

**Date:** March 20, 2024  
**To:** Board of Retirement  
**From:** Doris L. Rentschler, Executive Director  
**Subject:** Enterprise-wide Risk Assessment

**Recommended Action:**

None.

**Fiscal and Financial Impacts:**

No direct financial impact from this report. Any initiatives developed from the risk assessment will be included in future budgets for Board approval.

**Strategic Plan Importance:**

The risk assessment directly relates to the Board's goal to strengthen risk oversight.

**Background and Discussion:**

Larry Jensen with Audit and Risk Management Services recently completed the entity-wide risk assessment. The risk assessment is the first step in the process of identifying, monitoring and managing current and emerging risks that will regularly be reported to the Board. It is also the foundation of any future internal audit plan that may be undertaken.

The Risk Assessment Heat Map graphically illustrates the most prominent risks for monitoring by the Board. The size of the dot represents the velocity with which the issue could impact MCERA – not the magnitude of the risk. Items with greater impact are closer to the top of the chart and those with higher probability of occurring to the right side of the chart.

The Risk Narrative accompanying the Heat Map lists the risk and key business outcomes for Board discussion to identify potential mitigation efforts or acknowledgment of the level of risk the Board is willing to accept for a particular item.

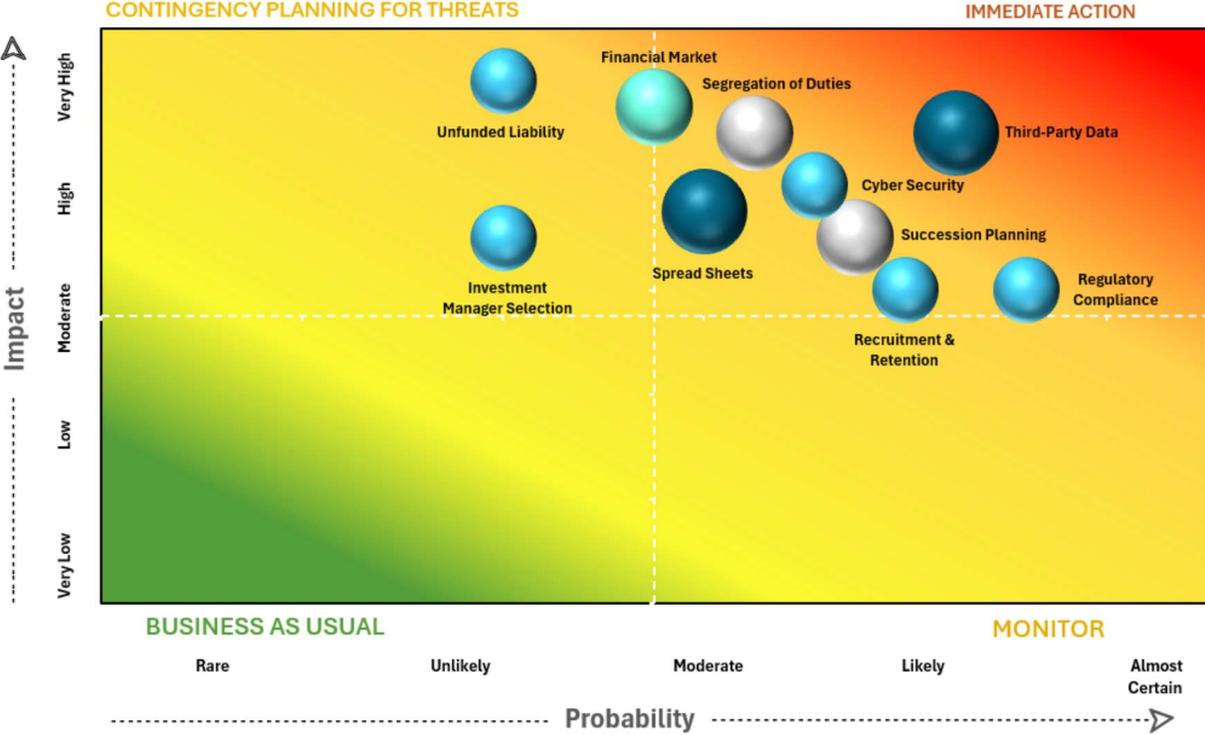
**Attachment(s):**

1. Risk Assessment Heat Map
2. Risk Narrative Report
3. Presentation

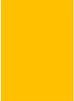
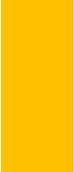
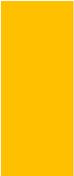
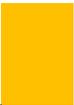
# MENDOCINO COUNTY EMPLOYEES RETIREMENT ASSOCIATION

