

Exhibit to Agenda Item #2

Accept the monitoring report for Strategic Direction SD-17, Enterprise Risk Management.

Board Policy Committee and Special SMUD Board of Directors Meeting
Wednesday, November 17, 2021, scheduled to begin at 5:30 p.m.
Virtual Meeting (online)

SD-17 Enterprise Risk Management (ERM)

Effectively balancing and managing risk to further SMUD's policies and business goals is a core value of SMUD.

Therefore:

SMUD will implement and maintain an integrated enterprise risk management process that identifies, assesses, prudently manages and mitigates a variety of risks facing SMUD, including financial, supply, operational, physical and cyber security, climate change, legal, legislative and regulatory, and reputational risk.

SMUD is compliant with SD-17, Enterprise Risk Management Policy

ERM Approach and Methodology

Approach

- Governance (Board Strategic Direction)
- Oversight & Accountability (EROOC)
- Consistent Definitions and Language (ERM Framework)
- Integration of ERM with Key Business Processes

Methodology

- Enterprise Risk Analysis (focused on top risks)
- Periodic EROOC Meetings
- Annual and Periodic Review of Enterprise Risk Portfolio

2021 Enterprise-wide Risk Activities and Outcomes

Increase capabilities in Enterprise Risk Management

- Third-party evaluation of ERM Program

Build resiliency for future impacts and capabilities for future opportunities

- Leveraged risk in planning process
- Hired an enterprise prioritization position

Increase capabilities in wildfire mitigation activities

- Conducted an enterprise-wide wildfire table-top exercise

Demonstrate SMUD's leadership in addressing carbon reduction

- 2030 Zero Carbon Plan approved by Board

Bolster SMUD's ability to respond to cyber incidents

- Enterprise Cybersecurity Operations Program
- Table-top exercise

Increase operational efficiencies through the alignment of audit and risk functions

- Reviewed and integrated 6 audit reports into risk assessments

New risks since 2020 Board Monitoring Report

- Backup control center
- 2030 Zero Carbon Plan
- Diversity, Equity, Inclusion, and Belonging
- Facilities Workplace Strategy
- Rancho Seco Park Facilities

Third-party review

Early 2021 Grant Thornton conducted an analysis of SMUD's ERM program to identify strengths and areas of opportunity and to develop ERM as a driver of a risk aware culture aligned to strategic objectives.

- Executive and Director interviews
- Qualitative assessment of program maturity
- Developed prioritized recommendations to address gaps

Increasing SMUD's ERM Capabilities

Foundational



Increase Risk Intelligence

Make risk conversations more intuitive for the business and shift assessments from risk centric to performance oriented



Clearly Define Roles and Responsibilities for all persons within the risk management process



Enhance Communication and elevate risks and education of ERM Program to increase risk informed decision making

Strategic



Risk is linked to strategy

Link risk to strategy, leverage ERM to support the creation, realization and preservation of value



Governance oversight/management of risk Make ERM more than just an isolated view of risk in the business and something that resonates with those responsible for oversight



Foster Risk-Aware Culture Making risk core to decision making and integrate risk into everyday conversations

Enhancement



Deepen understanding of risk tolerance have meaningful conversations around risks and what is acceptable or not



Technology Explore technologies to better manage risk portfolio and share information



Improve reporting Explore and develop reports that provide insight to users

SMUD's risk are consistent with benchmarking NCSU/Protiviti Research Top 10 risks

1. Pandemic related policies and regulation impact business performance
2. Economic conditions constrain growth opportunities
3. Pandemic-related market conditions reduce customer demand
4. Adoption of digital technologies may require new skills or significant efforts to upskill/reskill existing employees
5. Privacy/identity management and information security protection
6. Cyber threats
7. Impact of regulatory change and scrutiny on operational resilience, products and services
8. Succession challenges, ability to attract and retain top talent
9. Resistance to change operations and business model
10. Ability to compete with “born digital” and other competitors

Looking Forward

ERM Program enhancements

- Develop a plan for implementing third party recommendations
- Form the Risk Champion Network, a forum of Director level risk champions

Financial Risks

- Leverage risk tools to help build resiliency and future capacity in financial planning and prioritization; expanding upon approaches used for the 2021 budget plan

Operational Risks

- Attract and retain skilled and innovative workforce
- Enhance data quantity and quality for business and customer decisions
- Continue cyber security and privacy awareness and compliance activities
- Provide programs and services which reflect the customer's changing expectations

