

FROM RISK ASSESSMENT TO RISK MANAGEMENT: TURNING SECURITY RISK ASSESSMENTS INTO ACTIONABLE VALUE

by John DiMaggio and Angele Tran



John DiMaggio

(john.dimaggio@blueorangecompliance.com) is a Managing Director at Blue Orange Compliance, a CloudWave Company in Doylestown, PA.



Angele Tran

(atran@aqord.org) is a Compliance Manager at AQORD in Blue Bell, PA.

Healthcare organizations routinely conduct HIPAA Security Risk Assessments (SRAs) to meet regulatory requirements. Yet enforcement actions, audit findings, and breach investigations continue to show that many assessments fail to translate into sustained risk reduction or effective governance.

In practice, organizations often complete an assessment and receive a report, then struggle to operationalize the findings. The assessment technically satisfies a requirement, but it does not materially improve security posture or strengthen defensibility. In an environment of escalating cyber threats and increasing regulatory scrutiny, this gap presents critical compliance and governance risk.

To deliver meaningful value, an SRA must function as more than a point-in-time exercise. It must serve as the foundation for ongoing risk management, prioritization, remediation, and oversight.

In fact, the SRA is becoming increasingly important from a regulatory perspective, given the forthcoming updates proposed by the U.S. Department of Health and Human Services (HHS).

Healthcare organizations should be prepared to meet requirements that extend beyond the current HIPAA Security Rule. HHS has proposed significant updates to the Security Rule that would require a shift toward more rigorous and continuous cybersecurity oversight. As of mid-2026, however, the final rule has not yet been issued, and the timeline for finalization remains uncertain as the agency continues to review public comments.

The proposed changes would considerably increase expectations for ongoing risk management by eliminating the distinction between “required” and “addressable” implementation specifications in most circumstances.

They would also require written documentation of Security Rule policies, procedures, plans, and analyses, establish specific compliance time frames, increase the level of detail required in risk assessments, strengthen contingency planning and incident response requirements, mandate annual compliance audits, and require encryption of electronic protected health information (ePHI) both at rest and in transit, subject to limited exceptions.

While these changes have not yet been implemented, they reflect a

broader regulatory trend already evident in enforcement actions and the agency's Risk Analysis Initiative. Covered entities are expected not only to identify risks but also demonstrate how those risks are prioritized, managed, and reduced over time. Healthcare organizations should view this as an opportunity to move beyond the SRA as a periodic compliance exercise and instead leverage it as the cornerstone of an ongoing risk management program. Organizations that can translate assessment findings into measurable remediation, governance, and oversight activities will be better positioned to meet evolving regulatory expectations and strengthen cybersecurity resilience over time.¹

Components of a compliant and valuable risk assessment

From a compliance perspective, an SRA must first meet regulatory expectations. Under the HIPAA Security Rule and related guidance, assessments are expected to be accurate, thorough, and reflective of the organization's actual environment. This includes evaluating administrative, technical, and physical safeguards; identifying threats and vulnerabilities; analyzing likelihood, impact, and resulting risk; and documenting existing controls and gaps.

The proposed Security Rule modifications underscore the significance of risk analysis by requiring regulated entities to conduct and document SRAs at least annually and whenever major operational or environmental changes occur. Additionally, proposed requirements to maintain technology asset inventories and network maps would expand the scope and rigor of risk analyses,

making them substantially more comprehensive than those currently performed by many organizations.

However, compliance alone does not ensure usefulness or value.

A valuable risk assessment is distinguished by its ability to support decision-making. It focuses on risk exposure rather than isolated control deficiencies, differentiates theoretical concerns from realistic threat scenarios, and produces outputs that leadership, IT, and compliance teams can understand and act upon.

Regulators increasingly focus not only on whether an assessment exists, but on whether identified risks were addressed in a reasonable and documented manner. Assessments that lack clarity, prioritization, or follow-through provide limited protection during audits or enforcement actions.

Strategic value for compliance programs, leadership, and boards

When structured effectively, an SRA becomes a strategic tool rather than a technical deliverable. For compliance professionals, a thorough and accurate risk assessment supports alignment between regulatory obligations and operational reality. It provides a defensible framework for explaining why certain risks were remediated, deferred, or accepted and demonstrates good-faith efforts to manage known risks over time.

For IT professionals, it identifies specific weaknesses and gaps across technology, physical controls, policies, and procedures.

For executives and boards, a well-designed assessment answers critical questions:

- ◆ Where is the organization most exposed today?

