Enterprise Risk Management as a Strategic Enabler of Organizational Performance

Final Research Paper

Alan B. Palayil

University of the Cumberlands

Course: ITS-835: Enterprise Risk Management

Instructor: Dr. Dustin Hutchison

Date: December 5th, 2025

Abstract

Enterprise Risk Management (ERM) helps businesses find, evaluate, and deal with uncertainty in a structured way throughout the company so they can achieve their strategic goals. ERM doesn't treat risk as a separate part of compliance. Instead, it makes it a part of governance, strategy, and performance management. This paper explains what ERM is and why more and more companies are using ERM tools to help them follow the rules, make decisions, and add value. It looks at big problems that come up when trying to implement it, such as cultural resistance, broken data, and weak IT governance. It also offers helpful advice based on well-known frameworks like NIST risk management guidance and COSO ERM 2017. For ERM to work well, there are also some important things that need to be in place. These include a clear risk appetite, strong governance, portfolio-level risk views, and alignment with IT risk practices. Lastly, it shows how to use ERM in strategic planning by using Eli Lilly as an example from the real world. The paper concludes that ERM, when regarded as a strategic management discipline rather than merely a checklist, can significantly enhance resilience, capital allocation, and long-term performance.

Introduction

Business has always had to deal with risk, but digital transformation, global interdependence, and more rules have made it much more expensive to not do so. Most of the time, traditional risk management only looks at certain risks, like credit losses, cyber incidents, and operational failures. It also only works with separate departments. Enterprise Risk Management (ERM) was created because this way of thinking did not work. It helps businesses see how risks affect all of their strategic goals.

This paper addresses six principal inquiries. It starts by explaining what ERM is and how it is different from regular risk management. Second, it tells businesses why they should use ERM apps and what they can expect to get from them. Third, it talks about the biggest problems with ERM and how to fix them. Fourth, it tells you what is most important for a good ERM program, like how IT governance and cybersecurity frameworks fit into it. Fifth, it looks at Eli Lilly, a real company that has used ERM in a way that fits with its overall plan. Lastly, it talks about where ERM practice should go in the future and gives suggestions for how to make it better.

What Is Enterprise Risk Management?

Enterprise Risk Management is a planned, ongoing way to find, assess, manage, and keep an eye on risks across the organization in relation to its mission, strategy, and goals. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) says that ERM is the "culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value" (COSO, 2017). This definition makes three important points: ERM is part of strategy, everyone in the organization uses it, and it is more about value than just protection.

Risk management that is done the old-fashioned way usually works in functional silos. ERM, on the other hand, tries to look at risk from a portfolio point of view. Bromiley, McShane, Nair, and Rustambekov (2015) contend that the unique value of Enterprise Risk Management (ERM) exists in its capacity to show interdependencies among risks and to contextualize risk decisions at the organizational level, rather than simply combining departmental risk registers. We need to change the tools we use to manage risk as well as the way we think, share information, and govern in order for ERM to work better.

The 2017 ERM framework from COSO breaks this area down into five parts: governance and culture, strategy and goal setting, performance, review and revision, and information, communication, and reporting. All of these parts are linked to each other. These parts are based on a set of rules that connect risk factors directly to strategic decisions (COSO, 2017). In other words, ERM is more than just one method; it's a management system that includes specialized risk models and controls.

Why Should an Organization Implement an ERM Application?

Companies want better performance, more openness, and more resilience, so they use ERM applications, which are technology platforms and processes that help with ERM. Research shows that companies that use good ERM practices get benefits in both financial and non-financial areas.

First, ERM helps improve performance by taking risks into account. Florio and Leoni (2017), in their examination of Italian publicly traded companies, found a positive correlation between the implementation of Enterprise Risk Management (ERM) and corporate performance. They said that ERM helps management and boards make better decisions by giving them more complete risk information. Hoyt and Liebenberg (2011) also found that insurance companies that use ERM programs have a higher firm value, even when size and other factors are considered. This means that people who work in capital markets think that ERM can make things worth more.

Second, ERM makes it more likely that regulators and other important people will trust you. Regulators want industries that are heavily regulated, like healthcare, financial services, and critical infrastructure, to do a better job of managing risk as a whole. Gordon, Loeb, and Tseng (2009) proved that synchronizing information security investments with a company's comprehensive risk management strategy results in superior and more rational control frameworks. ERM makes it easier to do audits, tests, and disclosures by giving this kind of alignment a clear structure.

Third, ERM makes it easier to make strategic decisions. Kaplan and Mikes (2012) said that ERM helps leaders figure out what kinds of risks they face, such as strategy risks, avoidable risks, or external risks. It also helps them pick the right tools for each kind of risk. By including risk scenarios in their strategy and capital planning, organizations can better weigh the pros and cons of different options, avoid putting too much or too little money into controls, and go after opportunities with a better understanding of the risks involved.

