CASE STUDY

Building a Rock-Solid ERM Culture on FAIR

Rock Holdings, Inc., is a US-based holding company which owns several subsidiary companies including Quicken Loans, the US's largest mortgage lender. Due to strategic, operational and regulatory requirements, Rock Holdings has implemented quantitative risk analysis using Factor Analysis of Information Risk (FAIR). Over time, Rock Holdings' FAIR implementation transformed the business' enterprise risk management (ERM) program and risk culture. Along the way, Rock Holdings' Keith Weinbaum, an enterprise risk management architect and thought leader, has led the Rock Holdings enterprise risk team.

Introduction

A risk culture consists of the social and organizational backdrop for how an organization manages risk. In an effective culture, business risk owners are well informed about potential issues and are accountable for them. The owners are able to integrate considerations into managing value-producing business processes and strategies. They can express their risk appetite to technical and operational teams and, at a high level, direct the risk treatment strategies those teams take.

Risk Context

Many practitioners may be concerned primarily with information risk. However, organizations can benefit from creating an integrated risk management approach across information risk and ERM. The trick is to manage risk in the language of the business. That "language" is dollars, euros, yen or whatever local currency is used. The quantitatively oriented FAIR standard provides the analytical machinery to do this.

Risk Terminology

Risk (per FAIR)—The probable frequency and probable magnitude of future loss

FAIR—Factor Analysis of Information Risk

Information risk—Risk of business losses due to IT operational or cybersecurity events

Risk appetite—The level of risk an enterprise will take in an effort to accomplish its mission

Enterprise risk management—The methods and processes used by organizations to manage the business risk universe (e.g., financial, operational, market) and to seize opportunities related to the achievement of enterprise objectives

Dan Blum, CISSP, Open FAIR
Is an internationally recognized strategist in cybersecurity and risk management. His forthcoming book is *Rational Cybersecurity for the Business*. He was a Golden Quill Award-winning vice president and distinguished analyst at Gartner, Inc., has served as the security leader at several startups and consulting companies, and has advised hundreds of large corporations, universities and government organizations. Blum is a frequent speaker at industry events and participates in industry groups such as ISACA®, FAIR Institute, IDPro, ISSA, the Cloud Security Alliance and the Kantara Initiative.

Keith Weinbaum, CISSP, Open FAIR
Has worked at Quicken Loans for 20 years and is currently an enterprise risk architect. He built the information security function and led it for 10 years. From there, he built the enterprise risk management function which he led for six years. He oversaw the implementation of FAIR, which has been a centerpiece in how most risk is measured enterprisewide. As an architect, he now exclusively focuses on improving risk management-related processes and technologies.

The discipline used in the industry to manage risk culture at the enterprise level is called, appropriately enough, enterprise risk management (ERM). ERM processes plan, organize and lead activities to minimize risk impact on the business assets, revenues or earnings. ERM includes financial, strategic and operational risk and the risk of accidental losses.

Most organizations now operate as digital businesses with high reliance on IT. They can benefit by targeting overall risk reduction as a goal as opposed to focusing on meeting IT compliance obligations. Visibility into the overall security of the organization plays an important role in establishing this new dialog.

In recent years, investors and government regulators have begun to scrutinize the management policies and procedures of many different businesses. In some industries, boards of directors (BoDs) are now required to oversee and report on the adequacy of a business's risk management processes. In financial services, regulatory authorities such as the US Securities and Exchange Commission (SEC), US Federal Financial Institutions Examination Council (FFIEC), the US Consumer Financial Protection Bureau (CFPB) and their counterparts in other jurisdictions mandate a formal ERM-like approach to risk management.