## Risk Assessment Heat Map

March 20, 2024



Mendocino County Employees Retirement Association  
Strategic and Operational Risk Report  
March 20, 2024

| No | Risk Statement  | Rating  | Key Business Outcomes   | Action Status   |
|----|---|---|---|---|
| 1  | <b>Third Party Data Breach</b> is the risk of having sensitive or confidential data stolen from a third-party vendor or when vendor systems are used access and steal information stored on MCERA or business partner systems.  |    | MCERA business objective is to ensure member data is secure. MCERA uses trusted partners that have access or store confidential member data. Cyber security is constantly evolving and MCERA risk mitigation strategies will evaluate implementation of a vendor due diligence policy and vendor contract provisions to ensure ever evolving cyber security risks are addressed to protect member confidential data.  | TBD   |
| 2  | <b>Spread Sheet</b> The risk if errors caused by undetected mistakes, errors and omissions in vital spreadsheets threat MCERA depends on for things like service credit purchases, investment valuations, fee tracking, and financial reporting.  |    | MCERA uses spreadsheets to perform critical business functions. However, numerous risks are associated with the use of spreadsheets, including a tendency for manual data entry errors and inaccurate calculations. MCERA will evaluate the cost benefit of upgrading the pension system to perform service credit purchases in conformance with the CERL and implement internal controls to protect access and prevent unintentional errors. Spreadsheets used for critical processes should be audited regularly to ensure accuracy and validity.                             |    |
| 3  | <b>Succession Planning</b> is the risk of failure to create and implement a succession plan for key positions and employees.  |    | MCERA operates efficiently with a limited number key staff. Departure of MCERA staff in key positions can lead to inefficiencies, loss of knowledge and experience, impacts to culture, and unnecessary urgency to fill gaps. MCERA is in the process of developing a succession planning policy for developing succession plans for key staff and trustee positions.   |    |
| 4  | <b>Unfunded Liability</b> is the risk that unfunded pension obligations can strain the fund's financial health.   |    | MCERA continuously monitors and the financial health of the fund to meet future pension obligations. MCERA is evaluating investment strategies, actuarial assumptions, asset allocations, and financial impact on members and plan sponsors. MCERA will continue to evaluate strategies to ensure the financial position of the fund to provide the members a secure retirement.  |    |
| 5  | <b>Cyber Security</b> is the risk of an organization getting breached by cyber attacks or insider access, malware, phishing, ransomware, inappropriate sharing of confidential information, lack of encrypted data.   |    | MCERA depends on information technology to carry out key business functions today, creating exposure to cyber criminals, natural disasters and other cybersecurity threats that can knock critical systems offline or disrupt operations. MCERA primarily relies upon the county to manage information security however, cyber risk management is an on-going, iterative process rather than a one-time event. MCERA is assessing potential threats and vulnerabilities, along with technical solutions to protect confidential data and financial information.                 | TBD   |
| 6  | <b>Segregation of Duties</b> is a risk due to improper segregation of duties and internal controls not in place to ensure the integrity of information and to prevent/ detect fraud.  |  | Like other organizations with only a few staff, it can be difficult to ensure proper segregation of duties to prevent errors and misappropriation by ensuring that a least two individuals are responsible for separate parts of any task. MCERA is evaluating key financial accounting and reporting processes to ensure duties are assigned appropriately and that preventative and detective controls are in place to maintain the integrity of financial accounting and reporting.  |  |
| 7  | <b>Regulatory Compliance</b> is the risk of failure to act in accordance with rules, regulations, ethical standards, contractual obligations, policies, and ethical standards, resulting in a negative effect on the organization's reputation, and financial consequences to the organization or its members.. |  | MCERA strives to maintain an ethical culture that includes administering the system in compliance with the CERL, and in conformance with applicable compliance requirements. In 2022, MCERA conducted a review of historical benefit payments to conform with changes to the regulations and ensure business practices align with requirements. MCERA continues to monitor changes to the regulatory environment and implement business controls or processes to comply with applicable requirements.   |  |
| 8  | <b>Financial Market</b> risk includes general movements in capital market prices that affect the value of MCERA's financial assets which in turn affect stakeholders' confidence in the organization and its ability to achieve its expected rate of return to fund pension obligations.                        |  | MCERA strives to provide sustainable pensions though prudent investments in capital markets. As with all financial organizations, there is inherent risk investing funds in capital markets. MCEA relies upon financial advisors and actuaries who monitor market conditions and perform studies to assist the board making financial decisions and develop investment policy. Given the volatility in the financial markets, continuous monitoring and prudent investment strategies are critical to achieving the fund's expected rate of return to fund pension obligations. |  |
| 9  | <b>Investment Manager Selection</b> is the risk of investment manager poor performance, excessive cost, or misconduct harming the fund's returns and reputation.  |  | MCERA primarily utilizes external fund managers to invest in capital markets based on the guidelines established in the Investment Policy. Investment manager monitoring is performed by the trustees who rely upon reports and advices from an investment consultant and internal staff. Oversight of investment managers requires on-going training of the selection and monitoring processes and implementation of on-going due diligence activities.  |  |
| 10 | <b>Recruitment &amp; Retention</b> is the risk of failure to attract and retain talented staff.   |  | MCERA strives to maintain a culture and work environment to attract and retain talented staff. This is essential since MCERA operates with a limited number of positions. Recruitment and retention problems can also negatively impact the remaining workforce. MCERA is coordinating with the county to effectively recruit staff.  |  |

