Compliancy Group

Understanding and Applying Risk Assessment Procedures in Healthcare Compliance

A Practical Implementation Guide

While healthcare compliance officers are often well-versed in theoretical risk assessment needs, there is persistent difficulty in turning this into practical (and enforceable) procedures that comprehensively protect organizations.

Regulatory guidance offers clear mandates, but the fragmented web of healthcare legislation and regulation from the state to the Federal level makes it complex to implement, revealing gaps between policy and practice.

$3.2 million

fine issued to the Children's Medical Center of Dallas for ignoring recommendations to encrypt its data, which led to an eight-year trail of HIPAA violations that uncovered a failure to perform regular risk assessments.[1]

The consequences of inadequate risk assessment are severe—and escalating. Readers may be familiar with the $3.2 million fine issued to the Children's Medical Center of Dallas for ignoring recommendations to encrypt its data, which led to an eight-year trail of HIPAA violations that uncovered a failure to perform regular risk assessments.[1] Regulations and their enforcement are tightening, and superficial compliance is no longer sufficient.

This white paper addresses the compliance officer's dilemma, detailing how healthcare organizations can transform the risk assessment process from on-paper exercises to structured protection with measurable outcomes for organizational peace of mind.

It was informed by in-depth interviews with industry figures and supporting data from other thought leaders in this space.

[1] https://www.dallasnews.com/business/health-care/2017/02/02/childrens-dallas-docked-3-2-million-over-patient-privacy-breaches/

The Risk Assessment Implementation Gap

Traditional risk assessment approaches often fail in healthcare practice, by creating what Dr. Mahboob Khan, an independent policy advisor, calls "risk silos," or non-interlinked data that does not consider the full risk picture. "This approach delegates risk management to business units instead of treating it as an organization-wide responsibility.[2]"

Traditional risk assessments are designed for static environments, relying on annual checklists and surface-level audits that do not always translate to real change in practice, as the Dallas Children's Center case also showcases.

A recent HIPAA Journal survey[3] suggests that 43% of organizations do not use software to support compliance tracking, despite the fact that software automation simplifies the risk documentation necessary to demonstrate compliance during incidents or audits. Additionally, it exposes that risk assessments are often not updated annually.[4] According to Liam Degnan from Compliancy Group,

> **"As far as areas like cybersecurity, healthcare has never been doing worse. Even in the last couple of years, from 2022 to 2024, there has been a 300% increase in individual records breached."[5]**

43%

of organizations do not use software to support compliance tracking

[2] https://www.linkedin.com/pulse/risk-management-healthcare-dr-mahboob-ali-khan-mhm-advisor--5qtdf

[3] https://www.hipaajournal.com/editorial-at-least-43-of-covered-entities-still-not-using-software-for-hipaa-compliance-tracking/

[4] https://www.hipaajournal.com/wp-content/uploads/2025/04/The-HIPAA-Journal-Annual-Survey-2025.pdf

[5] https://www.youtube.com/watch?v=3tDGwmW-kO8

Developing Regulatory Imperatives Highlight the Need to Strengthen Compliance

In January 2025, we saw the first major proposed update to HIPAA Security Rules in a decade. It would make all implementation specifications mandatory unless explicitly exempted, especially around multi-factor authentication and encryption.[6] Tighter risk analysis, and rules around common digital security postures are in the public comment phase.

As of 2025, the Department of Justice, which overlaps with the HHS Office for Civil Rights (OCR) on criminal enforcement issues, has stepped up investigation and prosecution of healthcare violations, particularly related to fraud, waste, and abuse.[7] New healthcare cybersecurity legislation is making its way through the Senate currently and, as of April 2025, the Department of Justice forbids even de-identified/encrypted bulk data transfers of PHI without security oversight.[8]

The OCR likewise emphasizes that compliance failures will no longer be tolerated, with expanded audit guidelines and enforcement underway.[9]

