ERM and Mission Critical Risks

White Paper Series
St. John's University, Tobin College of Business
Greenberg School of Risk Management
Center for Excellence in ERM
Dr. Paul L. Walker
Schiro/Zurich Chair, Enterprise Risk Management

Mission Critical Risks

There are many things driving the enterprise risk management and board risk oversight process including SEC rules, stock exchange listing requirements, investor expectations, recommended best practices, and ultimately, meeting the needs of the board to fulfill their board risk oversight duty.

When evaluating board duties (and risk oversight) the Caremark case is the legal standard by which board duties are challenged. Boards are expected to exercise good faith and that is generally determined to mean that 1) the board implements a system of reporting and controls and 2) the board monitors the system. At the time of the Caremark ruling, enterprise risk management was in its infancy and was not considered or discussed in the court's ruling. However, rules, requirements, and expectations for managing risk have grown exponentially and the more recent cases frequently make risk and risk management part of their allegations. In the past, Caremark cases were difficult to win. Recently however, more Caremark cases are being filed and legal experts note that plaintiffs have been successful in 30% of Caremark cases.[1] This higher success rate necessitates a rethinking of enterprise risk management and board risk oversight processes.

One recent successful Caremark case (Marchand v. Barnhill) involved food safety and Blue Bell ice cream. According to the Delaware Supreme Court, the plaintiffs asked for documentation of the board's efforts on " the most central issues at the company: whether it is ensuring that the only product it makes - ice cream - is safe to eat." The court reiterated that a director is acting in bad faith if there is no effort to ensure that the company had in place any "system of control." According to the complaint, it was alleged that Blue Bell did not have a board committee on its *mission critical risk* of food safety, had no process to keep the board informed about this risk, did not schedule regular discussions at the board about this risk, that the board

[1] Alia et al. 2022. How to Structure a Board to Oversee Mission-Critical Activities. Docket.

was sometimes given positive information about food safety but was not given reports that showed the opposite, and that board meetings basically showed no regular discussion of food safety risks. All of this implied that the board had undertaken little or no effort.

Mission critical risks *must* (not may) be identified and addressed. Not doing so could have serious consequences. The court added (and perhaps defines mission critical risk for the first time) that food safety was "essential and mission critical." This definitely raises the bar because oversight systems now *must* cover essential and mission critical risks. Although the Blue Bell board was meeting with management, the case did not get dismissed because the board was not focusing on mission critical risks. Going forward, any oversight system must be designed to ensure adequate oversight of mission critical risks. This may not be the same as just having an ERM process.

In another recent successful case (In re The Boeing Company Derivative Litigation) the court noted that Boeing had a version of ERM but did not have a board committee for their number one risk, which was airplane safety. This implies that ERM is not sufficient to withstand these cases. The court also noted that the board committee charters did not mention this number one risk and that safety risk was not a regular agenda item at board meetings. Furthermore, the case alleges that enterprise risk management did not specifically emphasize safety risk and that the audit committee was not focused on airplane safety risk. Much of the case covers how Boeing was focusing on profits and rapid production, implying that the board had a misplaced focus (or at least a focus that shifted them away from their mission critical risk of safety). There is also a lot of discussion in the case about the fact that employees and management knew about the safety risk problems but that either the board did not know in some cases or was slow to get key information about safety risk related to the plane crashes.

Similar to the Marchand case, there is an overall emphasis on board risk oversight for essential and mission critical risks. For Boeing, it was noted that not only did the board not have a process or a committee for mission critical risk, but that it was also too passive. Evidence of

being too passive was that the board was not requesting enough information about safety risk and that the board was not challenging managements' conclusions about safety risk. It was also noted that when some reports about safety did come through from management they were ad hoc as opposed to having an official board process focused on safety risk.

Potential Implications and Lessons for ERM and Board Risk Oversight

One lesson from these cases is that an organization should have a conversation about defining and identifying mission critical risks. The courts appear to be using this concept more. Mission critical risk may or may not be on an organization's current risk register or set of enterprise level risks. Mission critical risks might be identified using traditional ERM approaches or perhaps nontraditional ERM methods. Using a COSO or ISO based ERM approach that identifies risks to objectives may not be the best way to identify mission critical risks. Perhaps a focus on the business model and value proposition, pre-mortem analysis, black swans, the value chain, or the value system outside the organization might be helpful in highlighting potential mission critical risk.

Another Caremark case (in 2019) identified a certain product as a mission critical product (In Re Clovis Oncology). For tech companies, mission critical could be privacy or it could be general cyber security. It might also be their key product. In the current environment perhaps mission critical risks are country or supply chain concentration, reliance on third-parties, or energy dependencies. One company may actually be a mission critical risk to another company. For other companies mission critical may not be clear and what is troublesome is that mission critical risk could change overtime. My reading of these cases is that a "system" that doesn't cover mission critical risks is considered not much of a system. The enterprise risk management and board risk oversight lesson seems to be that boards must know their mission critical risk and rigorously exercise oversight for those risks. The cost of not taking this approach is significant to the company and the board.

Another lesson is to not let a poorly designed enterprise risk management process become part of the case. These cases closely review the ERM and board risk oversight process that was in play at the time of the complaint. In one Caremark case the plaintiffs used how ERM was set up and all the related ERM documents to try to imply bad faith (including the CRO duties and reporting levels). Common solutions for this are to benchmark your enterprise risk management process, compare your process to both COSO and ISO, get an outside review of your enterprise risk management process, or perhaps get an audit of your enterprise risk management process. The COSO framework includes discussion of how to evaluate an enterprise risk management process and even goes on to add that organizations should seek continual improvement in that enterprise risk management process. Make sure your ERM process is good and let the board know.

Once all the enterprise level and mission critical risks have been identified such risks need to be assigned to board committees. We've known that much for a while. However, what is different and that the courts appear to be teaching, is that mission critical risks probably need a separate board committee focused on that mission critical risk. For all other potential mission critical and enterprise level risk it makes sense that each risk is not only tracked to a board committee but that it is also documented that the board gets systematic reports on that risk and has documentation of how often the board discusses such risks. It may also be important that the charter for these committees identify potential mission critical or enterprise risks instead of using boilerplate charter language.

Ultimately, enterprise risk management and board risk oversight is still about creating, protecting, and enhancing the value of an organization. It only makes sense for organizations to make sure their process is consistent with the times and updated for court rulings.

Lesson Summary

- Get an external view of your ERM and board risk oversight process.
- Consider having a board level committee specifically designated for mission critical risks.

- Have a clear board process to keep informed about mission critical risks.
- Have a clear risk escalation process around other risks that could be seen as mission critical risks by others.
- Document the regular board discussions of mission critical risks. Demonstrate that the board is not passive and actively seeks all information about the risks.
- Ensure the oversight process shows the board is requesting information on mission critical risks, is not being passive, and may even be challenging management on mission critical risks.
- Don’t rely on the ERM process alone to identify and provide adequate oversight of mission critical risks.
- Update board charters to acknowledge responsibility for mission critical risks.
- Have a conversation that addresses how the organization defines and identifies mission critical risks.
- Ensure your ERM process is strong and current.