High   
Significant   
Moderate 

Strategies agreed, implementation largely complete   
Strategies agreed, implementation is in progress   
Strategies agreed, resources required, limited implementation progress 





---

## MCERA Strategic Plan FY 2023-2027

---

### Goal 2:

Strengthen risk oversight

---

### Objective A:

Enhance the approach to identifying, monitoring and managing current and emerging risks.

# Risk Management

Risk is the effect of uncertainty on objectives.

Risk Management is a coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives.

Enterprise Risk management is a methodology that provides sustainable framework to proactively identify and manage strategic, operating, regulatory, and financial risks, both existing and emerging, across the entire organization.



# MCERA Risk Assessment Framework



# MCERA Risk Universe

## Strategic

### Governance:

- Fiduciary Duty
- Risk Management
- Control Environment
- Political
- Reputational
- Public Media Relations
- Community Relations

### Strategy and Policy:

- Strategic Plan
- Strategic Alignment

### Pension Funding:

- Funding Ratio
- Underfunding
- Pension Funding
- Unfunded Liability
- Contribution Rates

### Actuarial:

- Assumptions
- Longevity
- Asset Allocation
- Stress Testing
- Actuarial Experience
- Demographic Shifts

## Operational

### Administration:

- Lease Administration
- Catastrophic Loss
- Emergency Protocols
- Phone Calls Admin.
- Complaint Escalation & Resolution
- Records Retention

### Benefit Payments:

- Benefit Administration
- Preliminary Benefit Processing & Certification
- Final Benefit Processing & Certification
- Retiree Check Deductions
- Contribution Adjustments
- Monthly Pension process
- Salary Continuance & Salary Adjustment
- Annual Mbr Statements

### Employer Services:

- Employer Reporting
- Return to Service
- Records Retention
- Insurance Premium Withholding

### Member Services:

- Beneficiary
- Bank Account
- Service Credit Adjmts.
- Member Termination
- Member Enrollment
- Member File Admin
- Imaging Mbr Records
- Unclaimed Benefits
- Overpayment Collections
- Pension Recoupment
- 1:1 Benefits Meetings with Member/Retirees
- Benefits Estimates
- Record Review Process
- Post Retirement Employment
- Reciprocity
- Records Retention
- Member Refunds
- Required Minimum Dist.
- Service Purchases
- Service Retirement Apps
- Split Benefits Applications
- Member Education
- Vested Deferred Benefits Applications
- Disability Applications