Finally, ERM makes it easier for people to talk to each other and hold each other accountable. Vincent, Higgs, and Pinsker (2017) discovered that organizations showing superior IT risk management practices and enhanced alignment between IT governance and enterprise risk processes showed a greater degree of overall risk management maturity. ERM applications can bring together risk inventories, KRIs, and incident data. This makes it easier for senior management and boards to see patterns that would be hard to see in separate areas.

Key Challenges and Solutions in Implementing ERM

There are many good things about ERM, but it can be hard to use. There are a few problems that keep coming up in both the literature and in real life. These include cultural resistance, unclear value propositions, fragmented data and systems, and a weak connection between IT risk and enterprise risk.

Culture is a big issue. A lot of people think that risk management is a way to make sure things are done right, which stops innovative ideas from coming up. Bromiley et al. (2015) say that ERM projects do not work when they are seen as more red tape instead of being a part of important management processes. To get past this, top leaders need to show their support, the message needs to be clear that ERM helps, not hinders, strategic goals, and there needs to be rewards for taking risks that are well thought out, not just for avoiding them.

The second problem is showing how useful ERM is. People who have a stake in the investment might not be sure about it because it is hard to put a number on how much better decisions and avoiding losses are. Research by Hoyt and Liebenberg (2011) and Florio and Leoni (2017) shows that value is a group idea, but each company still needs to make its own business case. Linking ERM to certain outcomes, such as more stable earnings, fewer unexpected losses, better ratings, or better use of capital, is one way to fix this. It can be helpful to keep track of risky events and near misses before and after ERM is put in place to see how things have changed over time.

The third problem is making sure that different data and risk functions can work together. A lot of companies are good at handling operational, financial, or cyber risk, but they do not do all three at the same time. NIST's SP 800-39 on organization-wide IT risk management says that everyone in the organization, mission, and system should be able to manage risk, with clear roles and ways to talk to each other (NIST, 2011). For ERM to work with these other frameworks, taxonomies, common risk scales, and shared tools must all work together. The course presentation on IT governance shows how NIST's Cybersecurity Framework and Risk Management Framework can help businesses manage risks in a consistent and tiered way.

Finally, there is the question of how people act and IT governance. Digital transformation has made IT risk a big part of business risk, but many boards and executives still see cybersecurity and tech issues as technical issues instead of strategic ones. Vincent et al. (2017) discovered that organizations in which the CIO directly reports to the CEO show superior IT risk management practices. This shows how important the structure of governance is. To fix this, it might be necessary to move talks about IT and cyber risk up to the board level, make sure that IT risk metrics match enterprise KRIs, and make sure that ERM apps give the visibility and aggregation needed for informed oversight.

What Is Important for an Effective ERM Program?

Both research and practice show that there are some things that all good ERM programs have in common.

First, they are based on culture and how things are done. COSO (2017) says that boards and senior management need to set the tone for risk awareness, figure out what level of risk is okay, and make sure that risk is always a part of managing performance and strategy. If the top doesn't make this commitment, ERM could turn into a separate job.

Second, they talk about what risk appetite is and how to use it. A clear risk appetite framework makes vague statements into specific numbers and limits, such as how much earnings can change, how much capital is at risk, or how much operational disruption is okay. Gordon et al. (2009) say that organizations can change their controls based on how much risk they are willing to take if they align their risk appetite with their information security investment decisions. ERM apps can help by setting limits, keeping an eye on KRIs, and starting escalation when those limits are crossed.

Third, good ERM programs look at IT and cyber risk when they look at the risks that the whole business faces. The NIST Cybersecurity Framework (CSF) 2.0 has five parts: Identify, Protect, Detect, Respond, and Recover (NIST, 2024). This structure can be used in ERM processes. The "Identify" and "Govern" functions are immensely helpful for businesses because they help them understand how IT assets and cyber risks affect their goals. This lets them be added to the enterprise risk registers. The IT governance course material makes it clear that good governance connects these frameworks to ERM so that IT risk is not dealt with separately but as part of the whole risk portfolio.

Fourth, good ERM programs are always looking for new ways to measure and make things better. Bromiley et al. (2015) say that some people don't like ERM because it isn't strict enough. But companies that use quantitative methods like scenario analysis, stress testing, and Monte Carlo simulations can better weigh the pros and cons. ERM apps can help with these analyses by keeping track of loss events and making it easier to learn from near misses and incidents.

Finally, good ERM is just a normal part of running a business. Kaplan and Mikes (2012) say that ERM works best when it is used in planning, budgeting, and performance reviews. This means that managers need to be careful about risk factors when they decide how to spend money and run the business. This means that the results of ERM need to be clear, prompt, and related to the decisions that are being made, not just by board committees or regulators.

