

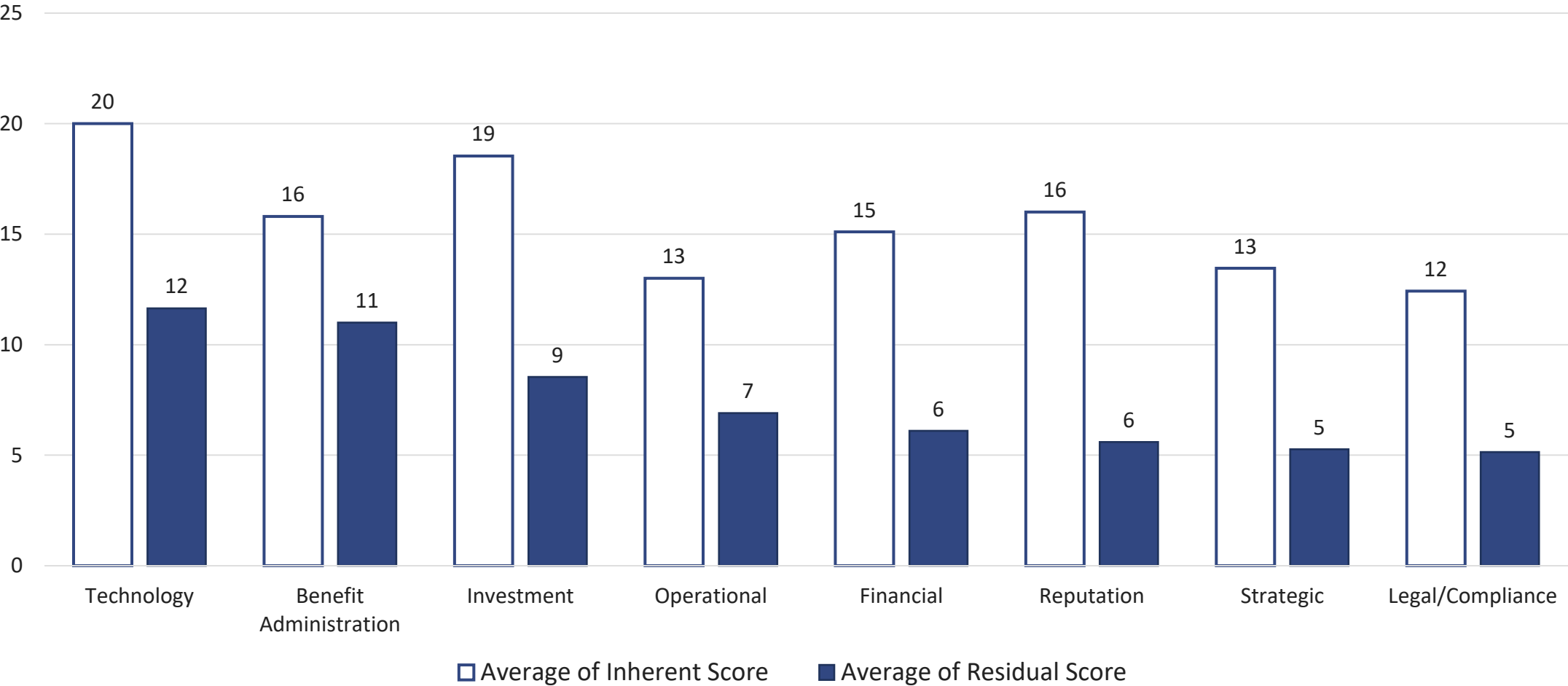


Enterprise Risk Management report as of September 30, 2026

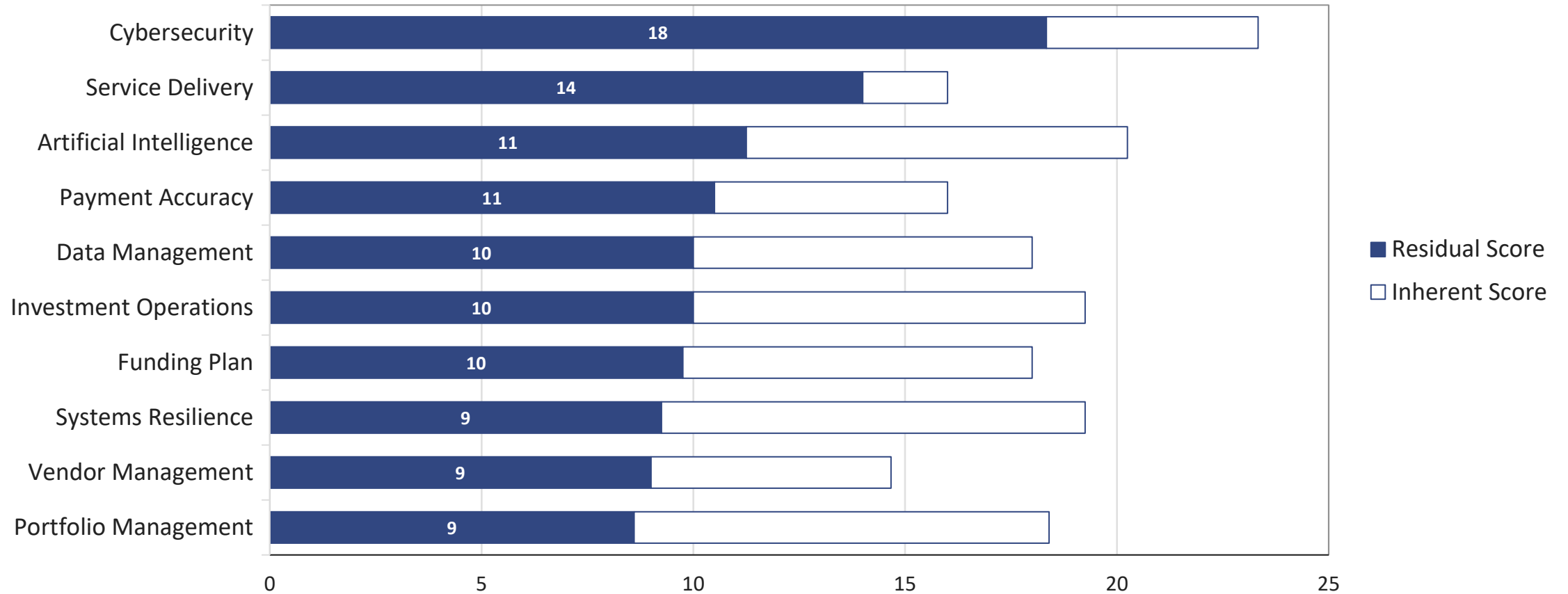
Presented to the Audits and Risk Management committee

