Adopting RiskOps to Streamline Governance and Risk Management

日本語版も入手可能
www.isaca.org/currentissue

Risk management is integrated across all disciplines, and it requires an enterprisewide, top-down approach to become embedded into the decisions, actions and mindset of an organization—its culture. Highmark Health, a US$22 billion integrated healthcare enterprise headquartered in Pittsburgh, Pennsylvania, USA, had the strategic imperative to elevate its risk strategy, governance and operations due to rapid industry changes. It was bolstered by a transformational five-year strategy and the buy-in—from the board of directors (BoD) down to the internal stakeholders engaged with its risk functions—that it needed to deliver.

Highmark Health's new approach to risk management, risk operations (RiskOps), is built on four pillars:

1. Instilling a risk appetite determined by the (BoD) and senior management into business cases and project planning
2. Quantifying risk at all levels of assessment
3. Restructuring and streamlining risk and compliance committees to align with an enterprise risk taxonomy
4. Adopting the Three Lines Model (as established by the Institute of Internal Auditors [IIA])[1] and a RiskOps model that reduces decision cycle time and improves decision quality.

This case study provides insight into Highmark Health's transition and highlights some of its immediate process improvements, including capacity creation to address emerging risk, clearer decision rights to enable stronger corporate governance and relentless standardization.

Traditional Organizational Structure

Highmark Health historically oriented its risk operating model around subject matter specialties such as privacy, enterprise risk management, information security, accreditation and government compliance. This approach helped the organization manage emerging risk amid measured enterprise expansion and regulatory change. However, it inherently created limitations and inefficiencies in the day-to-day delivery and scaling of risk management. As risk became more complex and the pace of regulatory oversight accelerated, each of the subject matter specialty teams began to establish redundant parallel processes and implement divergent technologies to support risk identification, risk assessment and decisioning, and risk treatment and monitoring.

CHUCK DONINA | CISA, CCSFP

Is the senior vice president of risk operations at Highmark Health, an integrated healthcare delivery and financing organization. In this role he has oversight of global operational, technology, third-party and government risk and compliance, including business resilience, privacy operations, operational quality and the assessment of incoming laws, regulations and industry standards. In addition, his team supports the implementation and governance of multiple government, industry and customer compliance requirements ranging from regulations promulgated by federal and state agencies to third-party certifications such as System and Organization Controls (SOC) 1, SOC 2, Payment Card Industry, HITRUST and Cloud Security Alliance STAR and accreditations from the National Committee for Quality Assurance and the Joint Commission.

KATHLEEN S. HARTZEL | PH.D., CPIM, CSCP

Is an associate professor of information systems and technology at the Palumbo-Donahue School of Business at Duquesne University (Pittsburgh, Pennsylvania, USA). Her teaching and research interests include the management of attitudes and behaviors during system development and use, the effects of computer-mediated support on decision-making and attitudes, the impact of information systems on interorganizational cooperation and competition and information security education.

To bring these specialized teams together to provide cross-functional input for oversight, additional forums, such as committees, were mobilized to foster collaboration. Although the committees met their stated goals, they unintentionally slowed organizational processes and encumbered the speed of decision-making. With several years of committee proliferation—and with no established path for committee dissolution—Highmark Health found itself with more than 70 standing committees dedicated to overseeing one or more of the 40 risk groupings in the enterprise risk taxonomy. Several standing committees had evolved from project teams during mandated implementation and, as a result, were not vested with decision-making or issue-resolution authority. In practice, they acted more as forums for awareness. To complicate matters, many of the forums for awareness were embedded as required steps in processes, such as contracting and third-party onboarding, which prolonged cycle times.

> The divergent intake capabilities, frameworks, processes and tools inherently created duplicative oversight and inefficiency.

While committees filled operating model voids, each specialized risk oversight team concurrently constructed its own operational infrastructure to support the identification, assessment and decisioning, and treatment and monitoring of the risk relevant to its discipline. The divergent intake capabilities, frameworks, processes and tools inherently created duplicative oversight and inefficiency. Further, as business unit management established compliance and risk support teams and audit management gradually increased compliance oversight, the boundaries in the organization's adopted Three Lines Model began to unintentionally blur.