Rock Holdings provides a unique risk culture case study with a:

- Financial services company that includes Quicken Loans (the US's largest mortgage lender)
- ERM program that started with information risk management using FAIR and evolved through three stages to become a valuable ERM program now in operation at most of Rock Holdings' subsidiaries

Company Background

Rock Holdings, Inc., is the parent company of several financial technology (fintech) businesses. These companies include:

- **Quicken Loans**—The US's largest mortgage lender, which created the first fully digital mortgage experience (Rocket Mortgage)
- **Quicken Loans Mortgage Services (QLMS)**—A tech-enabled mortgage origination platform and division of Quicken Loans serving independent mortgage brokers, community banks and credit unions across the United States
- **Rocket Homes**—A digital home search platform that can match clients with high-quality, prescreened real estate agents nationwide
- **Rocket Loans**—An online personal loan platform
- **Rock Connections**—A national strategic marketing company specializing in outbound and inbound client service for numerous online and technology-based businesses

Risk Management Pain Points and Timeline

Acquisitions, growth, digital business and financial services industry security challenges have driven an ongoing evolution of risk management at Quicken Loans and Rock Holdings over the past eight years. **Figure 1** shows the overall timeline for establishing ERM at Rock Holdings as it dealt with the following pain points:

- Inability to communicate information risk in business terms
- Increasing financial legal and regulatory requirements for risk management
- Information risk not integrated into ERM
- Increasing risk complexity

Figure 1—Quicken Loans' and Rock Holdings' Risk Management Timeline

Risk Management Program Development Stage	Scope	Timeline
Security program using qualitative risk management	Quicken Loans	Prior to 2012
Risk management program began using quantitative analysis with FAIR for information risk	Quicken Loans	2012–2014
ERM program established, also using quantitative risk management	Quicken Loans	2013–2014
ERM program expanded to additional Rock Holdings companies	Rock Holdings companies	2017–2020

> DESPITE THE MAGNITUDE OF PROJECTS REQUIRING THAT MORE THAN 100 IT AND OTHER RESOURCES BE DIVERTED TO WORK ON CONFIDENTIALITY CONTROLS,…THE COMPANY ACCEPTED THE NEED ONCE IT WAS EXPRESSED THROUGH THE ERM PROCESS.

There were a number of stages to the effort and, in each stage, pain points were addressed.

Establishing Information Risk Management and ERM at Quicken Loans

At the beginning of the timeline in **figure 1**, Keith Weinbaum was the director of information security. In his operational role, Weinbaum requested budgets and resources from the Rock Holdings chief executive officer (CEO). However, there was not a proper process established to handle such requests.

Pain Point: Inability to Communicate Information Risk in Business Terms

Once a process was established, there was still dissonance between the information security team and leadership. Creating a dialog between the two teams, where both understood exactly what the other was talking about, took time. Although most security requests were approved, neither Weinbaum nor the CEO were satisfied with stock answers such as "Hackers might break in and wire themselves money or steal personal or financial information about our customers."

Weinbaum investigated multiple risk management methodologies and processes, such as COBIT®, the US National Institute of Standards (NIST) Special Publication (SP) 800-30 and OCTAVE. He concluded, "The best one for the quantitative analysis capabilities we knew we required was FAIR. It produced feedback that was easier to report back to leadership because it broke risk down to dollars and cents—a language both leadership and I understood completely." In 2012, Weinbaum received approval to hire two FAIR experts and began building an information risk management program.

Even at the early stages of Quicken Loans' risk management journey, quantitative risk management enabled security program evaluation and improvement. After establishing tools and methodologies, the team began an analysis to assess Quicken Loans' top information risk scenarios and the risk-reducing benefits of all major security projects. Before completing this exercise, the enterprise risk team pivoted to work on financial and operational risk for the ERM program, but the team eventually shared its prioritized recommendations for security projects. Weinbaum found that approximately 90 percent of the recommendations were for projects previously requested, but 10 percent were new projects. Also, 10 percent of existing projects were found to have insufficient risk reduction benefits and were then deprioritized.

