CALSTRS

Enterprise Risk reporting refresh

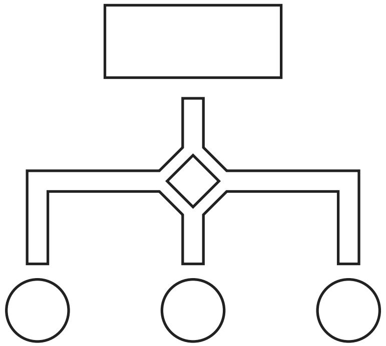
Audits and Risk Management Committee presentation

Enterprise Risk Management
September 2026

Why we did this, what we accomplished and where we are headed

- Mature the enterprise risk program
- Redesigned risk taxonomy
- Improved risk score and impact score methodology
- Enhanced risk discussions
- Next steps: Training and refinement

A risk taxonomy is a hierarchical **classification system** that standardizes how an organization defines and categorizes types of risks.



Mutually exclusive:

- Each risk category is distinctly defined so that any given risk can be assigned to only one category, eliminating overlap and ambiguity.

Collectively exhaustive:

- All possible risk areas are included within the framework, leaving no gaps where risks could be overlooked.

Benefits of our modernized ERM approach

Aspect	Previous Approach	New Approach
Distinct categories and subcategories	Limited	Robust
Automated processes	No	Yes
Dedicated ERM risk liaisons	No	Yes
Strategic plan mapping	No	Yes
Trend analysis	Limited	Robust
Reporting	Static	Dynamic

Proposed enterprise risk categories and subcategories

- Benefit Administration
- Financial Management
- Investment
- Legal/ Compliance
- Operational
- Reputation
- Strategic
- Technology

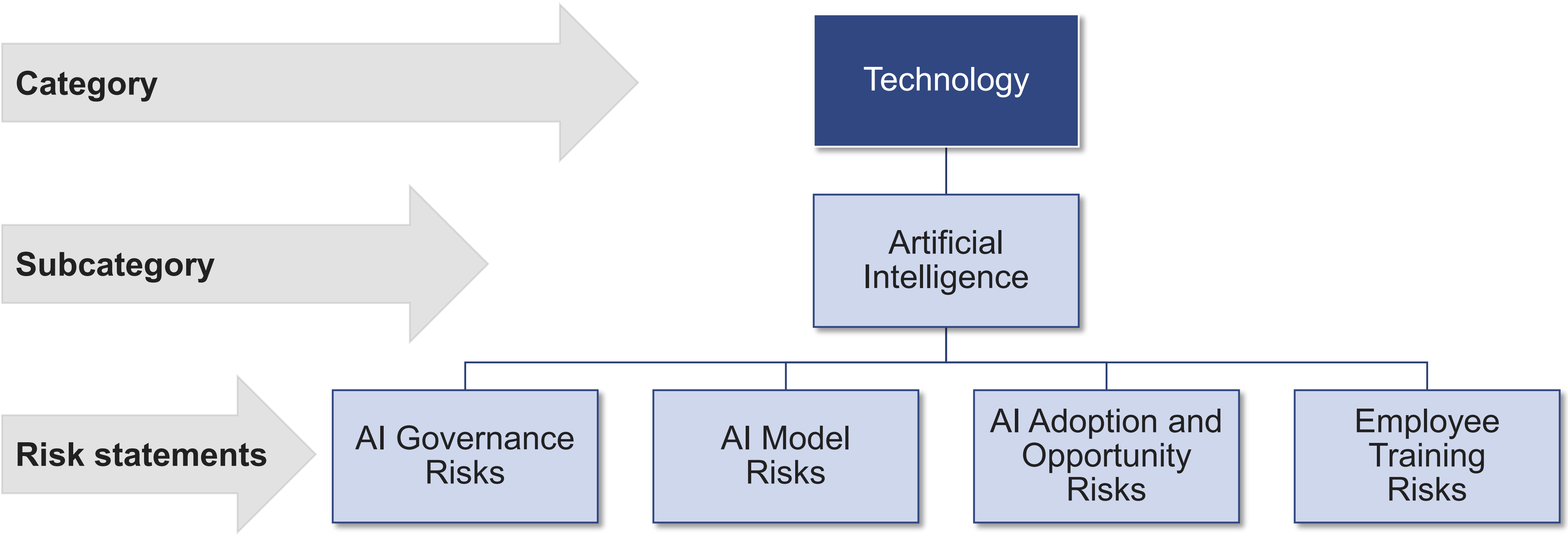
Proposed enterprise risk categories and subcategories

- **Benefit Administration**
  - Customer Education
  - Payment Accuracy
  - Service Delivery
- **Financial Management**
  - Accounting
  - Budgeting
  - Cash Management
  - Financial Reporting
- **Investment**
  - Investment Governance
  - Investment Operations
  - Portfolio Management
- **Legal/ Compliance**
  - Ethics
  - Legal Advice
  - Policy Management
  - Regulatory Compliance
- **Operational**
  - Business Continuity
  - Facilities Management
  - Talent Management
  - Vendor Management
  - Workplace Safety
- **Reputation**
  - Brand Reputation
  - Crisis Communications
  - Internal Communications
  - Stakeholder Engagement
- **Strategic**
  - Board Governance
  - Funding Plan
  - Strategic Planning
- **Technology**
  - Artificial Intelligence
  - Cybersecurity
  - Data Management
  - Project Management
  - Systems Resilience

Example of how we use this new approach to monitor risks

- Benefit Administration
  - Customer Education
  - Payment Accuracy
  - Service Delivery
- Financial Management
  - Accounting
  - Budgeting
  - Cash Management
  - Financial Reporting
- Investment
  - Investment Governance
  - Investment Operations
  - Portfolio Management
- Legal/ Compliance
  - Ethics
  - Legal Advice
  - Policy Management
  - Regulatory Compliance
- Operational
  - Business Continuity
  - Facilities Management
  - Talent Management
  - Vendor Management
  - Workplace Safety
- Reputation
  - Brand Reputation
  - Crisis Communications
  - Internal Communications
  - Stakeholder Engagement
- Strategic
  - Board Governance
  - Funding Plan
  - Strategic Planning
- Technology
  - Artificial Intelligence
  - Cybersecurity
  - Data Management
  - Project Management
  - Systems Resilience

Example of how we use this new approach to monitor risks



Improved risk scoring methodology

Aspect	Previous methodology	New methodology
Risk score calculation	= Impact x (Probability + Velocity) x Weighting factor	= Likelihood x Impact
Impact scoring categories	Operational	Strategic, Operational, Financial, Compliance, Reputation and Legal.

Example of Riskonnect dashboards and reporting

Next steps

- Continue configuration of Riskonnect and importing risk data.
- Training and rollout for risk champions and executives.
- Development of updated ERCC, ARM Committee and board risk reports.
- Ongoing refinement during FY 2026–27 as we monitor adoption and reporting needs.