[6] https://www.kirkland.com/publications/kirkland-alert/2025/01/proposed-changes-to-the-hipaa-security-rule

[7] https://corpgov.law.harvard.edu/2025/06/03/what-dojs-new-enforcement-plan-means-for-health-care-companies/

[8] https://www.hklaw.com/en/insights/publications/2025/05/us-health-data-affected-by-new-national-security-restrictions

[9] https://www.healthlawadvisor.com/recent-developments-in-health-care-cybersecurity-and-oversight-2024-wrap-up-and-2025-outlook

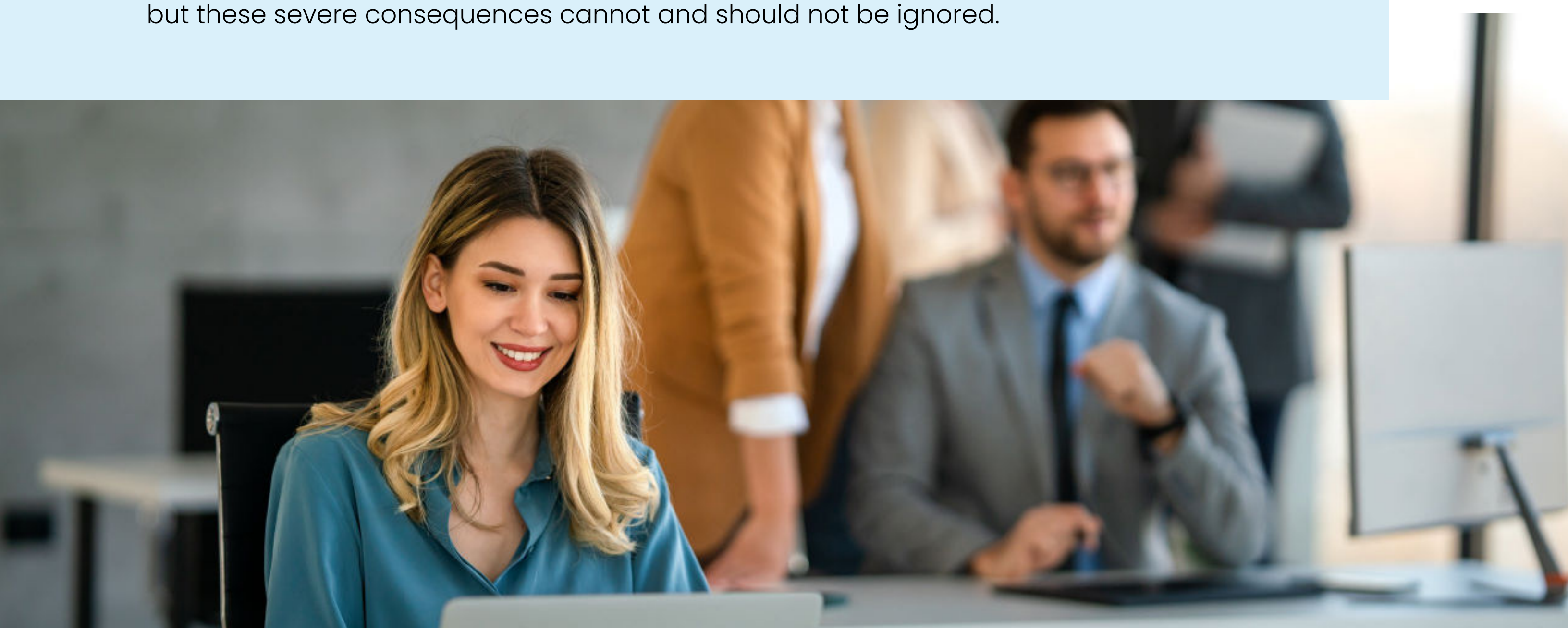
The Cost of Inaction and Inefficiencies

The Eisenhower Medical Center class action lawsuit paints a chilling picture of how compliance challenges can extend far beyond OCR scrutiny.[10] Violations spanning California's Confidentiality of Medical Information Act, Electronic Communications Privacy Act, and Invasion of Privacy Act, among others, resulted from the implementation of standard digital marketing tracking tools which inadvertently exposed sensitive patient information, resulting in steep payouts to affected parties. This showcases how standard compliance mindsets can overlook the many potential breach vectors modern healthcare environments offer.

