

# Beyond Silos

Strengthening Operational  
Resilience with Integrated  
Risk Management



**ORIGAMI RISK**

# Table of Contents

Executive Summary	3
IRM: A Unified Approach to Enterprise Risk	5
6 Challenges and Actions for Effective IRM Implementation	11
Key Features of an IRM Technology Solution	14
What's Next for IRM?	15

# Executive Summary

Organizational silos pose a significant threat to coordinated risk and safety management efforts. These functional and departmental barriers restrict an organization's ability to operate from a single source of truth, blocking the context and insights necessary for fully-informed decision making.

Integrated Risk Management (IRM) is a strategy that offers a solution to these challenges by breaking down silos, fostering a comprehensive understanding of an organization's risk landscape, and driving actions that lead to improved operational and financial outcomes.

## What are the benefits of "Integrated Risk Management" for your role?

### Insurable Risk

Enhanced visibility into safety programs and operational activities across the organization can significantly reduce the Total Cost of Risk (TCOR) by minimizing claims costs, lowering insurance premiums, and optimizing risk management expenditures.

### Enterprise Risk & Compliance

Greater visibility into insurable risk and safety programs across the organization leads to stronger enterprise risk assessment, mitigation, and management, as well as improved compliance and audit trails.

### Safety

Tying safety programs to financial and enterprise risk, allows EHS professionals to gain more organizational buy-in on their initiatives, ultimately leading to a reduction in incidents and injuries.

By eliminating data silos, streamlining processes, and providing a holistic view of risk, software supports IRM efforts by helping organizations better plan for, mitigate, and manage insurable, uninsurable, and safety risks across the enterprise.

Enabling true IRM requires more than just piecing together disparate software systems. Realizing the cost and time savings that can accompany IRM requires reducing duplicative efforts and systems.

This eBook provides an in-depth exploration of the essential components of an effective IRM approach by:



Demonstrating why true IRM requires a unified platform within which all safety and risk (insurable and uninsurable) data can be shared between functions and across the entire enterprise



Exploring Risk Management Information Systems (RMIS), Governance, Risk and Compliance (GRC) systems, and Environmental, Health, and Safety (EHS) systems and the part each system plays in identifying, assessing, and managing organizational risk



Highlighting practical challenges and best practices for implementing an effective IRM strategy, from aligning risk and safety teams and objectives to leveraging technology wisely



Outlining the key technological solutions that play a role in IRM implementation, including automation, advanced data analytics, real-time data monitoring, and enhanced communication tools



Looking ahead to the future of IRM and how emerging technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics are revolutionizing risk management by helping leaders make more informed decisions, anticipate risks, and build adaptability into their risk management frameworks



# IRM: A Unified Approach to Enterprise Risk

Originally defined by the tech research and consulting firm [Gartner](#), Integrated Risk Management (IRM) is a business strategy that seeks to identify, assess, and manage an organization's existing and potential risks. It involves integrating risk management practices across various departments and business functions to create a holistic, enterprise-wide risk management framework.

Unfortunately, organizational silos present significant challenges to businesses' coordinated risk management efforts, as safety and risk teams often work in isolation, lacking coordination and communication with other departments. A study from the [American Productivity & Quality Center \(APQC\)](#) found that such silos result in wasted time looking for information, or silo taxes, of at least an hour per week by most surveyed workers. By restricting an organization's ability to operate from a single source of truth, these silos also block the appropriate context and data necessary for fully-informed decision making.

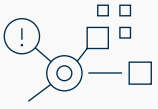
IRM software supports an organization's IRM strategy by "unsiloing" data to provide a comprehensive, enterprise-wide view of the risk landscape. By breaking down the barriers between different functional areas and data sources, organizations are able to aggregate and analyze information from across the enterprise. This context facilitates better decision making, drives preemptive actions and timely follow-ups, and ensures the right stakeholders are involved in risk mitigation processes.

