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)
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 (EROC)
• Consistent Definitions and Language (ERM Framework)
• Integration of ERM with Key Business Processes

Methodology
• Enterprise Risk Analysis (focused on top risks)
• Periodic EROC 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

November 17, 2021  
Board Policy Committee and Special SMUD Board of Directors Meeting
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

- **Minutes**: Material sustainable erosion in employee or customer confidence
- **Hours**: Several opinion leaders/customer groups publicly critical
- **Days**: Modest deterioration in Reliability Indices
- **Weeks**: Multiple negative media coverage
- **Months**: “Watch” or “Negative Outlook” from credit Rating Agencies
- **Years**: Incremental Impact of $2.5 Million

**URGENCY (increases exponentially)**

**SEVERITY (increases exponentially)**

- **Significant long-term reputational damage**: Widespread loss of employee confidence
- **Widespread public criticism from customer and the community**: Actual violations leading to severe regulatory scrutiny & sanctions
- **Sharp deterioration in Reliability Indices**: Continuous negative media coverage
- **Incremental Impact of $100 Million**
Year-On-Year Risk Summary

<table>
<thead>
<tr>
<th>Level of Residual Risk Exposure</th>
<th>Nov-19</th>
<th>Dec-20</th>
<th>Nov-21</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extremely High</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Orange</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Yellow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>33</td>
<td>36</td>
<td>40</td>
</tr>
<tr>
<td>Green</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>40</td>
<td>38</td>
<td>38</td>
</tr>
<tr>
<td>Blue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extremely Low</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>77</strong></td>
<td><strong>78</strong></td>
<td><strong>83</strong></td>
</tr>
</tbody>
</table>
### SD-17 ERM Portfolio: Residual Business Critical Risk Exposure: November 17, 2021

<table>
<thead>
<tr>
<th>Financial Risks</th>
<th>Operational Risks</th>
<th>Strategic Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budget Planning and Rate Setting</td>
<td>OP: People</td>
<td>Grid Infrastructure: Reliability</td>
</tr>
<tr>
<td>Capital Availability/Cashflow</td>
<td>Illegal Acts/Fraud</td>
<td>Poles</td>
</tr>
<tr>
<td>Liquidity</td>
<td>Strategic Workforce Agility</td>
<td>Secondary Network</td>
</tr>
<tr>
<td>Load Variation</td>
<td>Diversity, Equity and Inclusion</td>
<td>Underground Cables</td>
</tr>
<tr>
<td>Retail Load</td>
<td>OP: Systems and IT</td>
<td>T&amp;D Substation Assets</td>
</tr>
<tr>
<td>Customer owned generation</td>
<td>Applications Support</td>
<td>Telecommunications Assets</td>
</tr>
<tr>
<td>Price Volatility</td>
<td>Cyber Security</td>
<td>New Services &amp; Local Agency Projects</td>
</tr>
<tr>
<td>Commodity</td>
<td>Privacy</td>
<td>Labor: Business Disruption</td>
</tr>
<tr>
<td>Hydro Generation</td>
<td>Information Management</td>
<td>Legal Risk</td>
</tr>
<tr>
<td>Interest Rate</td>
<td>Data Governance</td>
<td>Operational Excellence</td>
</tr>
<tr>
<td>Project Execution</td>
<td>Enterprise-Wide Documentation</td>
<td>Payroll Disruption</td>
</tr>
<tr>
<td>Wholesale Credit Default</td>
<td>Grid Operational Systems &amp; Support</td>
<td>Pricing &amp; Rate Design Implementation</td>
</tr>
<tr>
<td>Wholesale Credit Default</td>
<td>Technology Systems Infrastructure</td>
<td>EAPR Implementation Process</td>
</tr>
<tr>
<td>OP: Process</td>
<td>OP: Systems and IT</td>
<td>Public Safety</td>
</tr>
<tr>
<td>Balancing Authority Operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulk Power Op &amp; Maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas &amp; Gas Pipeline Assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Supply Assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission Assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Communications/Alignment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media &amp; Community Relations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Serv Operations: Business Disruption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Facilities Op &amp; Maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Service Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energy Management Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing Corporation Yard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Headquarter Building</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Asset Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Control Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilities Workplace Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rancho Seco Park Facilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Climate Change</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Legend: by Risk Heat Zone
- Extremely High Residual Risk: Energy Management Center
- High Residual Risk: Existing Corporation Yard
- Medium Residual Risk: Headquarter Building
- Low Residual Risk: Physical Asset Security
- Extremely Low Residual Risk: Backup Control Center
- Recent Changes denoted in Purple: Facilities Workplace Strategy, Rancho Seco Park Facilities

---

November 17, 2021
Board Policy Committee and Special SMUD Board of Directors Meeting

SMUD®