Aside from monetary penalties and fines, failures in compliance can include:

- Loss of participation in Medicare/ Medicaid programs
- Restrictions on operations
- Reputational damage
- Erosion of patient trust

And, as we see in the Eisenhower case, even potential legal liability for severe violations. Outcomes vary significantly, depending on the specific offense and its internal response, but these severe consequences cannot and should not be ignored.



[10] https://www.classaction.org/media/bk-et-al-v-eisenhower-medical-center-complaint_1.pdf#:~:text=Plaintiff%20B.K.%20accessed%20Defendant%27s%20Website%20and%20Patient,receive%20healthcare%20services%20from%20Defendant%20and%20at

Building a Foundation Through Pre-Assessment Infrastructure

Risk identification and mitigation need to be core to how organizations work. Implementation gaps and regulatory exposure typically come from seeing risk assessment as an isolated "compliance event," not an integrated and ongoing process.

Establishing Governance Structures

Governance structures will vary considerably across organizational sizes. While a single risk officer with external consulting support is common in small practices, enterprise-level organizations may need multi-disciplinary committees across IT, clinical operations, legal counsel, and executive oversight.

Regardless of size and complexity, however, there must be clear reporting hierarchies and an organizational commitment to risk mitigation. The HHS Office of the Inspector General (OIG) recommends that an organization build its compliance program on seven elements: [11]

1 **Written Policies:** Maintain clear, accessible policies and a code of conduct outlining compliance expectations.

2 **Oversight Structure:** Appoint a compliance officer and committee with active leadership and board support.

3 **Training and Education:** Deliver regular, role-specific training on laws, risks, and ethical standards.

4 **Open Communication:** Provide confidential, non-retaliatory channels for reporting concerns.

5 **Enforcement and Discipline:** Apply consistent consequences for non-compliance at all levels.

6 **Monitoring and Auditing:** Conduct risk-based audits, track issues, and investigate promptly.

7 **Corrective Action:** Resolve problems with root-cause analysis, remediation, and updated practices.

A high-level, full-organization risk assessment as the starting point for establishing these structures, offering a holistic view of where the organization currently stands. Document retention schedules should be aligned with the statute of limitations, typically six years for HIPAA violations, although state regulations may require up to ten years.

[11] https://oig.hhs.gov/compliance/general-compliance-program-guidance/

Regulatory Framework Mapping

While HIPAA Privacy, Security, and Breach Notification Rule requirements are the foundational regulatory framework, the regulatory environment is expanding, as the rise in OCR enforcement highlights and Compliancy Group's Daniel Lebovic stresses,

> **"The HIPAA security rule has historically been a handshake rule, in the sense that it offers little guidance on how often you have to perform risk assessments. We're finding that providers are not necessarily conducting risk assessments or managing their risks sufficiently or enough. The proposed expanded landscape of enforcement governing security aims to ensure that people's health information is kept safe and is not compromised."**

All these new regulatory touchpoints must be thoroughly assessed and brought together in risk management practices.

State-specific privacy law considerations, such as 42 CFR Part 2, which requires specialized alignment strategies for substance abuse treatment providers, must also be considered and incorporated.

Risk management must also extend beyond organizational boundaries to include third-party vendors. Dotty Bollinger, President of Integrity Healthcare Advisors, says,

> "Healthcare organizations need to start thinking more broadly about their external relationships. Anyone can sign a BAA, keen to acquire your business. The due diligence in evaluating vendor security practices and verifying they are meeting their contractual obligations is up to the healthcare organization itself."