Although every organization is unique, this often includes employing a combination of the following technology solutions to track and measure various risks: Risk Management Information System (RMIS), Governance, Risk and Compliance (GRC), and Environmental, Health and Safety Management (EHS).

However, enabling IRM is not as simple as stitching together different software systems. Many organizations try to create a semblance of integration by piecing together disparate applications. This "Frankenstein" assemblage of solutions is not only cumbersome to use and expensive to maintain but also lacks the seamless connection of data points required for the degree of analysis that underpins effective risk management. Achieving true IRM requires a single platform specifically designed to meet the functional needs of each area of business while sharing data across the entire enterprise.



# RMIS



**Risk Management Information System** software is designed to help organizations identify, assess, manage, monitor, and mitigate risk. It consolidates risk and insurance data, automates processes, provides analytical tools, and supports decisions for effective risk transfer strategies.



## Role in IRM

### Data aggregation and analysis

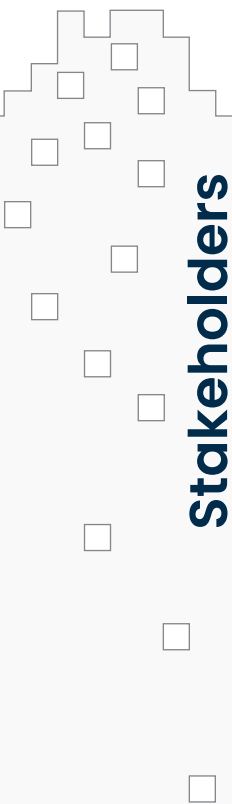
A RMIS is used to collect, store, and analyze risk and insurance data across an organization. This includes data related to incidents, claims, policies, and more.

### Reporting

Dashboards and reports help in monitoring risk exposure and performance. By integrating data from various sources, a RMIS contributes to a holistic view of risk for a variety of audiences.

### Decision support

A RMIS supports streamlined decision making by providing insights derived from comprehensive risk data analysis.



## Stakeholders

**Risk managers in compliance, insurance, operations, HR, and other departments** rely on RMIS software for identifying, assessing, and mitigating risk.

**Executives and senior management** utilize RMIS reporting and dashboards for strategic decision making and risk oversight.

**IT department professionals** are responsible for performing technical evaluations and security assessments of RMIS solutions to ensure compliance with organizational IT policies.

**Business unit and field employees** contribute data and may use RMIS tools for reporting incidents or accessing risk information.

**Vendors and partners** may interact with the RMIS for data exchange, reporting, and collaborative risk management.

# GRC



**Governance, Risk and Compliance** systems are designed to manage an organization's governance processes, risk management, and regulatory compliance. This software is used to help organizations achieve their objectives, address uncertainty, and act with integrity by streamlining workflows, ensuring consistent policy adherence, mitigating risks, and providing a holistic view of the organization's risk posture and compliance status.

## Role in IRM

### Governance

GRC systems help establish, enforce, and monitor organizational policies and procedures, and provide structures for decision-making processes.

### Risk management

These solutions facilitate the identification and evaluation of risks across various domains, including financial, operational, strategic, and IT risks.

### Compliance

By facilitating audits and providing assurance that compliance requirements are met, or identifying gaps and areas for improvement, these solutions help establish and maintain alignment with regulations and policies.



## Stakeholders

**Risk and compliance officers** are responsible for implementing and managing GRC systems to identify, assess, and mitigate risks, and ensure compliance with regulations. Monitoring compliance and risk management processes and reporting on their effectiveness are also key components of this role.

**Boards of directors and executives** use GRC systems to ensure that policies align with strategic objectives and to oversee risk management and compliance activities. They rely on GRC data and insights to guide informed decisions and manage accountability.

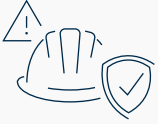
**Employees** adhere to organizational policies and procedures, report risks, and comply with regulatory requirements. Participating in training and awareness programs, facilitated by GRC systems, fosters a culture of compliance.