- ◆ Which risks could meaningfully disrupt operations or patient care?
- ◆ What remediation actions will most effectively reduce risk?
- ◆ Which risks are being knowingly accepted, and why?
- ◆ Do we have enough cyber-liability coverage?
- ◆ Does our security posture meet cyber insurance requirements?²

In this way, the assessment becomes a shared source of truth across compliance, IT, executive leadership, and governing bodies.

Regulators increasingly focus not only on whether an assessment exists, but on whether identified risks were addressed in a reasonable and documented manner.

Strategic value to keep up with a more dangerous and complex security environment

The importance of effective risk assessments has increased as the healthcare threat landscape has evolved. Cyber threats are more frequent and, with the addition of AI, more sophisticated and more disruptive than in prior years.

Key risk drivers include ransomware and extortion attacks targeting operational continuity, expanded attack surfaces driven by



cloud adoption and remote work, increased reliance on third-party vendors, and the growing use of AI to scale phishing and social engineering attacks.

Notably, the proposed Security Rule updates recognize this evolving threat environment by moving several long-standing cybersecurity safeguards from discretionary implementation to explicit requirements. The proposal would require multifactor authentication (MFA) and encryption of ePHI, subject to limited exceptions. These updates signal HHS's view that such controls are now baseline security expectations rather than optional enhancements.³

Risk assessments that rely on static checklists or outdated assumptions fail to capture this reality. Modern assessments must factor in threat capability, likelihood, and impact—not just the presence of controls—to remain relevant and defensible.

Value of identifying risks, weaknesses, and hidden gaps

One of the most noteworthy contributions a risk assessment makes to a compliance program is exposing gaps that are not visible through policy review alone.

Common findings include policies that exist but are

inconsistently implemented, technical controls applied unevenly across systems, informal practices that lack documentation, gaps between compliance documentation and IT operations, and limited oversight of vendors and business associates.

Effective assessments identify patterns of risk rather than isolated issues. Repeated findings often point to governance, training, or accountability weaknesses rather than one-off technical failures. Framing these issues in risk terms, explaining why they matter, and what could happen if they are not addressed, is essential for leadership engagement.

Value for prioritization and risk-based decision-making

Compliance officers frequently face the challenge of managing long lists of findings with limited resources. Risk assessments that lack prioritization offer little practical guidance.

A risk-based approach considers the likelihood of exploitation, potential regulatory and operational impact, existing compensating controls, and organizational constraints. Prioritization enables organizations to focus remediation efforts where they will have the greatest impact.

Particularly, regulators generally recognize that not all risks can be addressed immediately. They expect documented, reasoned decision-making that demonstrates thoughtful management of known risks.

At the same time, the proposed Security Rule changes suggest that certain safeguards may no longer be subject to the same level of organizational discretion. By removing the distinction between “required” and “addressable” implementation specifications, the proposal would narrow an organization’s ability to defer or substitute controls such as MFA and encryption without strong justification.

Value to develop and manage roadmaps and tactical remediation planning

To translate assessment findings into action, organizations need clear remediation roadmaps. Assessments, year after year, with similar gaps, are problematic.

An effective remediation plan includes defined actions tied to specific risks, assigned ownership, realistic timelines, documentation requirements, and mechanisms for tracking progress over time. For compliance professionals, remediation tracking is as crucial

as remediation itself. The ability to demonstrate progress, explain delays, and document risk acceptance decisions is imperative during audits, investigations, and post-incident reviews.

When remediation planning is integrated into the assessment process, the assessment becomes a living tool rather than a static report.

Risk assessments as governance and communication tools

SRAs also play a vital role in governance and communication.

Different audiences require different perspectives. IT teams need technical detail; compliance teams need regulatory alignment and evidence; executives need business impact and prioritization; boards need high-level risk visibility; and cyber insurers need evidence of maturity and oversight.

A structured risk assessment allows organizations to translate the same underlying information into appropriate formats for each audience, ensuring consistency and reducing misalignment. For boards, assessments provide oversight without requiring technical expertise. For insurers, they demonstrate ongoing risk management rather than point-in-time compliance.

Risk assessment as operational tools: From findings to a sustainable risk management program

A risk assessment generates substantially more value when its findings are translated into a prioritized remediation plan that can be governed, maintained, and executed over time. Managed in this way, the plan evolves from a standalone report into an actionable

tool. The resulting transparency and follow-through materially strengthen defensibility in an environment of increasing operational dependence on technology, heightened threat activity, and elevated regulatory expectations.