Resource Allocation and Planning

Effective risk management requires an honest evaluation of not just in-house expertise, but also resources. Where dedicated compliance teams are impractical, hybrid approaches, combining internal oversight with specialized external partners, can offer support and greater resources.

Elizabeth Simon, an independent Strategic Compliance Leader, suggests focusing compliance resources on mitigation through proactive planning or redesigning of policies and procedures to address identified risks.[12]

Technology infrastructure should support risk mitigation efforts through aspects such as:

- **Asset/inventory management**
- **Security tools**
- **Threat modelling**
- **Continuous monitoring of systems**

Dedicated compliance software solutions can support this, offering automatic and centralized data collection to avoid silos, standardized evaluation criteria, and clear audit trails to ensure documentation requirements are met.

To ensure complete organizational coverage, make certain all operational areas are accounted for, from clinic workflows to administrative support.

[12] https://www.linkedin.com/pulse/how-implement-robust-compliance-risk-assessment-reporting-simon

Systemic Risk Identification Methodologies

Identifying risk starts with analyzing incident reports and internal audits, which will highlight clear issues to address. Further hidden risks can be identified by a systemic organizational assessment, using all available data—from staff feedback to what logs reveal about technology use.

> **"Risk should not be defined solely based on financial impact",** cautions Kelly Saunders, Partner/Risk & Financial Advisory at Deloitte, **"as other non-financial impacts, such as reputation, patient safety, or quality, can be equally important, even if they are not easily measurable."**[13]

Compliance officers have a wealth of tools available for risk identification and mitigation, including:

- Electronic PHI access controls and user authentication systems
- Audit log analysis and automated monitoring capabilities
- Data encryption standards for data at rest and in transit
- Network security architecture evaluation tools
- Compliance software offering clear risk assessment frameworks

As Ben Beninati, IT Systems Manager, CHSP, CHSRP at Compliancy Group, observes,

> **"technological solutions do not have to be expensive or complex; they simply have to be fit for purpose, offering practical support that makes it easier for organizations to build risk assessment into their everyday operations."**

Safeguarding and Evaluating

Best practices for healthcare cybersecurity require clear structures and procedures. When compliance happens from the earliest levels of decision making, it **"shifts from a roadblock to a strategic part of addressing risk early"**, as Anne Marie Anderson, Director of Product Content at Compliancy Group, observes.

Organizations should focus on compliance-supportive administrative processes such as:

- Enacting workforce access management and role-based permissions
- Ensuring incident response procedure adequacy
- Establishing oversight and contract compliance for third-party vendors and business associates, including clear business associate agreements (BAA)

[13] https://www.linkedin.com/pulse/how-implement-robust-compliance-risk-assessment-reporting-simon

Physical Safeguards and Staff Buy-In

Compliance officers often encounter resistance from staff, and even executive boards, when asking them to prioritize compliance matters. Regular training and including compliance at grassroot levels can help offset this.

However, as Ajenay Drummond, Compliance Director at EMS|MC notes,

> “it’s not enough to merely provide information without ensuring it is absorbed. It is essential to monitor the outcomes and establish clear expectations after training to ensure effectiveness, including regular meetings. Employees must understand expectations and their benefits, and share concerns freely.”

To facilitate that understanding, training can be fortified or gamified with relatable real-life examples or current news events to help to foster a culture of compliance that feels immediate and relatable.

And raising awareness about compliance best practices benefits the organization, too, notes Anne Marie Anderson. **“Workers stay where they feel heard and respected, and knowing that integrity is the expectation can create significant workplace satisfaction.”**

Additionally, physical safeguards that support compliance must be in place, such as:

- Facility access controls and workstation security
- Properly configuring and maintaining devices and controlling access
- Restricting the use of personal devices
- Regular auditing (including stock and vendors) and risk assessments
- Clear media handling and disposal procedures
- Environmental threat assessment (against natural disasters and utility failures)
- Documenting processes and policies clearly and accessibly
- Strong interdepartmental communication, especially with security/compliance teams

Emerging Risk Vectors

Risk vectors, especially in a digital world, are ever-evolving. Procedures must adapt to these new risks in a timely manner. We have already seen remote work post-COVID raise new security implications. Cloud service providers have opened up attack surfaces considerably, where a single third-party vendor can inadvertently trigger massive data leaks.