### Human Resources:

- Payroll Administration
- Voluntary Deductions
- Leave Administration
- Performance Evals
- Termination Process
- Disciplinary Actions
- Privacy Issues
- Personnel Files
- Retention
- Recruitment
- Hiring Process
- Background Checks
- Compensation
- Employee Turnover
- Succession Planning
- Staff Bench Strength
- Training

### Information Technology:

- Information Security
- Cybersecurity
- System Access
- Building Systems
- Business Continuity
- Change Control
- Privilege Access
- Information Integrity
- Personal Computers
- Help Desk Procedures
- Upgrades/Versions
- Information Privacy
- Records Retention
- Technology Risk
- Technical Support
- Spreadsheet Risk
- System Failure
- System Back-up
- Third-Party Data Breach
- MCERA Website

### Death Benefits:

- Death/Survivor Benefits
- Death Notification

## Financial

### Financial Accounting:

- Journal Entries
- GL Reconciliations
- Investment Manager Reconciliations
- PensionGold JE to FS
- Monthly Accrual Process
- Segregation of Duties
- External Audit

### Financial Reporting:

- Popular Annual Financial Report (PAFR)
- Monthly Financial Statements
- GASB compliance

### Budget:

- Planning and Budget
- Budget Monitoring

### Benefit Payments:

- Retiree Payroll
- Federal Taxes

### Employer Reporting:

- Member Data
- Contributions
- Payments & Receipts
- Contribution Reconciliation
- Unclaimed Contributions

### Accounts Payable:

- Vendor Payments
- Purchasing Card
- Travel Expenditures
- Trustee Reimbursements
- Unclaimed Funds

### Procurement:

- Vendors
- Contract Management
- Third-Party Due Diligence

### Financial Markets:

- Market Volatility
- Inflation
- Financial Market
- Economic Recession
- Interest Rates
- Liquidity
- Credit
- Cash Management
- Climate Change
- Envion, Social, Gov (ESG)

### Investment Portfolio:

- Custodial Bank
- Counterparty
- Payments to Managers and Partners
- Portfolio Reconciliations
- Investment Trade Request
- Form ADV/Other Regulatory Disclosure Monitoring
- Default
- Currency
- Investment Manager Selection
- Investment Managers
- Limited Partnerships
- Alternative Investments
- Rebalancing

### Cash Management:

- Cash Receipts
- Tax Reporting - 1099s
- Capital Call Funding
- Cash Management
- Cash Flow Projections
- Bank Account Admin.
- Bank Reconciliations
- Stop Pymts/Rpl Checks
- BofA Stmt Recons
- Wire Transfers

## Legal / Compliance

### Laws, Rules, and Regulations:

- Public Info Requests
- Public Meetings
- Compliance
- State & Fed Tax
- Admin. Hearings
- Contract Management
- Court Orders (QDRO)
- Litigation
- Pension Reform
- Record Retention
- Regulatory Enviromnt
- Regulatory Changes
- Legislative Bills
- OFAC Compliance

### Internal Policy:

- E-Discovery
- Privacy and Confidentiality
- Records Mgmt.