Case Study: Eli Lilly’s Integration of ERM and Strategy

Eli Lilly is a big pharmaceutical company that people often use as an example of how to use ERM and strategy together. Do, Railwaywalla, and Thayer (2016) did a case study on how Eli Lilly set up a governance structure that closely ties ERM to ethics, compliance, and corporate strategy. The company set up a Compliance and Enterprise Risk Management Committee (CERMC) and an ERM Core Team with leaders from strategy, legal, compliance, and other critical areas.

One thing that makes Eli Lilly's approach different is that they hold ERM workshops at the same time as their yearly planning and budgeting cycle. Forty to fifty leaders from different business units and regions get together for risk workshops every year before big decisions are made about how to use resources (Do et al., 2016). This makes sure that risk information is up to date and has a direct impact on how projects are ranked, which portfolios are picked, and how much money is put into them.

Eli Lilly also has a set way to find and tell people about risks. Business units first look at their own risky landscapes to find problems that could have a significant impact on their goals. After that, the enterprise risk profile is changed to include any recurring themes or cross-cutting exposures. The CERMC then talks about these. This mechanism enables the company to transition from assessing risks individually to evaluating them collectively, aligning with the ERM literature's emphasis on the interconnectedness of risks (Bromiley et al., 2015; COSO, 2017).

Eli Lilly uses ERM to find both risks and chances to grow. Do et al. (2016) say that the company has begun to consider taking risks to get ahead of its competitors. This fits with COSO's definition of ERM as a way to make and protect value, not just cut losses. This is consistent with research showing that the implementation of ERM enhances performance and elevates market value (Florio & Leoni, 2017; Hoyt & Liebenberg, 2011).

Eli Lilly's story shows many of the same things we've talked about before: good governance and tone at the top, combining ERM with planning, looking at risk at the portfolio level, and knowing that risk can help or hurt strategic success. It shows that ERM can be more than just following the rules; it can also help you run your business.

Conclusion and Future Directions

Businesses that run-in complex, interconnected environments have gone from thinking about Enterprise Risk Management to needing it. Enterprise risk management (ERM) is the mix of strategy and performance with culture, skills, and ways of doing things. It helps us understand how distinct kinds of risks, like financial, operational, cyber, regulatory, and strategic, can work together to hurt an organization's goals. Studies conducted in diverse industries and countries

(Florio & Leoni, 2017; Hoyt & Liebenberg, 2011) show that organizations employing sophisticated ERM practices typically display enhanced performance stability and elevated firm value.

But it's not simple to put ERM into action. Companies need to get past cultural barriers, show how useful ERM is, combine different risk functions, and make sure that IT risk is in line with enterprise-level oversight. Governance structures, like the ones talked about in COSO (2017) and NIST's risk frameworks, make ERM better by making clear roles, processes, and information flows. Eli Lilly's case shows that when ERM is part of strategic planning and supported by cross-functional governance, it can help people make better choices and be more resilient.

As time goes on, ERM will need to change to deal with new risks, such as those from AI and algorithmic bias, climate-related financial risks, and cyber threats that are getting more complicated. More research can look into how ERM works with IT governance frameworks like the NIST Cybersecurity Framework 2.0 to help businesses manage the digital risks that are part of their overall risk views. Companies should be clear about how much risk they are willing to take, buy ERM software that helps with analytics and reporting, and make sure that the metrics for IT and cyber risk match up with the metrics for enterprise risk.

When people see ERM as a core management discipline instead of just a way to follow the law, it works best. When boards and executives use ERM to make decisions about strategy, where to put money, and the company's culture, they change risk management from a way to protect themselves into a way to get an edge over the competition.

References

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Journal of Risk and Insurance, 82*(3), 489–525. https://doi.org/10.1111/jori.12069

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance* (Executive summary). COSO.

Do, H., Railwaywalla, M., & Thayer, J. (2016). *Integration of ERM with strategy: Case study analysis*. Enterprise Risk Management Initiative, Poole College of Management, North Carolina State University.

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *The British Accounting Review, 49*(1), 56–74. https://doi.org/10.1016/j.bar.2016.08.003

Gordon, L. A., Loeb, M. P., & Tseng, C. Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy, 28*(4), 301–327. https://doi.org/10.1016/j.jaccpubpol.2009.06.006

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of Risk and Insurance, 78*(4), 795–822. https://doi.org/10.1111/j.1539-6975.2011.01413.x

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review, 90*(6), 48–60.

National Institute of Standards and Technology. (2011). *Managing information security risk: Organization, mission, and information system view* (NIST Special Publication 800-39). U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *Cybersecurity framework 2.0*. U.S. Department of Commerce.

Vincent, N. E., Higgs, J. L., & Pinsker, R. E. (2017). IT governance and the maturity of IT risk management practices. *Journal of Information Systems, 31*(1), 59–77. https://doi.org/10.2308/isys-51365

University of the Cumberlands, School of Computer & Information Sciences. (n.d.). *The critical role of IT governance in managing IT risk* [PowerPoint slides].