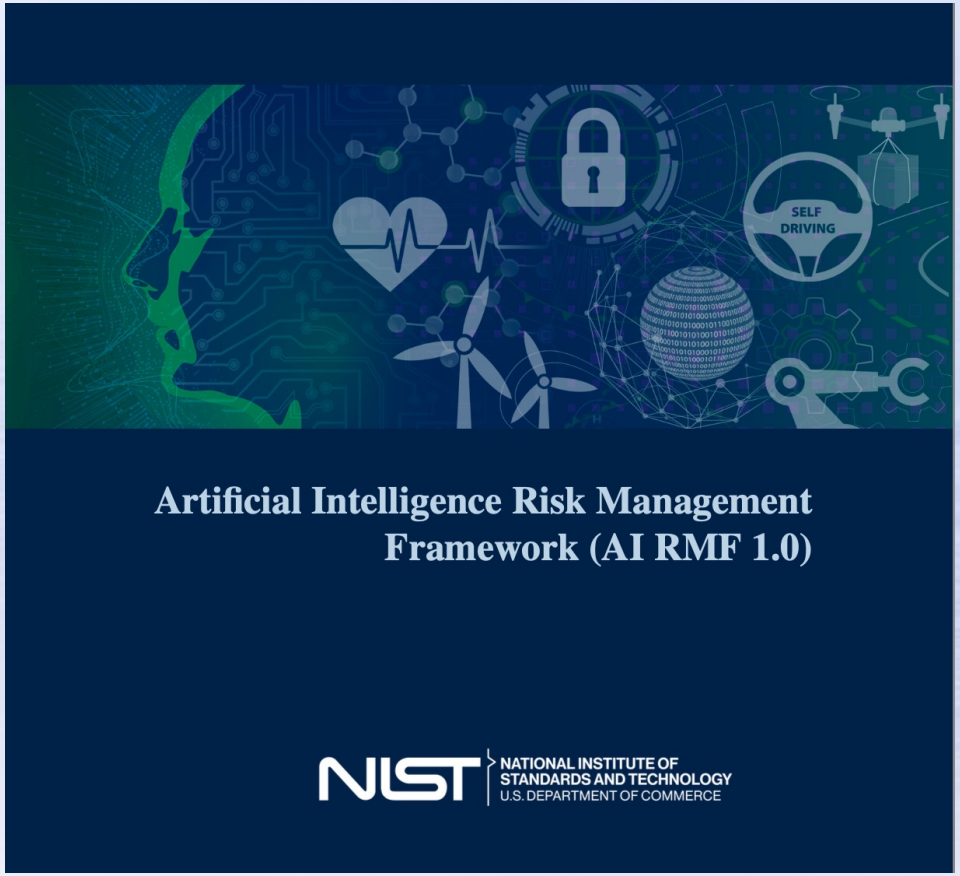
- Has any action been taken to define AI governance for the organization?
- Are teams or stakeholders established that are working from an established set of guiding principles?
- Are users made aware of the risks? Do they understand their obligations to safely and securely use AI?

Remaining Questions

- Is the organization developing any AI applications or systems?
- How is addressing AI integrated into existing processes (vendor risk, change management, quality control, data integrity, etc.,)?

AI Risk Management is Critical

- AI risk management is a key component of responsible development and use of AI systems
- Responsible AI practices can help align the decisions about AI design, development, acquisition and use with the intended aim and value