### Ethics:

- Conflicts of Interest
- Stds. of Conduct
- Ethical Behavior

# MCERA Risk Assessment Tools

| IDENTIFY THE RISK       |   |  | ANALYZE THE RISK |             |              |                    |              |                | EVALUATE THE RISK |                      |   |                       | TREAT THE RISK       |          |                        |  |
|-------------------------|---|--|------------------|-------------|--------------|--------------------|--------------|----------------|-------------------|----------------------|---|-----------------------|----------------------|----------|------------------------|--|
| Risk                    | Risk Description  | Risk Event / Context   | Impact           |             |              |                    | Impact Score | Likelihood     | Combined Score    | Inherent Risk Rating | Existing Internal Controls  | Control Effectiveness | Residual Risk Rating | Velocity | Risk Treatment Options | Risk Treatment Plan  |
|                         |   |  | Financial        | Operational | Reputational | Regulatory / Legal |              |                |                   |                      |   |                       |                      |          |                        |  |
| Third-Party Data Breach | The risk of having sensitive or confidential data stolen from a third-party vendor or when their systems are used access and steal information stored on MCERA or county systems. | Third party vendors maintain member data. Contact provisions should be updated for data storage, encryption, breach notifications, disclosure liability. | 3                | 3           | 4            | 5                  | Very High    | Almost Certain | 25                | Very High            | SOC-1/2 reviews, vendors systems segregated from County systems   | Minor                 | High                 | Rapid    | Reduce                 | <ul style="list-style-type: none"> <li>Update contracts to include breach notification requirements, notification responsibilities, liability for breach, data encryption, storage requirements etc.</li> <li>Consider vendor due diligence reviews, disaster plan requirements</li> <li>Consider independent pen testing and vulnerability scans for external member facing applications</li> </ul> |
| Employer Reporting      | The risk of incomplete or inaccurate reports received from the employer.  | Difficulty in obtaining spreadsheet from Superior Court to verify reporting, recently found errors. No employer audits performed.                        | 2                | 3           | 4            | 3                  | High         | Almost Certain | 20                | High                 | CFO reconciles pay dollars and files from County and Courts, RS reconciles pay files with PG, CFO communicates with Courts to get files as needed, RA reviews member account balances and interest postings | Moderate              | Low                  | Moderate | Reduce                 | <ul style="list-style-type: none"> <li>Consider conducting employer reporting audits of member data.</li> </ul>  |

## IMPACT / SEVERITY CRITERIA – Choose the most impactful risk criteria (even if more than 1 apply)

| Impact / Severity   | Very Low<br>(1) Insignificant | Low<br>(2) Minor          | Medium<br>(3) Moderate       | High<br>(4) Major          | Very High<br>(5) Extreme |
|---------------------|-------------------------------|---------------------------|------------------------------|----------------------------|--------------------------|
| Financial (Revenue) | ≤ \$100,000                   | \$100,000 to \$10 million | \$10 million to \$25 million | \$25 million to 50 million | >\$50 million            |

## LIKELIHOOD / FREQUENCY CRITERIA – Choose the most impactful risk criteria (even if more than 1 apply)

| Criteria            | Probability | Frequency | Qualitative Description  |
|---------------------|-------------|-----------|--|
|                     |             |           |  |
| 5<br>Almost Certain | > 90%       | Daily     | The opportunity for the risk event happening is very high. The risk is faced multiple times annually, such that an event is very likely to occur if adequate controls and management actions are not proactively and consistently taken. |
| 4<br>Likely         | > 60 - 90%  | Monthly   | The opportunity for the risk event is present under most conditions. MCERA has experienced the risk event in the recent past.  |
| 3<br>Moderate       | > 30 - 59%  | Quarterly | Event is unlikely but certainly possible to occur. Such an event may have been experienced by MCERA under specific conditions.   |
| 2<br>Unlikely       | > 10 - 29%  | Annually  | Event is generally unlikely to occur but may be possible under a specific set of conditions (i.e., multiple or simultaneous control failures may need to occur).   |
| 1<br>Rare           | < 10%       | > 1 Year  | Extremely rare event that typically occurs under exceptional circumstances.  |

## CONTROLS EFFECTIVENESS CRITERIA – Choose the most impactful risk criteria (even if more than 1 apply)

| Criteria             | Qualitative Description  | Value |
|----------------------|--|-------|
| 5<br>None            | Risk mitigation activities/controls appear insignificant or there is uncertainty as to whether existing activities/controls are geared towards mitigating the identified risk. | 0%    |
| 4<br>Minor           | Risk mitigation activities/controls seem to exist and appear somewhat geared towards mitigating the identified risk.   |       |
| 3<br>Moderate        |  |       |
| 2<br>Significant     |  |       |
| 1<br>Nearly Complete |  |       |