With the rise of new technology, we see two key novel vectors raising concerns:

- Internet of Things (IoT) medical device vulnerabilities
- AI and machine learning privacy implications

Although a full analysis of these new risks is outside the scope of this white paper, monitoring new developments and building security procedures accordingly must be an ongoing priority.

Quantifying, Prioritizing, and Frameworking Risks

Healthcare, by its very nature, is an intimate, personal, and data-heavy field. Protected PHI is handled in almost every process and by nearly all team members. This is why correctly modelling risks is vital. You cannot protect against what you don't know.

Quantifying Risk: Structured Risk Matrices

Every organization has its own risk profile and tolerance threshold, as does every department and function within it.

Risks can be quantified through likelihood assessment criteria, ranking the likelihood of occurrence and the severity of impact. This simplifies risk management, allowing compliance officers to identify what needs immediate attention and what can be monitored/improved over time.

Identify all risks and hazards that could impact the organization, from macro risks (impacting the whole organization) to micro risks.

Evaluate their likelihood of occurrence on a scale, from rare to almost certain.

Determine the potential impact of each hazard across financial, operational, and reputational areas, and rate the severity of the impact.

Combine these likelihood and severity scores for a clearer view of risk.

Pinpoint high-priority risks for immediate action.

Implement mitigation strategies or eliminate identified risks through concrete action, such as process changes or additional equipment and training.

This process should be revisited and updated regularly—at least annually, and whenever organizational changes occur.

Threat Modeling in Healthcare Environments

It is important to evaluate all potential risk vectors in this process, including hidden and qualitative risks (often behavior-related) as well as quantitative and known risks like cybersecurity. Consider all potential risks from:

- **Internal threats:** Such as workforce snooping and unauthorized access patterns
- **External threats:** Consider cyberattacks, social engineering, and vendor breaches
- **Environmental threats:** System failures and natural disasters also create risk vectors

Useful Tools to Know

There are many tools on the market to simplify risk modelling, including:

- Technical vulnerability scanning and continuous monitoring from IT departments
- Process gap analysis methodology
- Weighted scoring models
- Visual representation tools for executive reporting
- Software that integrates with existing compliance dashboards
- Risk matrix calculators

When Things Happen: Strategic Remediation Planning and Implementation

The HIPAA Journal's 2025 Annual HIPAA Compliance Survey reveals that, when it comes to preparedness for an OCR compliance audit or data breach/complaint investigation, confidence is low.[14]

No matter how diligent an organization is, incidents will occur. Developing clear remediation plans, implementing them before they are needed, and addressing any uncovered risk during an incident is essential. In many ways, how you respond is as important as the why.

Ideally, organizations should monitor their systems with audit controls in place. Automation helps to alert compliance teams the moment an anomaly is detected, allowing for faster responses and reducing negative impact.

Remediation Timelines and Plan Development

When an incident is detected, compliance teams must investigate. While all breaches are important, Daniel Lebovic advises that compliance teams must establish what is a critical or high risk, versus medium and lower risks, as this will guide appropriate responses.

Anne Marie Anderson recommends looking at the facts objectively, then asking:

Is this a single-time issue, or an ongoing one that's impacted a wider section of the organization?

Is outside help, such as a response partner, legal source, or a forensic investigation, required?

What processes led to the incident? How can they be addressed and remediated?

[14] https://www.hipaajournal.com/2025-hipaa-journal-annual-survey-results/

This will help you assess what action is appropriate and the severity of the organizational impact. The next step should be discussing the circumstances with proper counsel, reporting to the OCR, and showing those affected that you are taking steps to address the matter.