Pain Point: Financial Legal and Regulatory Requirements for Risk Management

In parallel with the enterprise risk team's early efforts to quantify information risk, the legal and regulatory landscape was driving financial services companies such as Quicken Loans to provide better financial and operational risk management at the business level. As the CFPB pushed for formalized risk reporting and internal auditing, Quicken Loans' general counsel became a strong advocate for ERM.

However, when Quicken Loans launched an ERM project, Weinbaum and the team were concerned that the effort might adopt qualitative rather than quantitative risk management methodologies. In other words, a financial or operational risk scenario might be rated as "high risk" because it was assessed as a "4" on a scale of 1 to 5 rather than having a dollar value placed on it (i.e., annual loss expectancy of US$150 million and worst case loss estimate of US$450 million for a scenario despite a risk appetite of only US$100 million). After expressing these concerns to the CEO, Weinbaum's risk team was given the opportunity to lead a project working to create an ERM model for Quicken Loans based on FAIR.

From 2013 to 2014, the team instrumented risk analysis tools using FAIR methods for analyzing financial, operational and other business risk. The team found that working with executives on analyzing potential mortgage default rates and other financial risk scenarios they already understood quite well made it easier to get buy-in for using FAIR modeling terminology, calibrated estimation methods, Monte Carlo simulation and other features in the ERM context.

Pain Point: Information Risk Not Integrated Risk Into ERM

Only after working through the top business risk scenarios over a two-year period and getting the ERM to a steady state did the program turn its full attention to one of the major top information risk challenges with which every enterprise is familiar—the risk of a confidentiality data breach. Analysis showed that more work needed to be done to bring confidentiality risk down below the enterprise risk appetite. Despite the magnitude of projects requiring that more than 100 IT and other resources be diverted to work on confidentiality controls, such as reducing the volume of sensitive information stored within data repositories where data were not absolutely needed, the company accepted the need once it was expressed through the ERM process. "It was a major commitment for the company and there were many other things those resources could have been doing. I don't think we would have been able to get this level of buy-in without first having our methodology accepted by the executives for use on their turf, for financial risk challenges they already understood," says Weinbaum.

Expanding Rock Holdings' ERM Coverage

As Rock Holdings expanded and grew its stable of subsidiary companies and IT systems, it faced new management challenges.

> "WE SHOULD IMPLEMENT ERM SERVICES FOR ALL ROCK HOLDINGS COMPANIES."

Pain Point: Increasing Risk Complexity

Weinbaum explains the challenges Rock Holdings' executives faced in the mid-2010s: "Companies were getting more complex, stretching executives' knowledge and decision-making abilities. The CEO and general counsel saw the value of quantitative ERM and how it could enable Quicken Loans to make more informed risk decisions."

In 2017, Weinbaum's risk team was tasked with expanding the ERM program to the other subsidiary companies. The expectation was to utilize ERM to provide decision makers a better understanding of the risk in existing business processes and the business cases for new projects as well as improved confidence in risk-informed strategic decision-making. "We should implement ERM services for all Rock Holdings companies."

From this point, the Rock Holdings enterprise was truly on the road toward creating an enterprise risk culture.

How Rock Holdings' Risk Team Established Multi-Company ERM

Once given the go-ahead for the Rock Holdings ERM project, Weinbaum began rolling out ERM to each of the (then) six companies. Rollouts started with the CEO for each company, as follows:

- Meet with the company CEO for a 90-minute session, including a demonstration of ERM processes and quantitative risk management.
- Identify a risk champion to work with from each company.
- Conduct a 25-question survey with each company CEO and report results to the Rock Holdings CEO.
- Work with the champion and other stakeholders to list the core business processes, assess each process's key risk factors, and update company-specific policies or procedures as necessary to create a repeatable assessment process.
- Build support for working with any specialized company processes into Rock Holdings' governance, risk and compliance (GRC) systems' risk management functions.

