**Chief Risk Officer**
**Office of Enterprise Risk Management**

## POSITION SUMMARY

Under the general supervision of the Secretary, the Chief Risk Officer (CRO) serves as the senior administrative leader responsible for overseeing the agency's enterprise risk management (ERM) program, business continuity planning, and Governance, Risk, and Compliance (GRC) functions—including enterprise privacy risk management and fraud prevention. As head of the Office of Enterprise Risk Management (OERM), the CRO develops and enforces agency-wide policies regarding the programs under the position's purview, provides strategic leadership on risk issues, and supports compliance with applicable laws and regulations.

The CRO exercises broad administrative and strategic oversight by managing personnel and financial resources to implement effective risk management initiatives across the agency. Acting as a principal advisor to executive leadership and governing bodies, the CRO influences top-level decision-making and setting of priorities based on risk exposure. This includes providing critical risk management and GRC oversight for significant employee benefits programs, such as the Wisconsin Retirement System and the State and Local Group Health Insurance Program, which serve hundreds of thousands of current and former public employees in Wisconsin and beyond. The CRO also represents ETF in external meetings with officials from other state agencies, oversight bodies, and the Legislature, and provides risk-related updates and recommendations to the agency's governing boards.

Additionally, the CRO supervises professional staff in the OERM, several of whom are in positions that have great impact on the agency's ability to administer benefit programs for Wisconsin's public employees and retirees. These staff include the Privacy Officer and agency Business Continuity Manager. The CRO collaborates with the Chief Information Security Officer and IT leadership on cybersecurity strategies and leads efforts to ensure that the agency's critical business operations are resilient in the face of disruptions. This impactful role requires exceptional leadership, strategic thinking, and communication skills to navigate complex regulatory environments and manage cross-functional teams.

ETF is a medium sized, non-shared services agency administering the Wisconsin Retirement System and related benefit programs to over 665,000 members receiving $7.2 billion in retirement benefits and $1.6 billion in health benefits annually. This position directly supports achieving the department's mission to develop and deliver quality benefits and services to our members while safeguarding the integrity of the Trust. As an employee of ETF, the incumbent will support and create a diverse and inclusive work force.

## TIME % GOALS AND WORKER ACTIVITIES

**45% GOAL A: Strategic leadership of the agency's enterprise risk management (ERM) program**

A.1 Exercise broad administrative and strategic oversight in developing and implementing the agency's ERM framework, policies, and procedures. (10%)

A.2 Manage the enterprise master risk register, ensuring risks are identified, assessed, and prioritized based on agency impact. Enterprise risk categories can include strategic risk, operational risk, reputational risk, IT/cybersecurity risk, workforce risk, business continuity risk, legal risk, vendor risk, and others.

A.3 Provide strategic direction to business operations areas across the department's diverse benefit programs to identify and assess risks, while ensuring comprehensive input and alignment in prioritization efforts.

A.4 Provide guidance to business operations areas on managing local risk registers that inform the enterprise master risk register. Ensure that business areas are still accountable for day-to-day management of their respective business operations risks.

A.5 Direct risk assessments as necessary for strategic initiatives, projects, and operational changes, and collaborate to develop actionable recommendations to the Secretary's Office and program managers.

A.6 Report regularly to the ETF Strategic Council and ETF Executive Team on the status of enterprise risk management, to discuss revisions to priorities, risk thresholds, and proposed mitigation strategies.

A.7 Represent ETF in external meetings related to enterprise risk management and other activities under the purview of the OERM, including reporting to ETF's governing boards, interactions with officials from other state agencies, legislative staff, federal or local government entities, professional associations, or external oversight bodies.

A.8 Evaluate and advise on proposed legislation or administrative code changes that may impact ETF's enterprise risk posture, strategy, compliance obligations, or operational resilience.

A.9 Direct risk training and education initiatives to promote a risk-aware culture.

A.10 Oversee the alignment of risk management strategy with the agency's strategic goals.

A.11 Provide strategic oversight and guidance to other areas of the organization to develop and enforce policies and procedures to address compliance and governance risks.

A.12 Provide management oversight of the Internal Control Plan, ensuring its alignment with the ERM framework and compliance with regulations. Review and update the plan at least annually to reflect changes in risks, policies, and agency priorities.