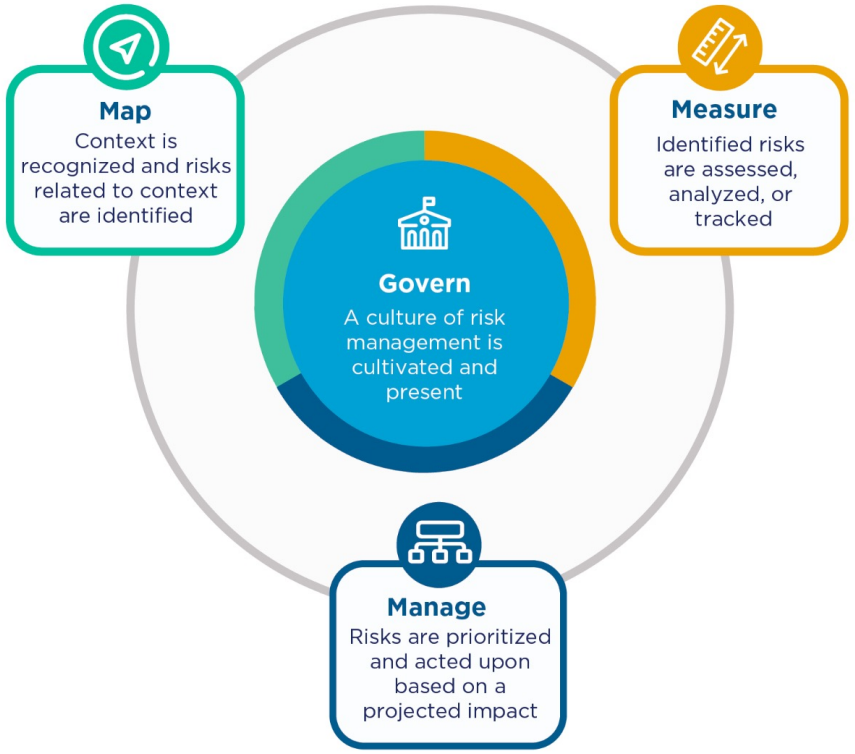


Understanding AI Risks

Harm to People	Harm to an Organization	Harm to an Ecosystem
• **Individual**: harm to a person's civil liberties, rights, **physical** or psychological safety, or economic opportunity • Group/Community: harm to a group such as discrimination against a population sub-group • Societal: harm to democratic participation or educational access	• Harm to an organization's **business operations** • Harm to an organization from **security breaches or monetary loss** • Harm to an organization's **reputation**	• Harm to interconnected and interdependent elements and resources • Harm to the global financial system, **supply chain**, or interrelated systems • Harm to natural resources, the environment, and planet

Align AI Practices to NIST AI RMF

- AI RMF Core
  - The Core consists of 4 Functions to organize AI risk management activities: **Govern**, **Map**, **Measure**, and **Manage**.
  - Governance is designed as a cross-cutting function to inform and infuse the other three functions.



Govern A culture of risk management is cultivated and present

Category	Description	Sub-Cat	Description
Govern 1	**Policies, processes, procedures, and practices across the organization related to the Mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.**	Govern 1-1	Legal and regulatory requirements involving AI are understood, managed, and documented.
		Govern 1-2	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.
		Govern 1-3	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.
		Govern 1-4	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.
		Govern 1-5	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned, and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.
		Govern 1-6	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.
		Govern 1-7	Processes and procedures are in place for decom- missioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.
Govern 2	**Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for Mapping, measuring, and managing AI risks**	Govern 2-1	Roles and responsibilities and lines of communication related to Mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.
		Govern 2-2	The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.
		Govern 2-3	Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.

Govern A culture of risk management is cultivated and present

Category	Description	Sub-Cat	Description
Govern 3	**Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.**	Govern 3-1	Decision-making related to Mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).
		Govern 3-2	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.
Govern 4	**Organizational teams are committed to a culture that considers and communicates AI risk.**	Govern 4-1	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.
		Govern 4-2	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.
		Govern 4-3	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing.

Govern A culture of risk management is cultivated and present

Category	Description	Sub-Cat	Description
Govern 5	**Processes are in place for robust engagement with relevant AI actors.**	Govern 5-1	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.
		Govern 5-2	Mechanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation.
Govern 6	**Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.**	Govern 6-1	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third-party's intellectual property or other rights.
		Govern 6-2	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.

Manage establishes the context to frame risks related to an AI system.