Prior to beginning the rollout, the enterprise risk team prepared a high-quality ERM demonstration to gain company CEO buy-in and to show that the effort was worthwhile and would yield valuable results. The team showcased policy management, compliance management, audit management, vendor risk management and issue management in the GRC tool. The demonstration concluded by showing how quantitative risk management could tie all the other GRC elements together to provide visibility of future loss exposure (in US dollars).

The risk team operationalized and instrumented ERM for each company during six overlapping four- to six-month periods. Including the company-level champions and ERM or FAIR specialists already on staff, the core risk team grew to approximately 10

Enjoying this article?

- Learn more about, discuss and collaborate on risk management and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

people. Internal auditors and other stakeholders were also engaged. The team sent monthly email updates to the list of stakeholders from all companies.

Scoping the Risk

The Rock Holdings risk team utilized a concept called the Scoping Triangle to create a generic risk matrix for business processes:

- **Assets**—Business processes, information, applications, services, facilities
- **Threats**—External cyberattacks, physical attacks, internal abuse, errors, etc.
- **Effects**—Process completed incorrectly or in an untimely manner, experienced breach of confidentiality, etc.

As the team analyzed risk scenarios, it leveraged information from the Rock Holdings business continuity management (BCM) process; however, it needed to go deeper. For each company, the team assessed business processes' data in the GRC system from business impact assessments (BIAs), which included dependency maps and availability risk assessments for the most important IT systems. However, the risk team needed to perform additional deeper analyses using the Scoping Triangle criteria.

Overall Risk Assessment Process

The risk team employed the following risk and control assessment methodology to analyze business-process-related risk for key risk scenarios:

- High-level inventory and scoping
- Key risk and control identification
- Key control documentation and testing
- Risk analysis, evaluation and treatment
- Risk monitoring

Risk Analysis Process

During the analysis process, the risk team took careful steps to ensure that key risk areas identified were both:

- **Comprehensively exhaustive**—Avoiding missing any key risk areas
- **Mutually exclusive**—Avoiding double dipping

Working with information from BCM teams and other stakeholders, the risk team mapped company functions to processes. It met with process owners seeking a deeper understanding of interprocess dependencies, applications or third parties used, success factors, failure modes, incident histories, known risk and performance metrics.

The team worked with the stakeholders and risk champions to decide which processes to measure first and, in some cases, to chain risk scenarios together (i.e., an effect on one asset is a threat to another) and identify potential root causes of risk in each scenario. The team endeavored to minimize its time demands on the business. Often, rather than scheduling meetings, risk specialists would temporarily embed themselves within a business process team and observe the team running its process.

The risk team employed a business process modeling notation (BPMN) tool and trained many stakeholders and business analysts in the tool's language. The team loosely measured risk to see if they appeared likely to exceed significant inherent quantitative thresholds and labeled those that did as "key" risk factors.

> "OFTEN, RATHER THAN SCHEDULING MEETINGS, RISK SPECIALISTS WOULD TEMPORARILY EMBED THEMSELVES WITHIN A BUSINESS PROCESS TEAM AND OBSERVE THE TEAM RUNNING ITS PROCESS."

Current State

As of Q1 2020, the ERM process at Rock Holdings, Inc.:

- Fully integrates Rock Holding's fintech companies into the ERM process
- Covers financial, market, credit, operational and information risk categories
- Documents all key risk areas in the multicompany GRC system
- Analyzes key risk scenarios using a customized quantitative risk analysis tool inspired by FAIR

- Reports key risk analyses to executives via periodic meetings and risk reports
- Provides monthly status updates to most Rock Holdings executives via the audit and risk team (ART)

Executive decision-making at Rock Holdings is benefiting from the ERM process. Through the monthly ART process, company executives can review risk exposure with senior leaders of operational functions such as mortgages, finance, human resources (HR) and IT. The enterprise risk team works with operational leaders in advance to prepare risk measurements. At the ART meetings, ERM facilitates risk decisions in discussions with executives and senior leaders.

