# MEMORANDUM

EUGENE WATER & ELECTRIC BOARD

Rely on us.

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

FROM: Sue Fahey, Chief Financial Officer; Sarah Creighton, Enterprise Risk Management Supervisor

DATE: August 1, 2017

SUBJECT: SD20 Enterprise Risk Management (ERM) Update

OBJECTIVE: Information Only

---

**Issue**

SD20 calls for a periodic report on the status of Enterprise Risk Management (ERM) activities. The following is a status report on projects completed in the last year, in progress, and planned.

**Background**

EWEB continues to use risk management approaches and programs to address several risks, including the Safety program, Power Risk Management Committee (RMC), Dam Safety program, Reliability Council, and involvement with regional disaster preparedness groups.

Following the adoption of SD20, EWEB has been moving toward the practice of an enterprise-wide approach to embed risk-based decision making throughout the organization, as well as identify, mitigate and manage various risks. In addition to the enterprise risk work, ERM staff is also responsible for claims, insurance procurement, record retention, public record requests, and internal reviews for operational efficiencies, controls and effectiveness.

**Discussion**

The Executive Team and ERM staff analyzed the risk inventory developed in 2016 to determine which risks to focus on from an organization-wide perspective in an effort to ensure responsible stewardship of our customers' financial and natural resources as well as maintain safety and regulatory compliance. These risks were determined to be:

- Compliance with contracts other than those for goods and services,
- Regulatory and legal compliance,
- Information and records lifecycle management, and
- Enhancing a risk-aware culture.

Governance Structure continues to be a risk given ongoing reorganizations, so ERM staff are working with management to ensure risks and compliance items for their team are proactively managed in the face of changing staff assignments. ERM has also partnered with Information Services staff to provide employee education on the existence of, and ways to mitigate, various cyber risks, such as phishing scams.

*Contractual Compliance:* The Contract Governance program referenced in last year's SD20 update has been operational since January 2017. This program addresses non-standard contracts developed outside of the Purchasing department with the intent of ensuring that all stakeholders have the opportunity to provide feedback during contract development. To date, eighteen new contracts have been reviewed by stakeholders via this process. Additionally, a tool was created to track these contracts and provide increased visibility throughout the contract term. Presently 162 contracts are tracked. The contract repository, reporting functionality and process continue to be refined in order to provide meaningful data to management.

*Legal and Regulatory Compliance:* ERM policy work has focused on enhancing compliance with laws and regulations in addition to improving internal controls. The following policies were revised by ERM since last year's SD20 update:

| | |
|---|---|
| Records Retention Policy | Revised September 2016 |
| Inspection of Public Records Policy | Revised September 2016 |
| Contract Management Policy | NEW November 2016 |
| Personal Mobile Device Policy | NEW November 2016 |
| Delegated Authority Policy | Revised November 2016 |
| Identity Theft Prevention Policy | Revised March 2017 |
| Shredding and Recycling Policy | Revised March 2017 |
| Ethics Policy | Revised June 2017 |

Training is an integral part of the compliance program. Last year, internal control training was offered to managers and supervisors. This organization-wide focus on controls and standardization was recently cited by the external auditors as one of the reasons audit fees were reduced. Earlier this year, all staff completed training on Oregon Ethics laws. Identity Theft Prevention training is scheduled for August 2017 for staff whose jobs require access to customers' personal information. The Privacy Committee, chaired by ERM staff, works to ensure Personally Identifiable Information (PII) is protected by investigating and responding to potential breaches of PII. Over the past year, one potential breach was reported to the Privacy Committee. The incident was fully investigated, and approximately 200 potentially affected parties were notified and offered credit monitoring services.

The process for receiving timely notification of regulation changes has been noted as an improvement area, particularly given organizational changes. ERM has begun actively monitoring certain regulations to ensure appropriate stakeholders are aware of new requirements. These regulations include the Telephone Consumer Protection Act of 1991, the Office of Foreign Assets Control, and Specially Designated Nationals and Blocked Persons List. ERM is partnering with management to evaluate what additional regulation monitoring might bring additional value. Staff also works to ensure ongoing and planned activities are in compliance with applicable laws and regulations by maintaining open lines of communication across the utility and participating in the review of new contracts.

*Information and Records Management:* The Information Management risk represents legacy practices that have the potential to lead to inconsistent or ineffective records management practices. ERM staff has created educational materials and is offering training opportunities to embed best practices for the management of records. Records Retention training was provided to all work groups. Staff completed an in-depth review and reorganization of archived records to improve efficiency and reduce storage expenses. Processes for intake and management of archived records continue to be enhanced, including making improvements to the archive retrieval process. Staff also responds to public records requests; over the past year staff has responded to 30 different requests for records.

*Risk-Aware Culture:* ERM staff continues to enhance a risk-aware internal culture to enable all employees to make effective, risk-informed decisions. A common language and risk assessment framework was introduced to increase consistency in the way risks are addressed. ERM staff meets at least quarterly with management to develop a common understanding of risks and mitigation strategies. Where gaps are identified between present and desired mitigation strategies, ERM staff partner with departments to assist in closing that gap. As an example, ERM has created and disseminated enterprise-wide communications and trainings on ethics and compliance to complement mitigation efforts of the Organizational Culture risk. Additionally, staff provide consulting services to internal decision-makers to guide them toward appropriately considering and addressing risks when making decisions.

*Other functions*: In addition to the work summarized above, ERM staff is also responsible for claims, insurance procurement, and internal reviews for operational efficiencies and effectiveness.

The majority of liability and recovery claims EWEB experiences are within the self-insurance threshold and are resolved internally. EWEB maintains a broad portfolio of insurance policies to cover a variety of other exposures including Cyber Insurance beginning in 2016.

Internal reviews are currently focusing on assessing internal controls, operational efficiencies and effectiveness for a variety of processes. Staff performed a limited review of purchase card usage and determined that practices aligned with procedures. Staff also assessed internal controls and efficiencies for a portion of the warehouse inventory exchange process, leading to a successful pilot program and improved organizational efficiency. Efficiency improvements to the purchase requisition and purchase order processes were reviewed to ensure compliance with internal controls and adequate segregation of duties. EWEB presently offers a variety of loans to residential and business customers to make energy efficiency and water conservation upgrades, and these programs are presently being reviewed to ensure compliance with internal controls and adequate segregation of duties.

**Recommendation**
This is for information only.

**Requested Board Action**
No action is requested at this time.