With healthcare being disintermediated by agile, consumer-centered technology enterprises (e.g., Google, Apple and Amazon), Highmark Health knew it needed to change. It was clear that there was an opportunity to improve organizational governance and risk management. The search for a better solution began with a strategic assessment. It was launched with goals of increasing the velocity and consistency of calculated risk taking, expanding organizational use cases for quantifying risk decisions and standardizing and streamlining risk management practices across all areas of the enterprise risk taxonomy.

Strategic Assessment: Anchoring to Risk Appetite

Defining the path and the operating model for faster, quantitative and standardized risk management required Highmark Health to ground itself in the risk appetite of its board and senior leaders. Through scenario-based workshops developed from its five-year strategy, the organization established tolerable boundaries for taking calculated risk for each category of its enterprise risk taxonomy. The output of those workshops included definition of a clear risk appetite aligned with the enterprise's strategic aspirations and establishment of an anchor point for governance, operating model sizing and oversight. In addition to an external market analysis, the policies, practices and perspectives of more than 70 leaders were compared to the risk appetite established by Highmark Health's BoD and senior leaders. Over a 10-month period, this qualitative input was solicited alongside a series of quantitative polling questions to provide a baseline for the efficacy of governance across the Highmark Health enterprise risk taxonomy. The feedback on governance effectiveness, correlated with a mapping of the departments and committees acting in the capacity of first, second and third lines of oversight, helped direct the assessment team to areas where risk decision-making was suboptimal, risk coverage was potentially duplicative and risk oversight blurred the Three Lines Model.

The market analysis and peer enterprise interviews reinforced a need for more purposeful adoption of the Three Lines framework. Moreover, the market analysis demonstrated that regulatory oversight of private insurance enterprises routinely lagged behind publicly traded banks by four to seven years (**figure 1**).

Four Pillars to Streamline and Simplify Risk Management

In anticipation of increasing examiner scrutiny over its alignment with the Three Lines Model, and armed with volumes of quantitative and qualitative leader feedback from its governance survey, Highmark Health isolated its four pillars required to address its objectives (**figure 2**):

1. Instilling the refreshed risk appetite from the board of directors and senior management into business cases and project planning
2. Quantifying risk at all levels of assessment
3. Restructuring and streamlining risk and compliance committees to clearly align with the Highmark Health enterprise risk taxonomy
4. Standardizing through adoption of the IIA's Three Lines Model and through RiskOps.

> Highmark Health began to explicitly build risk appetite scoring and guidelines into business cases and project planning templates.

Pillar 1: Cascading Risk Appetite

Highmark Health took several actions over the past decade that demonstrated it was an organization willing to accept calculated, mission-driven risk. For example, in 2013, it acquired a regional healthcare delivery system to preserve provider choice for its members in the US State of Pennsylvania. In 2015 and 2021, it created two affiliations with sister Blue Cross Blue Shield plans, expanding its reach into new regions of Pennsylvania and the US State of New York, respectively. In 2020, it entered into a transformative partnership with Google

FIGURE 1

Banking vs. Insurance Regulation and Oversight

In 2002, the US Sarbanes-Oxley Act became law.[a] The US National Association of Insurance Commissioners (NAIC) adopted similar internal control over financial reporting requirements under the Model Audit Rule in 2006 (2010 implementation).[b]

In 2008, US banking regulators issued final guidance for the supervisory review process over the capital adequacy requirements of Basel II.[c] The NAIC's Own Risk and Solvency Assessment (ORSA) requirements went into effect in 2015.[d]

In 2014, the Office of the Comptroller of the Currency (OCC) began overseeing bank implementation of the Three Lines of Defense risk governance framework.[e]

In 2020, the Three Lines of Defense governance framework evolved from an illustrative practice for mature risk functions to the Three Lines Model, a key consideration for all risk functions under NAIC oversight.[f]