Weinbaum also references Rock Holdings' Epic Ideas process for strategic decision-making as a proof point of ERM's success. The Epic Ideas process evaluates any large project involving IT. When submitting an Epic Idea, each project team can choose cost reduction, risk reduction or revenue generation as the project's primary theme. Risk reduction projects undergo a quantitative risk assessment. In a few cases, such projects were found not to reduce risk enough and were changed or cancelled.

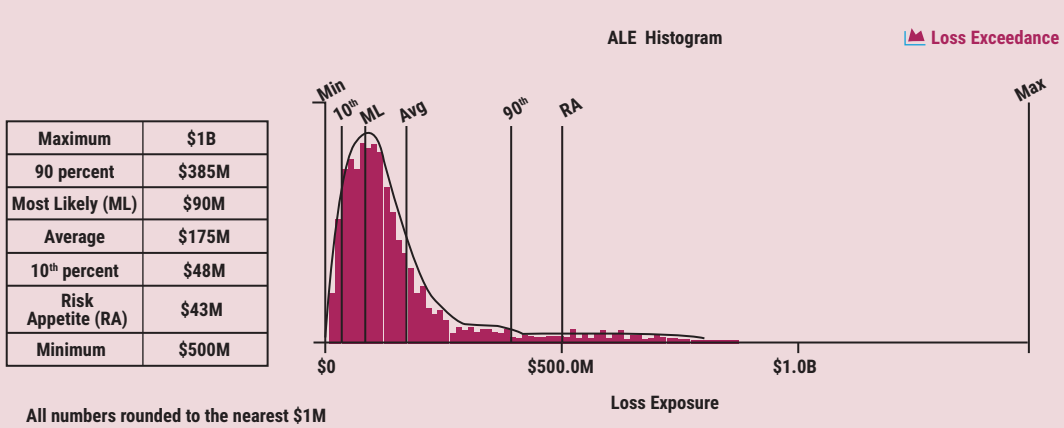
Not all Epic Ideas currently undergo quantitative risk analysis. ERM has a seat at the table for all the projects and performs less formal quantitative analysis on some revenue-increasing or cost-reducing projects on a case-by-case basis. As the Epic Ideas process continues to mature, Rock Holdings will likely want quantitative risk analyses performed on any proposed effort, regardless of its primary theme.

> "IN GENERAL, PROVIDING THE QUANTIFIED RISK INFORMATION IMPROVES DECISION-MAKING AND COMMUNICATION BETWEEN EXECUTIVES AND OPERATIONAL TEAMS IN THE BUSINESS."

In general, providing the quantified risk information improves decision-making and communication between executives and operational teams in the business. As noted earlier, risk appetite can be difficult to quantify or it may change based on business events or contexts. Having a number for the current risk at any given time enables executives to initiate a more informed conversation with operational teams.

Figure 2 provides a diagram representative of the risk measurements that Rock Holdings' enterprise risk team and other organizations' teams using FAIR can bring to the table. Risk analysts prepare calibrated estimates for more than a dozen FAIR model risk components including (at a high level) Threat Event Frequency, Vulnerability, Difficulty, Primary Stakeholder Impact and Secondary Stakeholder Impact. For each component, the model expresses estimates as a range with minimum, maximum and most likely data points. The risk measurement process performs Monte Carlo simulations on all these components using the ranges. It feeds them into a loss exceedance curve, as shown in **figure 2**, depicting aggregate minimum, maximum, average and, most likely, annual loss expectancy.

Figure 2—Sample Annual Loss Exposure (ALE) in US Dollars Histogram



Maximum	$1B
90 percent	$385M
Most Likely (ML)	$90M
Average	$175M
10th percent	$48M
Risk Appetite (RA)	$43M
Minimum	$500M

All numbers rounded to the nearest $1M

Metrics

Although Rock Holdings has not reached the point of tracking formal metrics yet, Weinbaum is able to provide data or estimates on many of the following metrics (**figure 3**) recommended for customers who use ERM projects**.**

Lessons Learned

It is instructive to review lessons learned—what went well, what could have been done differently—after reaching risk program milestones.