A.13 Collaborate with the Office of Internal Audit to identify gaps, recommend improvements, and integrate risk management strategies and practices into operational processes.

A.14 Collaborate with the Budget Officer to plan and allocate resources for risk management, ensuring that the program is adequately funded and staffed.

**20% GOAL B: Oversight of Privacy, Fraud, and Governance, Risk, Compliance (GRC) activities.**

B.1 Supervise the Privacy Officer, ensuring robust management of privacy policies, prompt responses to privacy issues, and strict compliance with applicable laws (e.g., HIPAA, state data protection laws).

B.2 Oversee agency responses to fraud incidents, guide investigations, and update the fraud response plan as needed. Collaborate with the agency's legal and audit areas to ensure compliance and risk mitigation.

B.3 Provide strategic leadership and oversight for the GRC program. Provide management direction in the development and enforcement policies and procedures to address compliance and governance risks. (6%)

B.4 Coordinate with the Office of Legal Services to address regulatory and compliance risks.

B.5 Collaborate with the CISO to identify information security risks and to align GRC strategies with agency goals and budget constraints.

B.6 Provide management oversight of annual staff training activities regarding GRC concepts, privacy compliance, and fraud awareness.

**20%** **GOAL C: Management of agency business continuity planning.**

C.1 Act as the agency's Deputy Agency Continuity Manager and ensure business continuity plans align with strategic priorities and critical business processes.

C.2 Provide high-level strategic oversight of the agency's business continuity planning, ensuring that recovery strategies are robust, tested, and aligned with Department of Administration (DOA) policies. (4%)

C.3 Collaborate with the Secretary's Office Administrative Policy Advisor on the development, alignment, testing, and updating of the agency's business continuity and incident response plans.

C.4 Direct business impact analyses to prioritize critical business processes and integrate findings into agency-wide recovery procedures, business continuity plan updates, and agency strategy.

C.5 Coordinate with ETF IT staff on technical management of business continuity planning elements.

C.6 Provide management oversight of annual tabletop exercises or other testing activities to validate the effectiveness of business continuity plans.

C.7 Lead an internal steering committee or Business Continuity Team to support the priorities and direction of ETF's business continuity planning and implementation efforts

**15%** **GOAL C: Management and direction of the Office of Enterprise Risk Management.**

D.1 Recruit, train, supervise, and evaluate OERM staff to ensure effective implementation of OERM responsibilities.

D.2 Oversee the development and management of the OERM budget, ensuring the agency priorities are met efficiently.

D.3 Establish performance metrics and reporting to monitor progress, inform leadership, and ensure continuous improvement of risk management activities.

D.4 Provide for training, guidance, and support to staff on ERM-related matters.

(Rev. 10/2025)

**KNOWLEDGE, SKILLS, AND ABILITIES:**

1. Extensive knowledge of enterprise risk management principles, frameworks, and methodologies, including their application in a public sector context.
2. Familiarity with risk management frameworks, such as COSO or ISO 31000, and their practical implementation.
3. Knowledge of federal and state laws and regulations applicable to public benefit programs, including privacy and data security requirements, such as the HIPAA Privacy and Security Rules.
4. Knowledge of organizational governance and fiduciary responsibilities, with an emphasis on compliance in a public sector environment.
5. Knowledge of fraud prevention, detection, and incident response planning, including coordination with internal and external stakeholders.
6. Analytical and problem-solving skills to assess risks, identify mitigation strategies, and make informed decisions.
7. Knowledge of privacy management practices, including data minimization, retention strategies, and effective response to privacy breaches and fraud incidents.
8. Knowledge of business continuity and disaster preparedness planning, including the development, testing, and implementation of continuity plans.
9. Familiarity with risk management and data analysis tools, such as Archer, MetricStream, or similar platforms, to inform decision-making and reporting.
10. Strong leadership and team management skills, including experience supervising diverse teams and fostering cross-functional collaboration.
11. Excellent written and verbal communication skills, including the ability to present complex information to a range of stakeholders.
12. Ability to align risk management initiatives with the agency's long-term objectives.
13. Knowledge of performance measurement and continuous improvement methodologies to enhance organizational resilience and efficiency.
14. Knowledge of principles and methods for effective training on risk management, compliance, and privacy.
15. Ability to understand and comply with all ETF and enterprise security standards, policies, processes, and procedures.