Recent enforcement activity further reinforces the need to move beyond risk analysis alone. Through HHS Office for Civil Rights' (OCR) Risk Analysis Initiative, OCR has focused on organizations that failed to conduct accurate and thorough risk analyses, while related OCR guidance emphasizes that risk management is a separate Security Rule requirement that requires organizations to reduce identified risks and vulnerabilities to reasonable and appropriate levels. Together, these efforts highlight regulators' increasing focus not only on identifying risks but also on demonstrating how those risks are managed over time.⁴

A well-structured remediation plan converts high-priority risks into discrete actions with clear ownership, milestones, and target dates. When completion criteria and evidence expectations are defined early (e.g., configuration baselines, system reports, approvals, or ticket artifacts), progress can be validated objectively, and closed items remain defensible and audit-ready. Operational systems such as ticketing, change control, and project governance can handle day-to-day execution, while the remediation plan provides a consolidated view of priorities, dependencies, milestones, and evidence status.

Routine governance reviews add value by creating a consistent forum to confirm closures, surface impediments, document decisions, and recalibrate priorities when

circumstances change. For executive leadership and boards, this structure supports a concise, risk-oriented view that includes top exposures, planned mitigations, overdue or blocked actions, and material changes since the prior review, without requiring a control-by-control walkthrough.

OCR guidance emphasizes that risk management is a separate Security Rule requirement that requires organizations to reduce identified risks and vulnerabilities to reasonable and appropriate levels.

A small set of repeatable measures, supported by verifiable evidence, helps leadership understand whether risk is trending in the right direction. Illustrative measures include the number of unsupported systems in patient-care areas, MFA coverage for privileged access, backup and recovery test outcomes, and completion rates for critical vendor security reviews. Consistent measurement improves prioritization, clarifies resourcing discussions, and provides stronger support during audits, investigations, and post-incident scrutiny.

The remediation plan also preserves the assessment's relevance between formal refresh cycles. When significant events

occur, such as major system implementations, cloud migrations, mergers, new vendors or business associates, facility moves, or security incidents, the plan provides a practical basis to revisit priorities without restarting the assessment from scratch. Incorporating outputs from tabletop exercises, penetration testing, and incident response lessons learned helps keep attention anchored to the most consequential risks and the organization's current operating reality.

Finally, documenting risk disposition within the remediation plan improves both accountability and defensibility. When remediation is deferred or risk is accepted, capturing the rationale, compensating controls, and time horizon, along with approval appropriate to the level of exposure, creates a durable record of decision-making. Defined escalation thresholds for overdue actions, repeated slippage, or evidence gaps further support timely executive attention and, when appropriate, board visibility.⁵

Conclusion

The value of a security risk assessment lies not only in its completion, but in its use.

In an environment of escalating cyber threats and increasing regulatory scrutiny, healthcare organizations are judged not only on their ability to identify risks, but also on their ability to demonstrate how those risks are prioritized, managed, and reduced over time. Risk assessments that produce findings without driving remediation, governance, and accountability provide limited value when audits or security incidents occur.

As HHS's proposed Security Rule updates and recent enforcement activity make clear,

expectations are shifting toward continuous risk management and documented oversight. Organizations that can translate assessment findings into measurable actions, track progress, and communicate risk effectively across leadership, compliance, IT, and other departments will be positioned to strengthen regulatory defensibility and cybersecurity resilience.

When designed to support action, oversight, and communication, an SRA becomes one of the most effective tools a compliance program can leverage by transforming a regulatory obligation into measurable, defensible value. ^{CT}

Endnotes

1. U.S. Department of Health and Human Services, "HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information," fact sheet, content last reviewed December 27, 2024, <https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html>.
2. U.S. Department of Health and Human Services, "Guidance on Risk Analysis," content last reviewed September 26, 2025, <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>.
3. U.S. Department of Health and Human Services, "HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information."
4. Jill Hughes, "HIPAA compliance in the era of OCR's risk analysis initiative," TechTarget, August 21, 2025, <https://www.techtarget.com/healthtechsecurity/feature/HIPAA-compliance-in-the-era-of-OCRs-risk-analysis-initiative>.
5. U.S. Department of Health and Human Services, "Guidance on Risk Analysis."

Takeaways

- ◆ Learn why HIPAA Security Risk Assessments should serve as the foundation for continuous risk management—not just a compliance exercise.
- ◆ Understand how proposed U.S. Department of Health and Human Services' Security Rule updates are raising expectations for ongoing cybersecurity oversight, documentation, and remediation.
- ◆ Discover how to prioritize security risks, develop actionable remediation roadmaps, and demonstrate defensible compliance decisions.
- ◆ Explore how effective risk assessments improve governance by providing meaningful insights for compliance, IT, executives, boards, and cyber insurers.
- ◆ See how organizations can transform assessment findings into measurable risk reduction, stronger cybersecurity resilience, and audit-ready compliance.