Category	Description	Sub-Cat	Description
Manage 1	**Context is established and understood.**	Manage 1-1	Intended purposes, potentially beneficial uses, context- specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative im- pacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.
		Manage 1-2	Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their participation is documented. Opportunities for interdisciplinary collaboration are prioritized.
		Manage 1-3	The organization's mission and relevant goals for AI technology are understood and documented.
		Manage 1-4	The business value or context of business use has been clearly defined or in the case of assessing existing AI systems re-evaluated.
		Manage 1-5	Organizational risk tolerances are determined and documented.
		Manage 1-6	System requirements (e.g., "the system shall respect the privacy of its users") are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI risks.
Manage 2	**Categorization of the AI system is performed.**	Manage 2-1	The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).
		Manage 2-2	Information about the AI system's knowledge limits and how system output may be utilized and overseen by humans is documented. Documentation provides sufficient information to assist relevant AI actors when making decisions and taking subsequent actions.
		Manage 2-3	Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation.

Manage establishes the context to frame risks related to an AI system.

Category	Description	Sub-Cat	Description
Manage 3	**AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.**	Manage 3-1	Potential benefits of intended AI system functionality and performance are examined and documented.
		Manage 3-2	Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness as connected to organizational risk tolerance are examined and documented.
		Manage 3-3	Targeted application scope is specified and documented based on the system's capability, established context, and AI system categorization.
		Manage 3-4	Processes for operator and practitioner proficiency with AI system performance and trustworthiness and relevant technical standards and certifications are defined, assessed, and documented.
		Manage 3-5	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.
Manage 4	**Risks and benefits are Mapped for all components of the AI system including third-party software and data.**	Manage 4-1	Approaches for Mapping AI technology and legal risks of its components including the use of third-party data or software are in place, followed, and documented, as are risks of infringement of a third party's intellectual property or other rights.
		Manage 4-2	Internal risk controls for components of the AI system, including third-party AI technologies, are identified and documented.
Manage 5	**Impacts to individuals, groups, communities, organizations, and society are characterized.**	Manage 5-1	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident re- ports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.

Measure employs quantitative, qualitative, or mixed-method tools, techniques, and methodologies to analyze, assess, benchmark, and monitor AI risk and related impacts.

Category	Description	Sub-Cat	Description
Measure 1	**Appropriate methods and metrics are identified and applied.**	Measure 1-1	Approaches and metrics for measurement of AI risks enumerated during the M A P function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not or cannot be measured are properly documented.
		Measure 1-2	Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities.
		Measure 1-3	Internal experts who did not serve as front-line developers for the system and/or independent assessors are involved in regular assessments and updates. Domain experts, users, AI actors external to the team that developed or deployed the AI system, and affected communities are consulted in support of assessments as necessary per organizational risk tolerance.
Measure 2	**AI systems are evaluated for trustworthy characteristics.**	Measure 2-1	Test sets, metrics, and details about the tools used during TEVV are documented.
		Measure 2-2	Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.
		Measure 2-3	AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented.
		Measure 2-4	The functionality and behavior of the AI system and its components as identified in the Manage function are monitored when in production.
		Measure 2-5	The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability be-yond the conditions under which the technology was developed are documented.
		Measure 2-6	The AI system is evaluated regularly for safety risks – as identified in the Manage function. The AI system to be deployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics reflect system reliability and robustness, real-time monitoring, and response times for AI system failures.

Measure employs quantitative, qualitative, or mixed-method tools, techniques, and methodologies to analyze, assess, benchmark, and monitor AI risk and related impacts.

Category	Description	Sub-Cat	Description
Measure 2	**AI systems are evaluated for trustworthy characteristics.**	Measure 2-7	AI system security and resilience as identified in the Manage function are evaluated and documented.
		Measure 2-8	Risks associated with transparency and account ability as identified in the Manage function are examined and documented.
		Measure 2-9	The AI model is explained, validated, and documented, and AI system output is interpreted within its context as identified in the Manage function to inform responsible use and governance.
		Measure 2-10	Privacy risk of the AI system as identified in the Manage function is examined and documented.
		Measure 2-11	Fairness and bias as identified in the Manage function are evaluated and results are documented.
		Measure 2-12	Environmental impact and sustainability of AI model training and management activities as identified in the Manage function are assessed and documented.
		Measure 2-13	Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.
Measure 3	**Mechanisms for tracking identified AI risks over time are in place.**	Measure 3-1	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.
		Measure 3-2	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.
		Measure 3-3	Feedback processes for end users and impacted communities to report problems and appeal system outcomes are established and integrated into AI system evaluation metrics.