Sources: a) United States Government Printing Office, 107th Congress Public Law 204, *Sarbanes Oxley Act of 2002*, USA, 30 July 2002, *https://www.govinfo.gov/content/pkg/PLAW-107publ204/html/PLAW-107publ204.htm*; b) National Association of Insurance Commissioners (NAIC), *NAIC Guide to Compliance with State Audit Requirements*, USA, 2010, *https://www.naic.org/documents/prod_serv_fin_receivership_gca_zu.pdf;* c) US Department of the Treasury, 12 CFR, Supervisory Guidance: Supervisory Review Process of Capital Adequacy (Pillar 2) Related to the Implementation of the Basel II Advanced Capital Framework, USA, 31 July 2008, *https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20080715a1.pdf*; d) National Association of Insurance Commissioners (NAIC), Own Risk and Solvency Assessment (ORSA), USA, 11 May 2022, *https://content.naic.org/cipr-topics/own-risk-and-solvency-assessment-orsa*; e) US Office of the Comptroller of the Currency, *Comptrollers Handbook—Safety and Soundness: Corporate and Risk Governance Version 2.0,* USA, July 2019, *https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/pub-ch-corporate-risk.pdf*; f) National Association of Insurance Commissioners (NAIC), Financial Examiners Handbook (E) Technical Group, USA, 12 November 2020, *https://content.naic.org/sites/default/files/call_materials/FEHTG%20Call%20Materials%2011-12-20_Updated%20%281%29.pdf*

FIGURE 2

Highmark Health's Four Risk Transformation Pillars

Pillar	Title	Objective
1	Cascading Risk Appetite	Empower all parts of the enterprise to deliver on Highmark Health's strategy within the guiderails set by its senior leadership team and BoD.
2	Quantifying Risk at All Organizational Levels	Enable leaders to take calculated risk, providing quantified insights on the range of outcomes from their decisions (avoiding confirmation bias).
3	Aligning Risk and Compliance Committees to the Adopted Risk Taxonomy	Streamline governance and oversight by aligning risk committees with Highmark Health's enterprise risk taxonomy, leveraging clear inform vs. decide frameworks and escalation paths.
4	Standardize Through Three Lines and RiskOps	Consolidate people, processes and technology to deliver risk identification, risk assessment and decisioning and risk treatment and monitoring activities in a standard way, assessing and producing multidisciplinary reporting.

Establishing a clear governance structure helped clarify where issues and risk needed to be elevated for broader socialization and where centralized approvals were required by enterprise processes.

Cloud to reengineer the healthcare delivery model between clinicians, insurers and patients/members. Despite this track record, the strategic assessment highlighted a separation between the risk appetite of the senior executive team and the tactical implementation of risk-related practices into some of the organization’s day-to-day business operations.

Compliance, risk mitigation and quality have always been core to Highmark Health’s business practices, but at the starting line of its strategic journey to “reinvent the health care experience,”[2] its leaders acknowledged a need to achieve those outcomes at scale and with accelerated speed. Specifically, a statistical majority of assessment participants felt that line management needed to be better empowered with data and tools to make more timely risk-based decisions, aggregated by and linked to organizational risk appetites.

To change this tactically, Highmark Health began to explicitly build risk appetite scoring and guidelines into business cases and project planning templates. Those scores and decisioning frameworks had always been a part of projects and investments that exceeded certain materiality thresholds, but applying those techniques broadly embedded the enterprise and business unit risk appetite into an expanded set of activities in a scalable way. Those scores are now leveraged as factors in investment decisions and escalatory data points for projects, and they are automatically aggregated against and aligned with enterprise and business unit risk tolerances.

Pillar 2: Quantifying Risk at All Organizational Levels

Cascading risk appetite consistently across all levels of the organization implies that risk is consistently and quantitatively measured. Prior to Highmark Health’s strategic assessment and due in large part to its federated operating model for second line activities, risk was assessed using different methodologies and frameworks and reported in myriad ways to its business leadership (e.g., critical/high/moderate/low, red/yellow/green, sometimes quantified, sometimes pseudo-quantified). As the organization sought to cascade its risk appetite consistently across its hierarchy, establishing a standard for quantification became foundational.