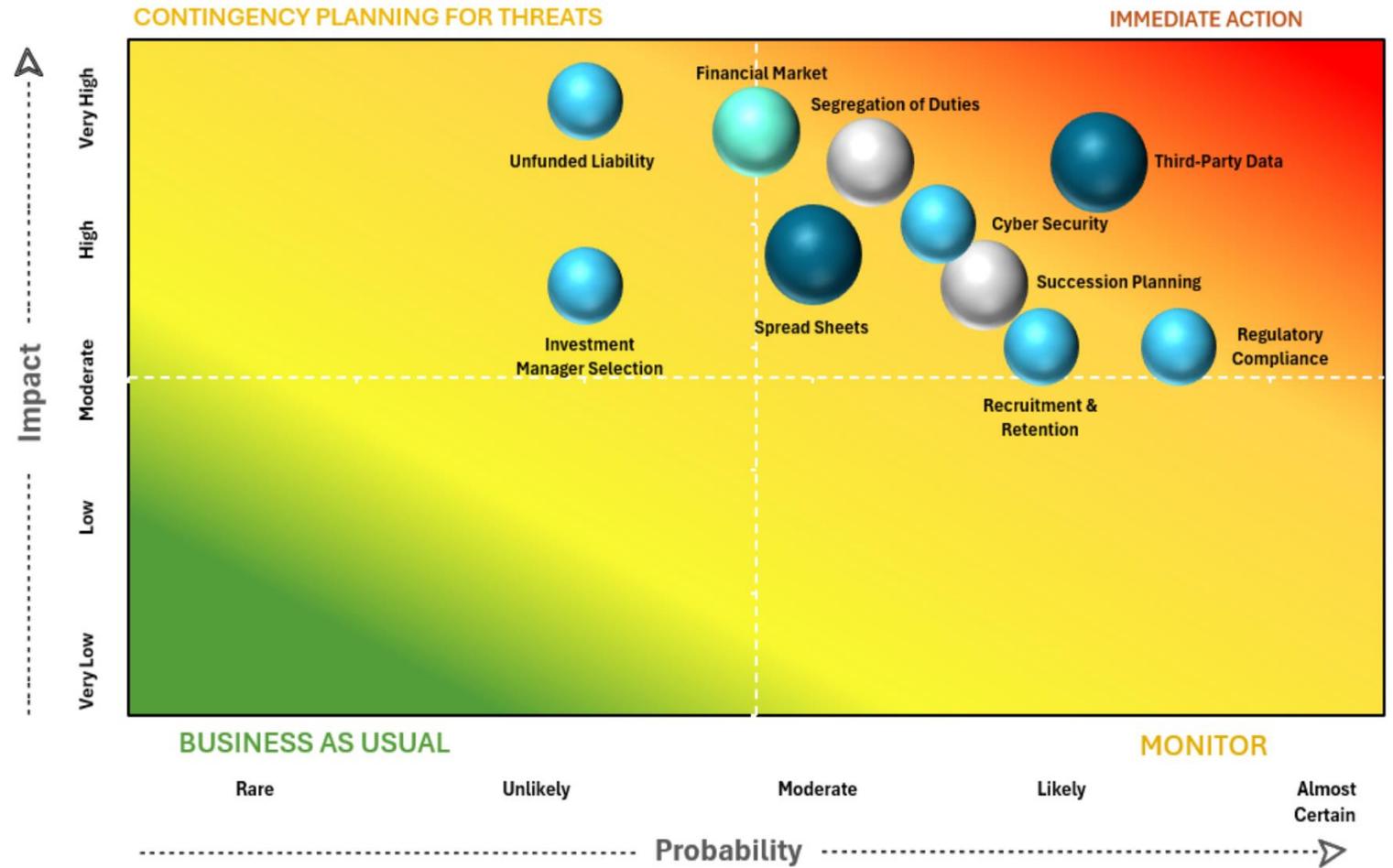
  

| Criteria         | Timeframe          | Qualitative Description  |
|------------------|--------------------|--|
| 5<br>Immediate   | < Immediate- Week  | Impact of the risk can occur without warning or up to a week. This type of risk will materialize immediately, leaving very little or no margin of time to take corrective actions. |
| 4<br>Rapid       | > Week - Month     | Impact of the risk is incurred within a month period. This type of risk will materialize quickly, leaving a small margin of time to take corrective actions.                       |
| 3<br>Moderate    | > Month - Quarter  | Impact of the risk is incurred across a month to a Quarter, leaving some degree of margin for corrective actions.  |
| 2<br>Slow        | > Quarterly – Year | Impact of the risk is incurred across one or more Quarter(s) to 1 year, leaving margin for corrective actions.   |
| 1<br>Longer-Term | > 1 years          | Impact of the risk is incurred over a period longer than 1 year.   |