Measure employs quantitative, qualitative, or mixed-method tools, techniques, and methodologies to analyze, assess, benchmark, and monitor AI risk and related impacts.

Category	Description	Sub-Cat	Description
Measure 4	**Feedback about efficacy of measurement is gathered and assessed.**	Measure 4-1	Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented.
		Measure 4-2	Measurement results regarding AI system trust- worthiness in deployment context(s) and across the AI lifecycle are informed by input from domain experts and relevant AI ac- tors to validate whether the system is performing consistently as intended. Results are documented.
		Measure 4-3	Measurable performance improvements or de- clines based on consultations with relevant AI actors, including affected communities, and field data about context- relevant risks and trustworthiness characteristics are identified and documented.

Manage entails allocating risk resources to Mapped and measured risks on a regular basis and as defined by the GOVERN function.

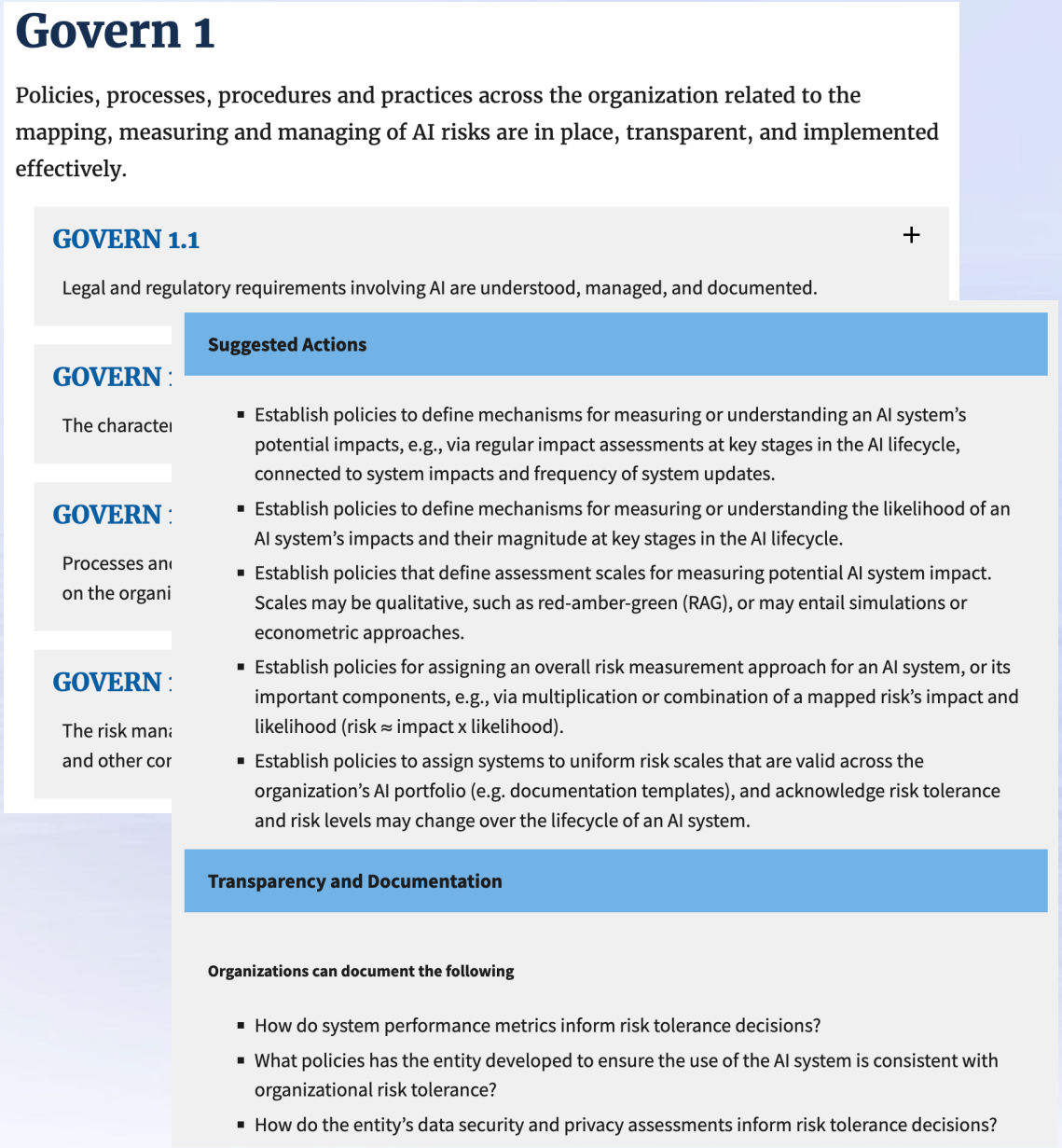
Category	Description	Sub-Cat	Description
Manage 1	**AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.**	Manage 1-1	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.
		Manage 1-2	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.
		Manage 1-3	Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options can include mitigating, transfer- ring, avoiding, or accepting.
		Manage 1-4	Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented.
Manage 2	**Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.**	Manage 2-1	Resources required to manage AI risks are taken into account along with viable non-AI alternative systems, approaches, or methods to reduce the magnitude or likelihood of potential impacts.
		Manage 2-2	Mechanisms are in place and applied to sustain the value of deployed AI systems.
		Manage 2-3	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.
		Manage 2-4	Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.