The OCR will investigate what happened, how it happened, and what can be improved. In many cases, the end goal is corrective action—has that hole in your defenses been sealed?

If you can respond to any potential investigation with clear evidence that you have put effective responses in place, you will be looked on more favorably, Daniel Lebovic stresses. The recent Recognized Security Practices Incentive even rewards companies that have certain security practices in place, which can reduce fines or offer early exits.[15]

Culpability is also important, as Ben Beninati observes. Knowing what you must do and deciding not to do it is more egregious than simply discovering a weakness in a process you thought was secure. Regardless of the official determination, however, ensure that the appropriate corrective actions are taken.

Implementing Better Practices When Weaknesses Emerge

Daniel Lebovic also notes that corrective actions differ per incident type and instigation. If the breach was a first-time offense, then addressing knowledge gaps among staff and implementing tighter security around the vulnerable process should suffice. However, if it is an ongoing issue, as we saw in the Dallas Children's Center case, harsher consequences will follow, potentially including criminal prosecution, and stricter remediation is required.

Ensure you implement change management strategies for any new processes to monitor and guide workforce adoption and measure the effectiveness of remediation efforts over time.

[15] https://www.hipaajournal.com/ocr-hitech-recognized-security-practices/

Documentation and Tracking

Roughly 80% of HIPAA fines cite missing risk assessment documentation[16], potentially drawing higher punitive measures. Ajenay Drummond, however, notes that a lack of formal, provable documentation, not necessarily a lack of discussion, drives this problem.

All steps of the remediation process must be comprehensibly documented, showing clear action and responses. Organizations will also need to assess and update their risk register and matrix and organizational procedures accordingly.

There will need to be clear executive reporting and board-level communications to all stakeholders, including those external parties that a PHI incident may have impacted.

Measuring the success of remediation efforts is essential to ensure the failings that led to an incident are adequately addressed and new incident prevention measures are properly implemented.

Roughly

80%

of HIPAA fines cite missing risk assessment documentation[16]

[16] https://www.youtube.com/watch?v=3tDGwmW-kO8

Continuous Risk Management Through a Culture of Compliance

As Dotty Bollinger points out, many compliance failings stem not from the technology or practices, but rather from failures in implementation.

> **"Compliance is everyone's job. The compliance officer leads the effort, but can't be the only person doing it."** Dan Troy, a BRG Managing Director, also stresses that **"compliance officers themselves need to feel empowered to raise concerns to truly foster transparency and accountability."**[17]

Encouraging a Culture of Compliance

Security policies are only one part of a culture of compliance. They often lapse in practice, through scenarios such as:

- Accessing systems under someone else's credentials for speed and convenience.
- Unauthorized hardware used without control, introducing vulnerabilities.
- Incorrect termination procedures, where credentials or access are retained after staff members leave.

One of the most important ways to build a culture of compliance, Anne Marie Anderson observes, is ensuring that people feel confident to report incidents transparently, without fear of retaliation. Obviously, if an act is intentional, a zero-tolerance policy should be in place. But the culture should be one where people are comfortable reporting incidents, and where they have an easy way to do it.

[17] https://www.thinkbrg.com/insights/publications/brg-healthcare-compliance-and-ethics-leadership-forum/

Ongoing Monitoring Strategies

When risk management is a regular part of operations, it not only relieves some of the burden from compliance officers, but also helps to foster this culture of compliance and ward off problems before they snowball.

Monitoring is key to smart risk management, and can be achieved through:

- Automated risk detection and alerting systems in software.
- Regular reassessment triggers and schedules.
- Integration with incident management processes.
- Regularly seeking feedback from staff and stakeholders and implementing any lessons learned from these conversations.