Piloting procurement contracting activities and leveraging decision analysis and capital modeling techniques adapted from its ORSA reporting, Highmark Health began to apply quantification techniques across all categories of risk in its enterprise risk taxonomy. Specifically, probability analysis leveraging measurable inputs—such as record counts at risk, product type, revenue at risk and quality score degradation—alongside traditional financial measures provided leaders with consistent, quantitative forecasts of a variety of potential outcomes. In addition, these activities positioned the organization to be able to assign risk-taking limits to organizational roles, so that assuming risk beyond an individual’s limit of authority (individually or in the aggregate) necessitated higher-level approvals. Taking risk outside the bounds of enterprise or business unit risk appetite could be restricted and escalated.

Pillar 3: Aligning Risk and Compliance Committees to the Adopted Risk Taxonomy

Applying risk-taking limits of authority provided some assurance that qualified decisions were being made at the right levels, guided by established tolerances. Even with those boundaries in place, Highmark Health’s legacy committee structure prolonged decision-making, extending cycle times for several dependent outcomes, including contracting and deciding risk mitigation activities. After evaluating the 70-plus internal committees charged with governing the enterprise risk taxonomy, Highmark Health undertook a multiyear program to redefine and simplify its oversight structure, ultimately targeting a future state of eight enterprise committees overseeing the risk taxonomy and redirecting or absorbing the legacy committee composition.

The eight committees (e.g., compliance and legal, security and resiliency) each were chaired by senior enterprise leaders ultimately accountable for the bundle of related risk factors in the taxonomy. The committees were administered consistently and had a direct escalation path to the broader senior management team and the board of directors. Establishing a clear governance structure helped clarify where issues and risk needed to be elevated for broader socialization and where centralized approvals were required by enterprise processes. Further, it

LOOKING FOR MORE?

- Explore the *Risk Start Kit. www.isaca.org/risk-starter-kit*
- Learn more about, discuss and collaborate on risk management in ISACA’s Online Forums. *https://engage.isaca.org/*onlineforums

clarified decision rights for business leaders engaging in risk management and compliance processes.

Pillar 4: Standardizing Through Three Lines and RiskOps

Along with the transformation of broader organizational governance practices, the way Highmark Health operationally delivered risk, compliance, quality and other second line activities via its model began to evolve. Highmark Health next turned to establishing a clearer alignment with the IIA's Three Lines framework. The organization reexamined activities of internal audit, transitioning second-line activities not required by contract or law to be performed by internal audit to the teams operating in the RiskOps model. This freed internal audit to have greater flexibility with its workforce capacity, presenting an opportunity to refocus resources on emerging risk areas and strategic project assurance and providing independent auditing and monitoring of second line programs.

Modern RiskOps Operational Structure

Highmark Health examined second line activities—some previously delivered by leaders with audit responsibilities but the preponderance federated among business units that could provide "expertise, support, monitoring and challenge risk-related matters."[3] During evaluation of these activities, it became evident that although the frameworks, tools and resources involved in doing the work were unique, they were fundamentally more alike than different. Whether it was a government compliance function, a third-party risk management activity, an accreditation evaluation or an assessment of internal control over financial reporting, they all started with the identification of risk, which was then assessed and decisioned and, ultimately, reported, treated and monitored. The need for technical subject matter expertise would still persist, but the processes and technology could be standardized so that the work executed could be better defined, more repeatable and more consistent from team to team. This was the genesis of the Highmark Health RiskOps model for second line delivery.

Risk Identification

The first opportunity for normalization found in evaluating second line functions was risk identification. For example, consider that a state law, industry requirement or regulation was proposed or issued. Irrespective of the subject matter, Highmark Health needed to understand and scope the policy, process, people, technology and reporting implications of the changes, implement the changes and then define a commensurate compliance and monitoring program. Rather than requiring a business or technology leader to manage that externally imposed change one way for a Payment Card Industry Data Security Standard (PCI DSS) update and another way for a claim processing requirement promulgated by a government agency, for example, the RiskOps model centralized the intake, evaluation and dissemination of those changes with input from the legal department and outside experts as required.

