M E M O R A N D U M

EUGENE WATER & ELECTRIC BOARD

Rely on us.

TO: Commissioners Carlson, Mital, Helgeson, Schlossberg and Brown

FROM: Sue Fahey, Assistant General Manager/CFO; Deborah Hart, Financial Services Manager; Sarah Creighton, Enterprise Risk Supervisor

DATE: June 26, 2019

SUBJECT: SD20 Annual Enterprise Risk Management (ERM) Update

OBJECTIVE: Information Only

Issue

Board Policy SD20 requires a periodic report on the status of Enterprise Risk Management (ERM) activities. This backgrounder provides that information for the last year.

Background

EWEB's risk management efforts are embedded across the utility. These efforts include the Safety program, Power Risk Management Committee (RMC), Cyber Security program and the Dam Safety program.

Board Policy SD20 outlines EWEB's commitment to an enterprise-wide approach to risk management. Enterprise risk management is designed to support the achievement of operational and strategic objectives, including safety, reliability, responsible stewardship of our customer-owners' financial and natural resources, and regulatory compliance. Managing risk is an integral part of decision-making across EWEB and is not a stand-alone activity. Risk analysis is an essential component when considering capital projects. ERM staff coordinates EWEB's ERM efforts, which includes identifying and analyzing existing risks, monitoring emerging risks, creating and implementing mitigation strategies, and reviewing those strategies to ensure that risk informed decisions are made and the risk retained is acceptable.

Discussion

At the end of 2018, an updated risk analysis was completed by ERM staff and Management to determine which risks ERM should focus on from an organization-wide perspective. Top risks were selected based on projected impact and likelihood of occurrence after mitigation strategies were applied. These risks were determined to be:

- Complying with contracts other than those for goods and services
- Legal and regulatory compliance
- Cyber security
- Enhancing a risk-aware culture

Last year's SD20 update reflected that IS Project Execution was identified as a top risk. Since that time, staff's efforts to standardize the Project Management Lifecycle have led to a more consistent approach with more predictable outputs. Effective and efficient IS Project Execution remains a top priority.

Contractual Compliance: The Contract Governance program has been operational since January 2017 and is designed to address non-standard contracts developed outside the Purchasing department. The program helps ensure stakeholders have an opportunity to provide feedback during contract development. Staff continues to use the tool that was created to track these contracts, providing increased visibility throughout the contract term. This tool also supports reporting functionality to aid in work planning. Presently, over 300 contracts have been identified and tracked.

Legal and Regulatory Compliance: ERM staff report monthly to Management on compliance activities, helping to ensure real time conversations on compliance opportunities. ERM staff also monitor legal and regulatory compliance changes. Training continues to be a strong focus. Moss Adams delivered Internal Controls training to managers, supervisors, and project managers in May 2019. Comprehensive ethics training continues to be required for all new hires, and all staff complete annual ethics refresher training.

Privacy of employee and customer personal information remains a high priority. Annual identity theft prevention training is required for staff whose jobs require access to personal information. Training occurred in fall 2018 and is scheduled again for the fall of 2019. The Privacy Committee continues to investigate and respond to potential breaches of personal information. Over the past year, one potential event was reported and investigated, and the investigation revealed no data breach occurred.

ERM staff maintains responsibility for compliance with public records archival and request laws. Over the past year, ERM staff responded to more than 30 public records requests.

Cyber Security: Employee awareness is a critical component of cyber security. Annual identity theft prevention training includes a strong focus on cyber security. Staff employs a variety of communication methods including posters, emails, articles, and online training modules to help keep cyber security in the forefront of staff's minds. Teaching users to know when something does not look right is an integral piece of ongoing cyber security strategy.

EWEB has adopted a new Cyber Security charter, which supports and emphasizes EWEB's commitment to a holistic approach to cyber security. The charter formalizes partnerships between Cyber, ERM, Continuous Improvement and Physical Security staff, recognizing that cyber security is a risk with broad implications. Plans are underway to draft a cyber breach response plan, complete a tabletop exercise, and implement employee phishing email education.

Risk-Aware Culture: Decisions are made every day at all levels of EWEB. ERM staff created and implemented simple risk-aware decision-making tools that walk users through the risk assessment process, to help ensure decisions are made by considering a variety of perspectives and potential outcomes. ERM staff supports risk-based decisions and prioritization by consulting on various projects across the utility. Examples of this partnership include EWEB's draft Natural Hazard Mitigation Plan Annex and the upcoming Risk and Resilience Assessment and Emergency Response Plans required by the recently enacted America Water Infrastructure Act.

<u>Other Functions:</u> ERM staff are responsible for claims, insurance procurement, and responses to subpoenas. The majority of liability and recovery claims EWEB experiences are within the $2 million self-insurance threshold and are resolved internally. EWEB maintains a broad portfolio of insurance policies to cover a variety of other exposures. This portfolio is evaluated at least annually to ensure the types and levels of coverage purchased continue to be adequate to mitigate risk.

Requested Board Action
This item is information only and accordingly there is no requested Board action.