Manage entails allocating risk resources to Mapped and measured risks on a regular basis and as defined by the GOVERN function.

Category	Description	Sub-Cat	Description
Manage 3	**AI risks and benefits from third-party entities are managed.**	Manage 3-1	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.
		Manage 3-2	Pre-trained models which are used for development are monitored as part of AI system regular monitoring and maintenance.
Manage 4	**Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.**	Manage 4-1	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.
		Manage 4-2	Measurable activities for continual improvements are integrated into AI system updates and include regular engagement with interested parties, including relevant AI actors.
		Manage 4-3	Incidents and errors are communicated to relevant AI actors, including affected communities. Processes for tracking, responding to, and recovering from incidents and errors are followed and documented.

AI RMF Methodology

Assess/review applicable practices against Suggested Actions outlined in the published NIST AI RMF Playbooks



Govern 1

Policies, processes, procedures and practices across the organization related to the mapping, measuring and managing of AI risks are in place, transparent, and implemented effectively.

GOVERN 1.1

Legal and regulatory requirements involving AI are understood, managed, and documented.

Suggested Actions

- Establish policies to define mechanisms for measuring or understanding an AI system's potential impacts, e.g., via regular impact assessments at key stages in the AI lifecycle, connected to system impacts and frequency of system updates.
- Establish policies to define mechanisms for measuring or understanding the likelihood of an AI system's impacts and their magnitude at key stages in the AI lifecycle.
- Establish policies that define assessment scales for measuring potential AI system impact. Scales may be qualitative, such as red-amber-green (RAG), or may entail simulations or econometric approaches.
- Establish policies for assigning an overall risk measurement approach for an AI system, or its important components, e.g., via multiplication or combination of a mapped risk's impact and likelihood (risk ≈ impact x likelihood).
- Establish policies to assign systems to uniform risk scales that are valid across the organization's AI portfolio (e.g. documentation templates), and acknowledge risk tolerance and risk levels may change over the lifecycle of an AI system.

