AGN. NO.

MOTION BY SUPERVISOR HOLLY J. MITCHELL July 9, 2024

Continuing to Protect and Enhance Los Angeles County Risk Management Efforts

The County of Los Angeles (County), which has a budget exceeding that of at least 35 states and serves a population larger than 40 states, is arguably at a high exposure for risks. Pressures from providing a wide array of services to 10 million constituents; complying with federal, state, and county requirements; and having more than 100,000 employees, are complex responsibilities to manage. Additionally, the County is subject to economic, social, and political pressures that impact any organization, public or private. These factors expose the County to operational risks (*resulting in approximately $800 million in workers and non-workers compensation payouts in 2022-23*), technology and data risks, regulatory risks due to non-compliance with privacy laws, and reputational risks, which all together may undermine its ability to provide services and preserve the public trust.

Last year, the Board of Supervisors (Board) unanimously approved a motion to assess the County's risk management apparatus and risk readiness[1]. The goal of this motion was to ultimately reduce the likelihood of liability payments, which made up 2% of the County's operating budget. Now that the Department's risk management efforts have been assessed including corrective actions plans, the County needs to consolidate

[1] https://file.lacounty.gov/SDSInter/bos/supdocs/181253.pdf

- MORE -

MOTION

SOLIS	_____
MITCHELL	_____
HAHN	_____
BARGER	_____
HORVATH	_____

existing efforts and enhance them to better protect the County and mitigate all potential risks. The County must also establish a foundation to build on for a robust risk management apparatus. According to the Harvard Business School, "risk management is the systematic process of identifying, assessing, and mitigating threats or uncertainties that can affect your organization. It involves analyzing risks' likelihood and impact, developing strategies to minimize harm, and monitoring measures' effectiveness[2]." While tasked with using technology and data, the County has a responsibility to protect itself and reduce its exposure to risks through a comprehensive, inter-departmental, and effective risk management apparatus. This will allow the County to maintain the public's trust, minimize loss, innovate operations, positively transform organizational culture, and optimize decision-making abilities and capabilities.

Over the past few years, the County's Risk Management arm, the Chief Executive Officer's Risk Management Branch, has made a lot of progress assessing its vulnerability to risk and shoring up the risk management apparatus. One of these efforts included a motion asking for various report backs with analyses of the County's risk management status quo and areas for improvement, including the County's cybersecurity and data privacy risks[3]. The County has also explored the feasibility of creating a Department of Technology. Due to the recent increase in cybersecurity attacks and data privacy breaches, including a recent phishing attack over the Presidents' Day Holiday, the County must modernize cybersecurity and privacy incident response protocols. In addition, a formal communication process should be established between the Board, department heads, and other key stakeholders to discuss investigation developments and to confirm resolution, root cause, and lessons learned, all of which are vital to managing cybersecurity and privacy risks for the County.

I THEREFORE MOVE THAT THE BOARD OF SUPERVISORS:

1. Direct all County Departments with one or more outstanding Corrective Action Plans, that have been outstanding for more than 90 days, from liability incidents above $100,000 to provide to the Chief Executive Office – Risk Management

[2] What Is Risk Management & Why Is It Important? | HBS Online
[3] https://file.lacounty.gov/SDSInter/bos/supdocs/154475.pdf

Branch (CEO-RMB) their plan to fully implement those corrective actions within the next 60 days. Direct the Chief Executive Officer (CEO), through the CEO-RMB, to report back to the Board in writing within 90 days on a plan to ensure all outstanding corrective action plans are fully implemented.

2. Direct the CEO, in collaboration with all County departments, to report back to the Board in writing within 120 days on an action plan to embed risk management more effectively in all department's business models and across their functions. The action plan should have the following areas:
    a. Creating a Countywide risk management strategy, which accounts for the County's risk vulnerabilities and exposure in Information Technology, Artificial Intelligence, privacy/security, program delivery, operations, etc.
    b. Creating an accounting of all the organizational/countywide risks and vulnerabilities (in IT, Artificial Intelligence, privacy/security, programs, operations, etc.), with the ability to score, evaluate, and rate them and establish standards to evaluate departmental responses and readiness, so the County can measure and understand its risk exposure and key risk indicators to help inform risk management policy improvements.
    c. Creating a reporting method which identifies the top risk vulnerabilities and exposures for departments with the lowest risk management performance score per service cluster in areas including, but not limited to, loss prevention, privacy, general liability, and workers' compensation. This reporting method will identify steps taken by these departments in lowering their top risk vulnerability and exposure.
3. Direct CEO to report back to the Board in writing within 120 days on an action plan to create and implement a County Risk Management Policy, which will help centralize and better coordinate overall risk management authorities and responsibilities at the County level. This policy must include but not be limited to workers' compensation, liability claims, loss control, privacy, the Risk Management Inspector General, and all relevant and best-practice policies and functions for a robust risk management structure.

4. Direct CEO-RMB to review existing protocols, policies and practices for incident response and internal communication for security and data breaches and other risks and identify gaps or opportunities for improvement and provide a plan to the Board in 90 days to execute these improvements. Also, direct CEO-RMB to create and implement a process and protocols to provide a comprehensive analysis of the impact of breaches, also known as After-Action Report, to the Board at least 30 days after the incident. Ensure that these processes are automated and effective. If needed, CEO may use their existing delegated authority and budget to engage a contractor to assist with this analysis.

# # #

(KK)