> Once a risk was identified, the next opportunity for operating model normalization centered on risk assessment and decisioning.

Changes were evaluated and reported consistently, communicated, tracked to implementation and transitioned to the operating model function accountable for developing and operating the ongoing compliance program. Similarly, risk events such as a new engagement with a supplier, a new facility, a changing product or a new technology asset would be managed in standardized (automated or manual) ways through the intake element of the operating model. They would then be handed off to the next function of the operating model—risk assessment and decisioning.

Risk Assessment and Decisioning

Once a risk was identified, the next opportunity for operating model normalization centered on risk assessment and decisioning. In the legacy federated operating model, despite a consistent good faith effort to minimize disruption and coordinate across functions, business leaders were subject to audits, risk, compliance and quality assessment requests that were similar or duplicative. Sometimes those assessments arrived during peak times and—because each siloed second line function had a reporting format—findings were shared using a variety of qualitative and quantitative means to calculate risk. With risk quantification moving on a trajectory toward standardization in connection with Pillar 2, Highmark Health saw an opportunity to streamline and simplify second line interactions with business leaders via its operating model.

The SRPs at Highmark Health were the single points of contact for the senior leaders of the organization with a direct reporting line to the chief risk, audit and compliance officers.

Whether it was a risk event transitioned from the risk identification function of the operating model or a scheduled engagement or activity from an annual workplan, the targets of assessments (e.g., business processes, technologies, products, entities) frequently had similar or overlapping requirements. Beginning with available content such as the HITRUST Common Security Framework (CSF)—a health information compliance framework that normalizes US state, federal and industry compliance requirements[4]—Highmark Health broadened its scope, creating a unified risk and compliance framework that included operational, quality, accreditation, licensure and customer requirements arriving from, for example, the National Committee for Quality Assurance (NCQA), the Centers for Medicare and Medicaid Services (CMS) and the Joint Commission.

Integrating these frameworks into a common set of control activities aligned with business processes and technologies positioned Highmark Health to perform multidisciplinary risk assessments encompassing financial, technology and operational, security, privacy, quality and compliance considerations. The assessment target could be evaluated once across all dimensions and reported to multiple internal and external stakeholders at optimal times. Coupled with the Pillar 2 quantification methodologies, the multidisciplinary risk assessments gave consistency and clarity to business leaders faced with strategic risk decisioning alternatives.

Moreover, consolidating second line activities and assessments in the RiskOps operating model inherently led to significant operational efficiencies, such as:

- Thirteen different vendor assessments were previously performed to evaluate the delegation, resilience, quality, safety, privacy and security risk of onboarded suppliers. They were combined, aligned and reduced to one nested questionnaire that addressed all risk and compliance-related items.
- The assessments identified more than 53,000 transactions that were audited by more than one resource. With combined assurance checklists, enhanced sampling techniques, and automation to identify the applicable frameworks for a particular claim, enrollment or customer service transaction, duplication was eliminated and resources could be freed to focus on higher-risk, higher-value activities.

Operating efficiencies were further complemented by streamlined delivery. With risk assessment processes standardized and agile working methods employed—such as operating in scrums or leveraging scrumban (a combination of scrum and Kanban techniques)—work item management became embedded into daily working routines, reducing cycle times.

Risk Treatment and Monitoring

Based on the assessment and quantification of risk, findings and recommendations were crafted and multidisciplinary reporting was standardized for stakeholder consumption. The final normalization opportunity identified was in the risk treatment and monitoring element of the RiskOps operating model. When polled, more than 100 employees performing second line activities were dedicating some percentage of their job to supporting ongoing risk monitoring. Because the legacy operating model was siloed, many of the tolerances and thresholds being monitored were overlapping and/or unsynchronized (e.g., compliance monitoring was mobilized quarterly for a metric another area monitored weekly), and the expediency of treatment triggered was inconsistent from team to team.