Transparency and Documentation

Organizations can document the following

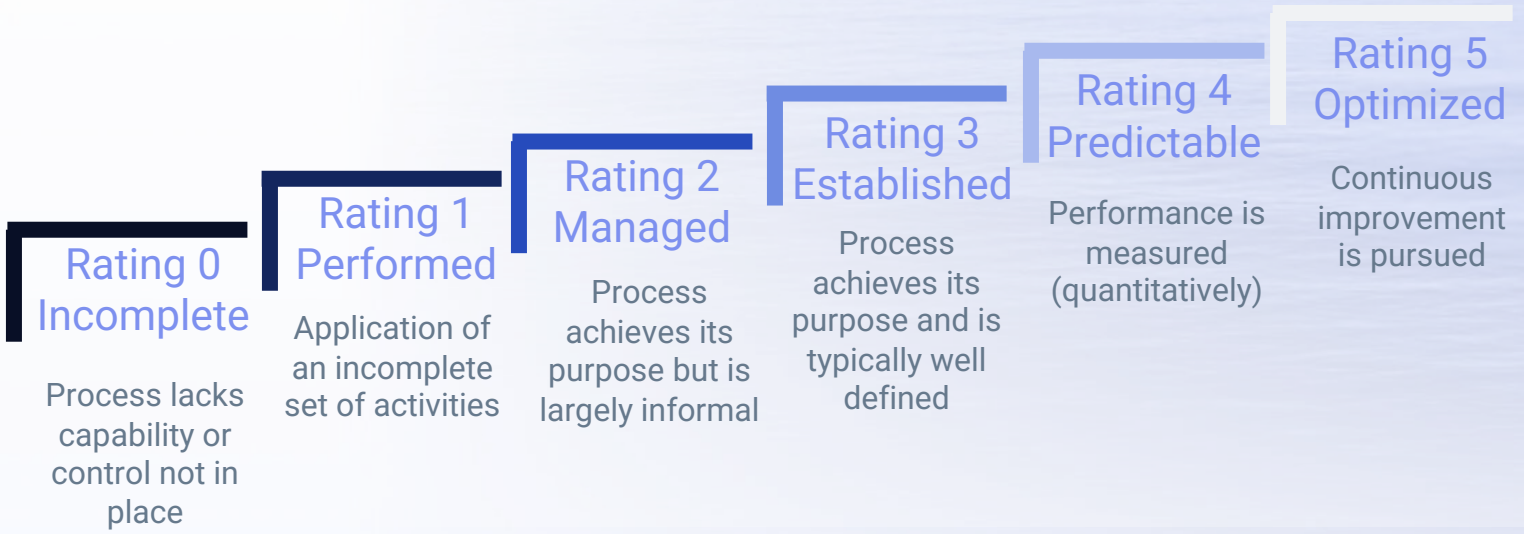
- How do system performance metrics inform risk tolerance decisions?
- What policies has the entity developed to ensure the use of the AI system is consistent with organizational risk tolerance?
- How do the entity's data security and privacy assessments inform risk tolerance decisions?

Clearwater

Clearwater's Performance Measurement Model

How we measure: *The adherence to* and *degree of adoption* of control expectations are assessed using the maturity scale as outlined in the Control Objectives for Information Technologies (COBIT) 2019 framework.

COBIT Maturity Model



Artificial Intelligence Risk Management Framework (AI-RMF) Assessment

Benefits:

- Confidence the current approach to AI governance aligns to NIST
- A detailed plan to address gaps
- Enables dialogue to address and manage AI risk
- More trustworthy AI systems unleashing benefits and managing risks

Establish effective AI cybersecurity practices

Determine Current AI Security Posture

Manage and drive down AI Risk

Clearwater

Q&A

Dave Bailey

We are here to help.

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

Upcoming Events

Hlth | October 8-11

HPE NYC 2023 | October 13

SCALE Healthcare Leadership Conference |October 18th

Clearwater

Healthcare – Secure, Compliant, Resilient

Contact us

info@clearwatersecurity.com

www.clearwatersecurity.com

1.800.704.3394

Legal Disclaimer

Although the information provided by Clearwater Compliance 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 Compliance LLC.