## VELOCITY CRITERIA – Choose the most impactful risk criteria (even if more than 1 apply)

# MCERA

## Top 10 Risk Heat Map



# MCERA

## Top 10 Risk Report

| No | Risk Statement  | Rating | Key Business Outcomes  | Action Status |
|----|---|--------|--|---------------|
| 1  | <b>Third Party Data Breach</b> is the risk of having sensitive or confidential data stolen from a third-party vendor or when vendor systems are used access and steal information stored on MCERA or business partner systems.  |        | MCERA business objective is to ensure member data is secure. MCERA uses trusted partners that have access or store confidential member data. Cyber security is constantly evolving and MCERA risk mitigation strategies will evaluate implementation of a vendor due diligence policy and vendor contract provisions to ensure ever evolving cyber security risks are addressed to protect member confidential data.   | TBD           |
| 2  | <b>Spread Sheet</b> The risk if errors caused by undetected mistakes, errors and omissions in vital spreadsheets threat MCERA depends on for things like service credit purchases, investment valuations, fee tracking, and financial reporting.  |        | MCERA uses spreadsheets to perform critical business functions. However, numerous risks are associated with the use of spreadsheets, including a tendency for manual data entry errors and inaccurate calculations. MCERA will evaluate the cost benefit of upgrading the pension system to perform service credit purchases in conformance with the CERL and implement internal controls to protect access and prevent unintentional errors. Spreadsheets used for critical processes should be audited regularly to ensure accuracy and validity.                              |               |
| 3  | <b>Succession Planning</b> is the risk of failure to create and implement a succession plan for key positions and employees.  |        | MCERA operates efficiently with a limited number key staff. Departure of MCERA staff in key positions can lead to inefficiencies, loss of knowledge and experience, impacts to culture, and unnecessary urgency to fill gaps. MCERA is in the process of developing a succession planning policy for developing succession plans for key staff and trustee positions.  |               |
| 4  | <b>Unfunded Liability</b> is the risk that unfunded pension obligations can strain the fund's financial health.   |        | MCERA continuously monitors and the financial health of the fund to meet future pension obligations. MCERA is evaluating investment strategies, actuarial assumptions, asset allocations, and financial impact on members and plan sponsors. MCERA will continue to evaluate strategies to ensure the financial position of the fund to provide the members a secure retirement.   |               |
| 5  | <b>Cyber Security</b> is the risk of an organization getting breached by cyber attacks or insider access, malware, phishing, ransomware, inappropriate sharing of confidential information, lack of encrypted data.   |        | MCERA depends on information technology to carry out key business functions today, creating exposure to cyber criminals, natural disasters and other cybersecurity threats that can knock critical systems offline or disrupt operations. MCERA primarily relies upon the county to manage information security however, cyber risk management is an on-going , iterative process rather than a one-time event. MCERA is assessing potential threats and vulnerabilities, along with technical solutions to protect confidential data and financial information.                 | TBD           |
| 6  | <b>Segregation of Duties</b> is a risk due to improper segregation of duties and internal controls not in place to ensure the integrity of information and to prevent/ detect fraud.  |        | Like other organizations with only a few staff, it can be difficult to ensure proper segregation of duties to prevent errors and misappropriation by ensuring that a least two individuals are responsible for separate parts of any task. MCERA is evaluating key financial accounting and reporting processes to ensure duties are assigned appropriately and that preventative and detective controls are in place to maintain the integrity of financial accounting and reporting.   |               |
| 7  | <b>Regulatory Compliance</b> is the risk of failure to act in accordance with rules, regulations, ethical standards, contractual obligations, policies, and ethical standards, resulting in a negative effect on the organization's reputation, and financial consequences to the organization or its members.. |        | MCERA strives to maintain an ethical culture that includes administering the system in compliance with the CERL, and in conformance with applicable compliance requirements. In 2022, MCERA conducted a review of historical benefit payments to conform with changes to the regulations and ensure business practices align with requirements. MCERA continues to monitor changes to the regulatory environment and implement business controls or processes to comply with applicable requirements.  |               |
| 8  | <b>Financial Market</b> risk includes general movements in capital market prices that affect the value of MCERA's financial assets which in turn affect stakeholders' confidence in the organization and its ability to achieve its expected rate of return to fund pension obligations.                        |        | MCERA strives to provide sustainable pensions through prudent investments in capital markets. As with all financial organizations, there is inherent risk investing funds in capital markets. MCEA relies upon financial advisors and actuaries who monitor market conditions and perform studies to assist the board making financial decisions and develop investment policy. Given the volatility in the financial markets, continuous monitoring and prudent investment strategies are critical to achieving the fund's expected rate of return to fund pension obligations. |               |
| 9  | <b>Investment Manager Selection</b> is the risk of investment manager poor performance, excessive cost, or misconduct harming the fund's returns and reputation.  |        | MCERA primarily utilizes external fund managers to invest in capital markets based on the guidelines established in the Investment Policy. Investment manager monitoring is performed by the trustees who rely upon reports and advices from an investment consultant and internal staff. Oversight of investment managers requires on-going training of the selection and monitoring processes and implementation of on-going due diligence activities.   |               |
| 10 | <b>Recruitment &amp; Retention</b> is the risk of failure to attract and retain talented staff.   |        | MCERA strives to maintain a culture and work environment to attract and retain talented staff. This is essential since MCERA operates with a limited number of positions. Recruitment and retention problems can also negatively impact the remaining workforce. MCERA is coordinating with the county to effectively recruit staff.   |               |