In the RiskOps operating model, a multidisciplinary risk treatment and monitoring team consistently measures, tracks and follows up on exceeded thresholds, findings and tolerances via centralized monitoring dashboards. New risk identified from monitoring is escalated to business leaders and returned for reevaluation to the risk intake and assessment and decisioning functions of the operating model. This inherently drives standardization and rigor across functional areas by ensuring, for example, that the documentation, escalation and tracking of items such as technical vulnerabilities are consistent with the documentation, escalation and tracking of compliance metrics or metrics with associated financial penalties.

Collaboration With Strategic Risk Partners

The last significant element of the operating model transformation was defining the strategic risk partner (SRP) role. Although risk identification, assessment and decisioning, and treatment and monitoring were largely standardized and centralized at that point, senior business leaders still expected a curated experience with the operating model. Acting in a capacity similar to a business segment risk officer, the SRPs at Highmark Health were the single points of contact for the senior leaders of the organization with a direct reporting line to the chief risk, audit and compliance officers. Concurrent with their governance and oversight role within the business units, the SRPs were consistent sources of new input based on information and strategies they became aware of as they participated in business unit leader staff meetings and business reviews. Their daily interactions with senior leaders helped ensure that the work performed in connection with the RiskOps model reflected the highest priorities of senior management and the BoD. Moreover, the SRPs were enabled to engage in meaningful interactions via the briefings provided and multidisciplinary reporting shared by the RiskOps team.

Conclusion

Mobilizing the RiskOps model is an organizational commitment. As Highmark Health shifted to the RiskOps model of delivery, certain enablers were identified as critical for transition:

- **Strict alignment with the IIA's Three Lines Model**—Centralization of second line functions into a RiskOps model leads to standardization of risk, compliance, quality, accreditation, licensure and similar activities, and it frees internal audit to focus discretionary time on emerging risk. Highmark Health experienced a 65 percent reduction in the internal time it took to deliver its third-party assurance reporting after converging teams in the RiskOps delivery model. Its internal audit team, no longer anchored by work assumed by the second line, increased the amount of engagement time spent on discretionary, strategic or emerging risk by more than 50 percent, to account for approximately 90 percent of the engagement hours in its internal audit plan.
- **Intersecting with the enterprise risk taxonomy**—Highmark Health purposefully connected its governance, delivery and operations to its risk taxonomy, enabling integrated visibility for its senior leadership and board of directors to a broad range of factors that could impact risk tolerances.
- **Knowledge management and talent management**—During the transition to the RiskOps model, well-documented procedures coupled with learning maps and a structured training curriculum were critical to advancing team skillsets and capabilities needed for multidisciplinary assessments. After subject matter specialists memorialized the more routine activities they performed in their roles, they were able to focus on the development of training collateral, practice aids and work programs. This expanded Highmark Health's network of experts freed upward of 30 percent of available hours from its annual plan to be performed through more leveraged staffing models or at alternate delivery locations.

> Ease of use drove broad adoption, while broad adoption drove better risk management outcomes.

For Highmark Health, these enablers made engaging with and managing outputs from the second line functions of the organization much simpler, more standardized and better streamlined. Ease of use drove broad adoption, while broad adoption drove better risk management outcomes and helped build a strong foundation for the advancement of its risk governance and culture.

Endnotes

[1] The Institute of Internal Auditors (IIA), *The IIA's Three Lines Model,* USA, July 2020, *https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf*

[2] Highmark Health, "Highmark Health Partners With Google Cloud to Raise Standard for Customer and Clinician Engagement in Health," 17 December 2020, *https://www.highmarkhealth.org/hmk/newsroom/pr/2020/2020-12-17-Living-Health.shtml*

[3] *Op cit* IIA

[4] HITRUST Common Security Framework (CSF), "Understanding and Leveraging the CSF," USA, May 2022, *https://hitrustalliance.net/understanding-leveraging-csf/*