**Vendors and partners** are expected to comply with the organization's GRC policies and standards, and play a role in ensuring that their products and services do not introduce additional risks. Third parties engage with the organization through GRC systems for monitoring compliance and managing risk in their supply chain.

**Regulatory bodies** set and enforce regulations and standards, which can be monitored and managed through GRC systems that support inspections and reviews to help ensure organizational compliance.

**Internal audit** teams conduct audits to evaluate the effectiveness of GRC processes and provide assurance and recommendations for improvement based on findings.

# EHS



**Environmental, Health and Safety** management systems are the structured technology frameworks and tools that organizations use to manage their environmental responsibilities, workplace health, and safety protocols. These systems are designed to ensure compliance with regulations, promote a safe working environment, and minimize environmental impact through systematic processes and continuous improvement practices.



## Role in IRM

### **Risk identification and assessment**

EHS systems identify potential hazards to employee safety (unsafe working conditions and exposure to harmful substances) and environmental risks (pollution, waste management, and resource consumption).

### **Compliance and incident management**

Software can be used to ensure adherence to EHS regulations and provide tools for reporting, investigating, and analyzing incidents.

### **Performance monitoring and reporting**

Continuous monitoring of EHS performance through audits, inspections, and metrics provided by these systems ensures compliance, identifies areas for improvement, and supports transparency.



## Stakeholders

**EHS and safety professionals** responsible for creating a proactive safety culture use EHS systems to reduce incidents and injuries and maintain compliance with regulatory bodies.

**Employees and contractors** rely on EHS systems for a safe and healthy working environment through tracking participation in safety training, managing compliance activities, and reporting of unsafe conditions.

**Management and executives** who set the values and cultures as it relates to safety at the organization leverage data and reports to make informed decisions about a safety program's impact on areas such as the bottom line, retention, and reputation.

**Regulatory bodies** such as government agencies and industry regulators that set EHS standards conduct inspections and audits to ensure organizational compliance with regulations facilitated by EHS systems.

## The Intersection of RMIS, GRC, and EHS Technology on a Single Platform

RMIS, GRC, and EHS systems are designed for identifying, assessing, and managing risks to help ensure an organization is operating efficiently and can meet its business objectives with minimal disruptions. However, their potential is only fully realized when they are unified on a single platform that inherently fosters information sharing between functional units and stakeholders.

The friction caused by using multiple, unconnected systems can result in inaccessible critical data, operational inefficiencies, and a degraded decision-making process. [Research conducted by Forrester Consulting](#) on behalf of a micro-application solution provider found that 65% of employees ignore data for making decisions when they must pull it from multiple systems.

With insights drawn from a single source of truth, safety, risk, and compliance professionals, alongside leadership, can identify overlapping risks, ensure common blind spots are covered, and identify opportunities for win-win scenarios.

### How various stakeholders benefit when risk and safety data is in a single system

#### Safety Leaders

- Tie safety program to concrete financial data
- Leverage financial data on safety programs to gain internal buy-in, investment in safety initiatives, and executive support of safety culture, ultimately preventing incidents and injuries, improve productivity, ensure compliance, and reduce downtime

#### Risk Leaders

- Track the impact of safety programs on total cost of risk, negotiate reduced premiums, and streamline broker communications
- Maintain business continuity and operational resilience with data insights into risks and controls across the enterprise
- Fortify a risk-aware culture


#### Organizations

- Cut costs by eliminating duplicative efforts and systems
- Increase process efficiencies with integrated workflows
- Simplify risk IT stack
- Receive better continuity of implementation and services with a single vendor

## Success Spotlight



The Cheesecake Factory's  
Unified Risk & Safety Team

[View Case Study](#) 

The size and scale of the Cheesecake Factory's operations across 318 restaurants and 55,000 staff members presented deep stress on their risk and safety professionals, who were being asked to dig across multiple systems and departments to influence safety throughout the organization. Along with streamlining their processes, the team was looking for a tool to help better incentivize their staff members around safety initiatives.