High

Significant

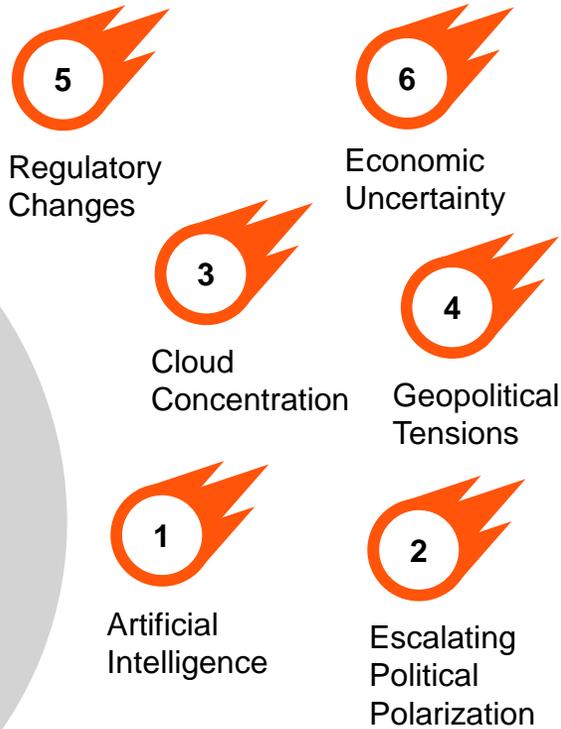
Moderate

Strategies agreed, implementation largely complete

Strategies agreed, implementation is in progress

Strategies agreed, resources required, limited implementation progress

# Emerging Risk Report



**Mendocino  
County  
Employees  
Retirement  
Association**

Ranked Time to Impact

| Score Rank | Risk Name                         |
|------------|-----------------------------------|
| 1          | Artificial Intelligence           |
| 2          | Escalating Political Polarization |
| 3          | Cloud Concentration               |
| 4          | Geopolitical Tensions             |
| 5          | Regulatory Changes                |
| 6          | Economic Uncertainty              |

Audit & Risk Management  
Services, LLC

Larry Jensen  
Larry.Jensen.ARMS@gmail.com

March 20, 2024

Questions ?