What went well:

- **Closely engaged with stakeholders on areas of the risk universe that are familiar to them.** Because the risk team met with each company CEO and other stakeholders multiple times, executives were well-prepared for the ERM process. Because the team began by surfacing deeper analyses of business process risk areas that executives were familiar with, such as mortgage underwriting, the team found it relatively easy to get buy-in for the quantitative methodology.
- **Worked with one company or business unit at a time.** To enable a small team to cover multiple companies (or business units), Rock Holdings introduced the ERM program to one company at a time and focused exclusively on risk areas at the business process level. "Don't boil the ocean," says Weinbaum.

What could have been done differently:

- **Provide just-in-time training, or refresher training at critical points in the transformation process.** Stakeholders were trained once and bought into the methodology, but training was not repeated before ERM reports were exposed at the group level. By that time, some stakeholders had forgotten key concepts and became confused. In hindsight, Weinbaum advises periodically refreshing or reorienting stakeholders on key quantitative risk management concepts from time to time if they have not been involved recently.
- **Use off-the-shelf quantitative risk management tools.** When Rock Holdings began Open FAIR implementation in 2013, the discipline was at a very early stage. Commercially available tools, training and implementation support are now more widely available from vendors and consultants. Weinbaum believes that if he were starting the project now, Rock Holdings would be better off not to build its own risk analysis tool.

Figure 3—High-Level Metrics Recommended for Quantitative Risk Management Programs

Metric	Rock Holdings Results Representative of the Metric
Percent of corporate divisions covered by ERM process	Approximately 60 percent (this number was higher prior to acquisitions)
Percent of IT projects undergoing risk assessment	100 percent of large IT projects that are focused on reducing risk undergo a quantitative risk
Percent of security projects undergoing risk assessment	80 percent of security projects that get worked on are now validated by quantitative risk assessments
Percent of stakeholders satisfied with ERM process	90 percent stakeholder agreement with risk treatments recommended after assessments
(Yes/No) Complies with regulatory requirements	Y
Dollar value of inherent risk exposure reduction due to risk program	Rock Holdings has reduced millions of dollars of loss exposure by its own measurements
Cost savings (dollar value)	Saved on canceled security projects or Epic Ideas
Number of trained risk specialists	10
Number of trained stakeholders, conversant with the methodology	Enterprise risk team and stakeholders are able to perform "on the fly" quick assessments using the FAIR model
Average time required to perform quantified assessment	Typical risk assessment takes two to four weeks depending on the scenario's scope

Benefits

Rock Holdings acknowledges the benefits from the ERM program to be that executives and senior leaders can:

- Focus primarily on revenue generation
- Always know their future loss exposure and what is being done about it
- Compare different types of risk on an apples-to-apples basis
- Gain efficiencies from implementing consistent risk processes across the organization

Conclusion and Next Steps

In a constantly changing environment with multiple business units, processes and systems, ERM will never be perfect. Likewise, the work of evaluating risk scenarios will never be "done." ERM is an ongoing process. Rock Holdings' goal is to expand it to all companies and to measure all key risk scenarios. The enterprise risk team will continue to implement each component of the ERM process consistently, find best practices and spread them to all the companies. It is also a team goal to perform risk management through a more automated, real-time process so that risk owners can see loss exposure estimates based on current data values rather than only through point-in-time briefings.

Although Rock Holdings will continue to require specialists to operate its risk assessment tools and to fully understand FAIR and related quantitative analysis methodologies, the company plans to better train additional staff outside of the ERM group in basic risk analysis skills. This training will raise the general level of knowledge about the methodology and processes to reduce biases, improve staffs' ability to provide calibrated estimates and enable the risk process to operate more efficiently.