Partnering with Origami Risk, the Cheesecake Factory started by integrating their RMIS and EHS data in a single system. Through a unified platform, the risk and safety teams can track training, program participation, and other safety-related compliance requirements. The public dashboards allow teams to visualize current initiatives, wins, and areas for improvement at the location level, and easily share information across the organization. A comprehensive allocation program was developed and enabled by this new system as well. Proactive safety measures to reduce the risk of frequency and severity of incidents and injuries, such as documenting safety training and meetings, in addition to utilizing nurse triage at the time of an injury, choosing approved medical providers for treatment, and follow-up actions like documenting incidents all helped locations reduce their base allocation charge. Combining allocations with a safety program, all within a tool that allows management to monitor its effectiveness and gain insight, has proven to be an effective way of aligning the company's goals with performance.

## 6 Challenges and Actions for Effective IRM Implementation

Implementing IRM presents a variety of challenges that can differ significantly from one organization to another. IRM strategies and the software supporting them must be tailored to how each organization's risk management, safety, and compliance functions are aligned. Equally critical is the organization's risk culture – whether risk management is perceived as a collective responsibility or solely the domain of a specialized team.

Here are the most common challenges organizations face and the necessary actions to take when implementing effective IRM:



### Challenge

**Lack of communication and collaboration.** Often risk and safety managers don't report to the same people, work in silos, or simply don't want to share data. However, as both risk and safety professionals have a shared goal of reducing risks and incidents across the organization, enhancing processes, and ensuring data integrity, it's beneficial for them to establish a good working relationship.



### Best Practices

**Align on shared goals, communicate information that can benefit both parties, and work together towards mitigating risks.** Collaborate on an integrated charter that outlines shared goals and outcomes to better mitigate risks and reduce incidents across the business.



### Challenge

**Letting terminology, definitions, and existing practices get in the way of collaboration.**

One of the most significant challenges is developing a formal risk management framework and standardized risk nomenclature that all departments and stakeholders can get behind. Without a unified approach, the risk management efforts can become fragmented, undermining the overall effectiveness of the IRM program and potentially increasing the organization's exposure to unmanaged risks.



### Best Practices

**Set aside a "this is the way we've always done it" mindset to establish a centralized and comprehensive risk management framework that includes standardized risk nomenclature and clear guidelines.** Consistent processes for identifying, assessing, and reporting risks must be established, as well as collaboration and communication channels to ensure that everyone is aligned and engaged in risk management efforts. A unified approach from the start helps prevent fragmentation, enhances the effectiveness of the IRM program, and reduces the organization's exposure to unmanaged risks.



### Challenge

**Lacking an enterprise-wide risk-aware culture.** When risk management isn't perceived as a collective responsibility across an enterprise, if it is seen as the exclusive domain of a specialized or independent team, or if employees fear retribution for reporting risks rather than viewing such actions as valuable data for improvement, it can significantly jeopardize the success of an IRM approach.



### Best Practices

**Securing leadership buy-in aids in providing the authority needed to initiate IRM efforts; building a sustainable culture of risk management requires action.** Leadership must follow through with allocation of resources, continued engagement with risk team members, and setting the tone for the entire organization to achieve the risk mitigation and cost and time benefits of an IRM program.



### Challenge

**Unrecognized value of IRM.** When the organization's leaders and change makers don't see the benefits of an IRM strategy, other organizational initiatives will take precedence. This results in insufficient resources being allocated to identify risk and maintain the program.



### Best Practices

**By tailoring metrics to the organization's risk profile and strategic IRM goals, the benefits become more apparent.** Benchmarking and KPIs offer a standard for measuring risk management performance, highlighting successes, and identifying areas for improvement. Each organization should tailor metrics to align with its unique risk profile and strategic goals, and review them regularly.



### Challenge

**Resistance to change.** IRM implementation requires a change in existing policies, processes, and procedures across the business. That type of change can be scary for employees who have negative past experiences or fear of automation replacing them.