Policies and Procedures are Always Evolving

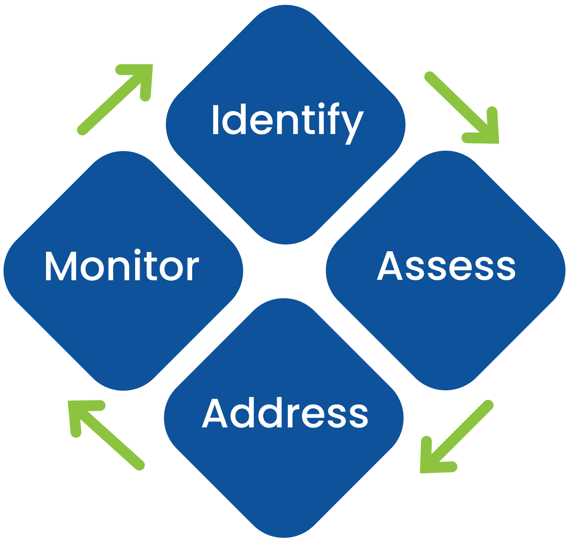
Daniel Lebovic advises that, any time there is a shift, be it in the organization (such as introducing new software or restructuring), environment (such as new facilities or upgrades), or regulations and evolving threats, existing risk management frameworks should be reevaluated.

This includes:

- Conducting regular risk assessments (at least annually) and effectiveness audits.
- Establishing risk-informed policy update cycles.
- Regularly updating BAAs and other documentation.
- Monitoring changes in privacy laws and regulatory compliance integration.
- Ensuring practice standards don’t lapse into bad habits and “quick fixes” that compromise security.
- Using industry best practice adoption frameworks.

Additionally, training should be regularly conducted and adjusted based on both risk findings and the success of prior iterations, addressing any pain points or failures observed and why policy is failing to work in practice, advises Ajenay Drummond.

Taking Action Through Risk Assessments: Getting Started



Risk assessment, alongside a wider risk management framework that not only identifies risk but takes clear steps to address it, should be at the heart of any healthcare compliance framework.

Smart risk management in healthcare organizations takes a systematic, four-pronged approach.

To get started, you need that overarching assessment of your risk posture, properly quantified and evaluated through a risk assessment. Evaluate your current risk state, and see where you can identify:

Quick Wins:
Simple actions that will improve your risk posture

Critical Risks:
Larger or more complex issues that must be urgently and systemically addressed

Resource Gaps:
Where you are lacking tools, policies, or procedures to support risk management

From there, build momentum (and your culture of compliance) through:

Stakeholder engagement

Initial pilot programs addressing quick wins and critical risks

Establishing clear success metrics and measurement protocols

Encouraging staff buy-in through training and education

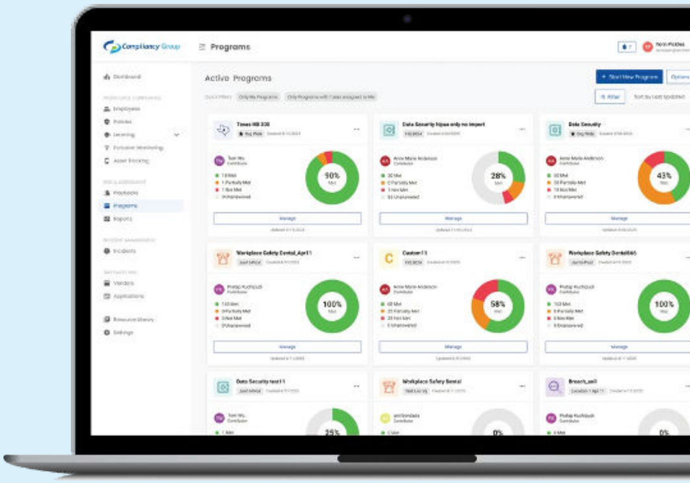
Don't overlook the need for continual risk monitoring and regular revisions to risk management processes to stay current with legislation and changing threat vectors.

☑ Our easy-to-use checklist on the next page breaks it into simple, manageable steps.

A Smarter Approach to Risk Management:

Risk Assessment Checklist

Use this quick checklist to get started on assessing risk in your organization.