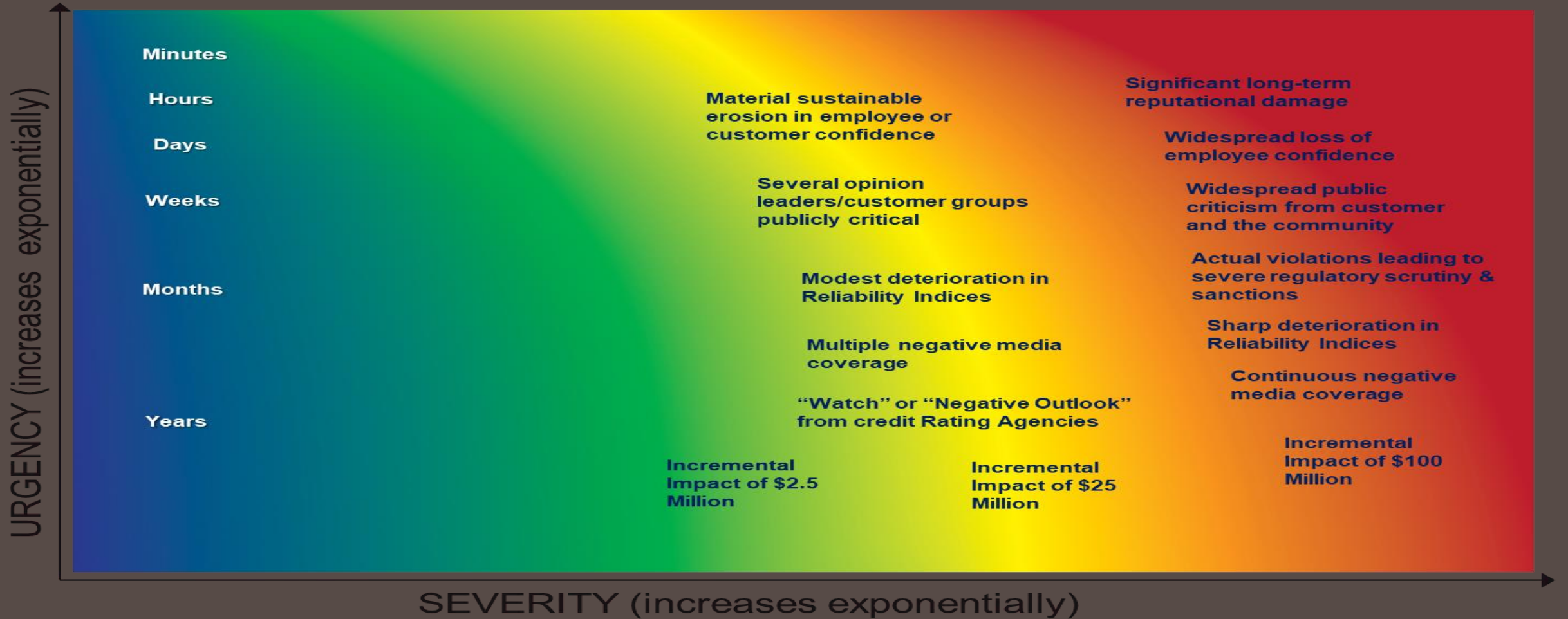
Strategic Risks

- Support 2030 Zero Carbon Plan and SMUDs Diversity, Equity and Inclusion goals

External Risks

- Positively influence state and federal legislative and regulatory issues

SMUD's Risk and Opportunity Heat Map



Year-On-Year Risk Summary

Level of Residual Risk Exposure			Nov-19	Dec-20	Nov-21
	Red	Extremely High	0	0	0
	Orange	High	4	4	4
	Yellow	Medium	33	36	40
	Green	Low	40	38	38
	Blue	Extremely Low	0	0	0
Total			77	78	83

SD-17 ERM Portfolio: Residual Business Critical Risk Exposure: November 17, 2021

Financial Risks	Operational Risks	Strategic Risks
Budget Planning and Rate Setting <u>Financing</u> Accounting/Financial Report Capital Availability/Cashflow Liquidity <u>Load Variation</u> Retail Load Customer owned generation <u>Price Volatility</u> Commodity Hydro Generation Interest Rate Project Execution Wholesale Credit Default	OP: People Employee Safety Ethics/Integrity Illegal Acts/Fraud <u>Strategic Workforce Agility</u> <u>Diversity, Equity and Inclusion</u> OP: Systems and IT Applications Support Cyber Security Privacy Information Management Data Governance Enterprise-Wide Documentation Grid Operational Systems & Support Technology Systems Infrastructure OP: Process Balancing Authority Operations Bulk Power Op & Maintenance Gas & Gas Pipeline Assets Power Supply Assets Transmission Assets Enterprise Continuity Management <u>Communications</u> Internal Communications/Alignment Media & Community Relations Customer Serv Operations: Business Disruption <u>General Facilities Op & Maintenance</u> Customer Service Center Energy Management Center Existing Corporation Yard Headquarter Building Physical Asset Security Backup Control Center Facilities Workplace Strategy Rancho Seco Park Facilities	Business Model <u>2030 Zero Carbon Plan</u> <u>Technology/Competition Driven</u> Demand Response Distributed Generation Distributed Storage Electrification of Transport Sector Energy Efficiency Innovation Changing Customer Expectations Competitive Workforce Total Rewards <u>Corporate Governance</u> Board Driven GM Driven Enterprise Grant Integration, Execution and Alignment Sustainable Energy Carbon Emission/AB32 Load Serving Capability Renewable Portfolio Standard CEC: Integrated Resource Planning External Risks Economy - Business Agility Legislative & Regulatory <u>Federal</u> Dodd-Frank Implementation Limits on Muni Bond Tax Exemption <u>Local Gov't</u> <u>State</u> Bay Delta Flow Issues Post 2020 Carbon Markets <u>Natural / Other Hazards</u> Pandemic Wildfire Climate Change
Legend: by Risk Heat Zone Extremely High Residual Risk High Residual Risk Medium Residual Risk Low Residual Risk Extremely Low Residual Risk Recent Changes denoted in Purple		