### Best Practices

**Success in navigating this resistance hinges on effective training and change management.** Providing targeted training and support by the risk and safety manager(s) championing the IRM program, including specialized sessions on new technologies, can help ensure that all parties are well-prepared to utilize new systems and practices effectively. Regular meetings between the risk and safety manager(s) and analytics teams can help address any issues and demonstrate the impact of new tools.



### Challenge

Ownership of compliance regulations. The regulatory landscape is always evolving, often creating a complex web of compliance obligations, subjecting organizations to high levels of scrutiny and potential confusion over ownership of meeting compliance mandates.




### Best Practices

Fostering a connected risk and safety culture helps the organization stay agile and responsive to changing regulatory environments. Open communication, personal relationships, and connecting initiatives to individual roles rather than just organizational goals will aid in making these programs successful.

## Success Spotlight



McCarthy Building Companies  
Mitigation Action Planning  
(MAP) Program

[View Case Study](#) 

From humble beginnings in Ann Arbor, Michigan, McCarthy Building Companies now participates in over 200 construction projects annually. As McCarthy grew, the organization realized the foundational processes they built around risk management were tedious and time consuming, and unsustainable in their highly-regulated industry. McCarthy needed a robust technology solution to streamline processes and enhance compliance.

In partnership with Origami Risk, McCarthy developed a Mitigation Action Plan (MAP) program configured to the organization's rigorous objectives and compliance standards. The program connected their RMIS, enterprise risk management (ERM), safety data, and audit technology, building fully-automated risk identification, project briefs, and connected views of risk, insurance certificates, and risk action plans. This enabled McCarthy to see a full risk profile and allow the team to best identify where risks exist and how successful the organization is at managing them. The interconnected system and capabilities across internal teams improved efficiencies as well, decreased the likelihood of regulatory fines or penalties, and facilitated productive relationships with team members, business partners, and clients alike.



# Key Features of an IRM Technology Solution

The following are the key features of technological solutions that form the foundation of a robust IRM technology solution:

## ☆ **Automation of Administrative Tasks**

One of the primary advantages of IRM technology solutions is the ability to eliminate repetitive administrative tasks through automation. This includes automating risk assessments, data collection, alerts and notifications, task management, and reporting. Automation enhances efficiency, reduces the likelihood of human error, and ensures that critical tasks do not slip through the cracks. However, to prevent the creation of additional layers of complexity, automated workflows must be based on good processes and the tools used to configure workflows should be user friendly. The right balance ensures that risk and safety professionals can focus more on strategic activities and high-value insights rather than managing cumbersome software or administrative tasks.

## ☆ **Advanced Data Analysis**

IRM technology solutions leverage advanced data analysis tools to detect patterns, forecast risks, and quantify potential losses. These tools provide deeper insights into risk factors and help in making more informed decisions. By analyzing vast amounts of data with these tools, the technology can identify emerging risks and trends that might not be apparent through traditional methods.

## ☆ **Real-Time Data Monitoring**

Real-time data monitoring allows organizations to track and analyze risk indicators as they arise. By providing up-to-date information, real-time monitoring enables prompt responses to adverse changes, helping to mitigate potential impacts or capitalize on opportunities. This dynamic approach to risk management supports both preventative and strategic actions.

## ☆ **Enhanced Communication and Collaboration**

Effective risk management requires seamless communication and collaboration among various stakeholders. Technological solutions facilitate this through online portals, messaging platforms, shared dashboards and reporting, and document-sharing tools. These collaborative features ensure that all relevant parties are swiftly informed and aligned regarding potential risks and mitigation strategies. This enhances transparency and coordination across the organization.

## ☆ **Go Beyond Integrating Systems**

To maximize effectiveness, organizations need to adopt an IRM solution that is truly a single, unified system. This ensures that safety programs and risk management activities are operating from a single source of truth and that processes can be tightly interconnected. This eliminates the struggles of working from disparate systems and solutions, and provides a comprehensive view of risk and safety data to guide assessment, mitigation, and management activities.