Identify Risks

- □ Check for regulatory changes & new cyber threats
- □ Review your organization's past incident reports
- □ Ask for employee feedback

Assess Risks

- □ Determine the likelihood & impact of each risk
- □ Rank risks based on their severity & likelihood
- □ Determine which risks to prioritize & which can wait until next quarter

Address Risks

- □ Implement controls to mitigate identified risks
- □ Update policies & procedures to account for identified risks
- □ Train employees on compliance & cybersecurity best practices

Monitor Effectiveness of Safeguards

- □ Establish performance metrics that mark controls effective
- □ Test effectiveness of safeguards periodically
- □ Review new incident reports for gaps in controls
- □ Update and adapt controls to address new risks

Pro Tip: Monitor changes in your organization, environment, regulatory requirements, and emerging threats. Conduct a new risk assessment when changes occur.

5 Principles for Effective Risk Management in Healthcare

Ongoing

Evidence-Driven

Shared

Integrated

Updated

Continuous Risk Management

Principle: Risk management is not a once-a-year exercise; it must be a living, ongoing process.

Why it matters: Most HIPAA fines cite missing or insufficient documentation—not the absence of a riskassessment.

How Compliancy Group supports this: Built-in review cadences that schedule controls monthly, quarterly, or annually, with automated reminders.

Risk Findings Linked To Remediation

Principle: A risk assessment without follow-up action is just areport; true compliance comes from documented remediation.

Why it matters: Auditors don't just ask for a risk assessment—they ask, "Show us what you did to address the risks you found."

How Compliancy Group supports this: Every control canbe linked to policies, vendor contracts, BAAs, incidents, ortraining evidence – all viewable from your dashboard.

Ownership Across the Organization

Principle: Effective risk management requires shared accountability, not reliance on one individual.

Why it matters: Concentrating responsibility increases the chance of oversights and burnout. Distributing ownership builds resilience.

How Compliancy Group supports this: Role-based permissions let IT, Compliance, and Security manage their domains. Tasks and reminders are assigned by control.

Integrate Risk With Compliance The Broader Compliance Ecosystem

Principle: Risk analysis shouldn't live in isolation; it should connect to policies, vendors, workforce compliance, and incidents.

Why it matters: Fragmented tools and spreadsheets create gaps. Regulators evaluate the whole compliance program, notjust one document.

How Compliancy Group:

- **Vendor risk:** monthly OIG/state exclusion checks, contract/BAA tracking, due-diligence questionnaires.
- **Incident management:** anonymous reporting, digital case files, linkage back to risk register.
- **Policy & application inventories:** one system for audit-ready traceability.

Stay Current with Regulatory Change

Principle: Compliance requirements evolve; risk programs must evolve with them.

Why it matters: Static assessments quickly become outdated, leaving organizations exposed.

How Compliancy Group:

- **Built-in guidance:** for every control, updated as regulations change.
- **Regulatory notifications:** keep teams ahead of new requirements without extra consulting fees.
- **Monthly educational webinars and content:** extend the organization's regulatory intelligence.

Conclusion

As Daniel Lebovic pithily notes,

> **"compliance can be daunting and overwhelming, but a lot of things in the abstract are. When compliance is at the core of your business and you understand what you are doing, however, it becomes intuitive."**

With a structured, confident approach, compliance officers can use risk assessment to its full potential—highlighting potential danger areas and offering a clear response roadmap to mitigating risks and responding to incidents.

Book A Demo →

About Compliancy Group

Compliancy Group makes healthcare compliance simple. Our platform streamlines risk assessments, workforce compliance, and incident management—so your team spends less time on paperwork and more time on patient care. By simplifying complex requirements and documenting due diligence, we help you reduce risk, protect your organization, and build confidence with regulators, partners, and patients. Learn how our software can help you mitigate risk in your organization!

sales@compliancygroup.com

compliancygroup.com

Compliancy Group