November 2026

Risk scores by category



Top 10 residual risk scores by subcategory



Risk mitigation actions for top five risks

Risk subcategory	Risk owner	Mitigation actions
Cybersecurity	General Counsel	<ul style="list-style-type: none"> • Improve incident detection and response capabilities through 24/7 continuous monitoring with human oversight. • Strengthen identity and network elements of the zero-trust architecture to protect against unauthorized access.
Service delivery	Benefits and Services	<ul style="list-style-type: none"> • Recurring executive steering and operational workgroup meetings to guide BenefitConnect system stabilization. • Adjust staffing resources and workload to meet customer service needs.
Artificial intelligence	Technology Services	<ul style="list-style-type: none"> • Implement and test new AI tools in compliance with established standards; includes new technology evaluation process. • Implement training and processes to support AI adoption. • Continuously enhance governance processes.
Payment accuracy	Benefits and Services	<ul style="list-style-type: none"> • Provide training to employers on requirements for the new file format. • Provide training to employers to address audit findings. • Continuous improvement of payment reconciliation processes and reasonableness checks.
Investment operations	Investments	<ul style="list-style-type: none"> • Implement approved Investment branch shared vision, designed to maintain CalSTRS' position as a top global allocator.

Emerging and existential risks

Emerging risks

- Geopolitical disruptions
- Human capital
- Political polarization
- Post-quantum cryptography (NEW)

Existential risks

- Shift in pension fund management
- Demographic shift
- Shift to alternative education
- Federal funding restrictions to employers
- Next-generation artificial intelligence
- Cybersecurity event
- Comprehensive pension reform

Managing AI risk: Proven discipline, new controls



Same as
any other
risk

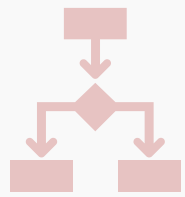
Same governance: Leadership sets the tone and risk tolerance
Same risk management lifecycle: Identify, assess, manage, monitor
Same risk equation: $\text{Impact} \times \text{Likelihood}$
Integrates into enterprise risk management – not a silo
Familiar risks: Privacy, data security, vendor management



What is
different

Probabilistic, not deterministic
Harder to explain and reproduce results
Risk from how people use it, potential for over-trust
Every use-case depends on context
Laws and regulators still catching up

AI risk framework



Govern

- Gen AI Policy, responsible-AI principles, and enterprise use-case intake



Map

- Risk-and-control map tying each AI risk to owners and mitigation plans



Measure

- Human-in-the-loop today; moving towards accuracy and drift monitoring



Manage

- Tiered access, approved-vendor catalog, tools blocking unapproved AI

Every identified risk has an owner, a control, and a maturity path.

CalSTRS AI risk landscape — Risks we are actively managing

AI Risks	Risk Rating	Key Controls in Place	Owner	Next Maturity Step
Cybersecurity and system resilience	High	Threat modeling; cyber reviews; network controls	General Counsel	Enhanced incident detection; zero-trust architecture
Third-party / vendor	Moderate	AI assessment questionnaire	Procurement / General Counsel	Contract addendum; model documentation
Strategic and emerging AI	Moderate	Portfolio governance; use-case intake	Executive Leadership / Tech Services	Formalize AI roadmap; agent governance
Model design and performance	Moderate	Human-in-the-loop on all decisions	Business Areas / Tech Services	Accuracy and drift monitoring
Data quality, privacy and leakage	Moderate	Data governance; tiered access; block unapproved AI	Business Areas / Tech Services	Metadata custody; shadow-AI scanning
Workforce	Moderate	AI literacy training; human-in-the-loop	Human Resources / Tech Services	AI literacy by role; readiness metrics
Ethical, fairness and reputational	Low	Gen AI Policy; responsible-AI principles	General Counsel / Compliance	Fairness testing; regular audits
Regulatory and compliance	Low	Compliance review; legal oversight	General Counsel / Compliance	Monitor regulatory environment; regular audits

Next steps

- Control validation
- Strategic plan mapping
- Reporting options for full board