## What's Next for IRM?

Risk and safety management is moving beyond traditional roots. IRM helps organizations respond to the rapid pace of change and increasing intricacies of global and operational environments. As discussed in the [2024 State of Risk Report](#), organizations must address the growing threat of novel and emerging risks impacting organizations in new and unforeseen ways.

Emerging technologies, including AI, are revolutionizing risk and safety management processes. These technologies combine big data and predictive modeling to enable organizations to make more informed decisions and anticipate future risks. Having your data in a single system can help your organization be more ready to adopt these new technologies. However, more data doesn't always lead to better insights; the key lies in filtering through the noise to extract actionable intelligence that can drive effective and efficient strategies.

Jumping on the tech bandwagon without considering the specifics of the program and processes that the technology needs to empower can lead to investment in solutions that may not align with an organization's needs and, ultimately, lead to ineffective risk management practices.

To best align new technologies with the unique risks and strategic objectives of an organization, ask these critical questions:

- What are our strategic goals?
- What technologies are necessary to achieve these goals?
- How can we leverage these tools to manage risks effectively?

As you engage in strategic planning, consider not only how to address current risks, but also how to build resilience and adaptability into your risk management framework. By anticipating future risks and aligning your strategies with emerging technologies, you can better prepare for uncertainties and ensure that your risk management practices remain robust and responsive.

# Interested in learning more about how Origami Risk can help support your IRM program?

Download our **integrated platform solutions** brochure: [origamirisk.com/IRMsolutions](http://origamirisk.com/IRMsolutions)

## Incident Intake & Processing

From the initial collection of incident details to analysis of the effectiveness of change management initiatives, Origami helps clients transform the way they report, track, and respond to incidents.

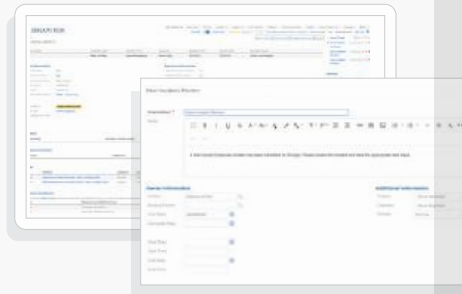
Web Portal & Mobile Intake Forms

Grant Access Links

Automate Investigations, including Root Cause Analysis (RCA) & Corrective Actions

Incident Triage & Electronic Reporting to Carrier/TPA

Loss Control, including integration with EHS suite



## Policy & Renewals Management

Origami tracks all policy and program details for all lines of coverage captured in the system, including policy, carrier, and broker information, terms, limits, named insureds, perils and exclusions, and any other client-defined data field required. Scanned policy documents and endorsements can be attached to the policy record, making it easy to access policy details at any time.

Certificate of Insurance (COI) Tracking

Outbound Certificate Requests Automation

Claims Integration

Automated Renewals

Policy Analysis & Modeling, including Policy Erosion, Coverage Levels, Retention Scenarios & Counterparty Exposure

Broker Access

Vendors & Contracts Governance



## Integrated platform solutions

**RMIS**

Risk Management Information System

**GRC**

Governance, Risk and Compliance

**EHS**

Environment, Health and Safety

**Improved Insights & Outcomes**  
Through **Inherently Connected Data**

 **ORIGAMI RISK**

## About Origami Risk

Origami Risk provides integrated SaaS solutions that simplify risk, insurance, compliance, and safety management. Origami delivers its highly configurable RMIS, GRC, EHS, and Healthcare risk management solutions from a secure, scalable platform that includes tools for centralizing data, automating critical workflows, and providing insight into risk and safety initiatives. A singular focus on client success underlies Origami's approach to developing, implementing, and supporting their innovative, award-winning software. For more information, visit [origamirisk.com/risk](http://origamirisk.com/risk).



**ORIGAMI RISK**