Position #512318
IS Technical Services Specialist
Information Security Analyst

POSITION SUMMARY

Working under the general review of the Chief Information Security Officer (CISO) in the Bureau of Information Security Management (BISM) this position provides the Department of Employee Trust Funds (ETF) with professional-level IS work including; technical design, implementation, maintenance, and ongoing operation of security controls for all aspects of ETF's information technology enterprise, including those systems and services hosted by the Wisconsin Department of Administration (DOA) Department of Enterprise Technology (DET).

This position assists the BISM Team Lead to ensure that ETF successfully manages information security risk with its technical initiatives, tools and processes. To that end, the incumbent provides advanced technical support in the development and implementation of security controls designed to support ETF's information security strategy and applies comprehensive knowledge to technical security projects for the development, testing and implementation of major platforms in the ETF application portfolio.

This position requires the incumbent to develop, maintain and optimize professional, collaborative relationships with internal ETF project teams, DET business and infrastructure teams and ETF contractors and vendors. This position independently resolves conflicts and problems through the skilled application of theoretical and practical knowledge of information security best practices as well as the application of ETF policies and standards.

The incumbent performs security administration tasks, as directed. The incumbent may also serve as a BISM representative at committees, meetings and other forums.

GOALS & WORKER ACTIVITIES

40% GOAL A: Provision of Scrum Leadership, Technical Expertise, and Industry Best Practices and Standards for Security-related Projects.

- A1. Lead projects, as assigned, to research, select, plan for, install, configure, operationalize, and maintain technical information security controls for ETF's enterprise-wide technical infrastructure and data across all platforms.
- A2. Function as security technical expert and serve as the Scrum Master to cross-functional project teams assigned to deliver security-related solutions, products and services.
- A3. Complete tasks to ensure timely, accurate and quality project delivery. Provide status and completion reports to the BISM Project Manager, Team Lead, and CISO.
- A4. Contribute to the development of information security-related strategic, tactical and operational plans.
- A5. Work with DET and approved vendors to oversee the secure installation, configuration, operation and maintenance of ETF infrastructure.

A6. Represent ETF BISM interests and/or act as a representative of BISM at state committees, meetings, conferences or other forums, as directed.

35% GOAL B: Provision of Technical Expertise Related to Advanced-level Support of Information Security Operations.

B1. Assist the Team Lead for BISM technical planning, research, advice and integration of information security-related improvements to ETF enterprise applications and infrastructure systems.

B2. Provide technical expertise to BISM technical staff providing information security-related support for ETF application and infrastructure issues.

B3. Define, research, recommend selection of, and integrate technical security controls to protect ETF data.

B4. Coordinate internal, state and vendor-provided technical risk assessments of ETF infrastructure and applications, the evaluation of results, and the proposal of solutions.

B5. Work with the CISO and Team Lead to implement and periodically test ETF's Incident Response Plan.

B6. Respond to information security incidents. Provide accurate, timely and quality technical and forensic information to ETF's strategic incident response team and other stakeholders' incident response teams, as appropriate.

B7. Provide consultation to the CISO and other ETF stakeholders to ensure ETF's information security-related systems are an integral part of the ETF Continuity of Operations Plan (COOP).

B8. Monitor compliance with security policies and procedures.

B9. Provide metrics and other output from information security-related systems and processes to CISO and ETF leadership as requested.

B10. Maintain change management documentation for information security-related systems.

B11. Provide domain administrator support to BITS, when needed.

15% GOAL C: Development, implementation and maintenance of information security standards and procedures.

C1. Collaborate with Bureau of Information Technology Services (BITS) personnel to ensure BITS operations comply with security principles, policy, standards and procedures.

C2. Collaborate with internal and external stakeholders, to develop and implement standards, procedures and technology that supports ETF's information security strategy.

C3. Develop and perform information security-related procedures for continuous monitoring of ETF's business applications.

C4. Collaborate with the ETF Office of Communications to ensure quality information security-related messaging to the ETF user community and other relevant stakeholders.

10% GOAL D: Participation in Employee Development Activities

D1. Work with other BITS staff on new and developing technologies and their impact on agency system security.

D2. Read books and periodicals to improve knowledge of information security and system design principles.

D3. Attend training sessions and workshops to increase knowledge of information security.

D4. Read security reports published by various public and private organizations, to stay current on newly discovered computer security vulnerabilities.

D5. Maintain knowledge and an ongoing awareness of Department values. Actively embrace the Department's values and fully incorporate them into the way you approach your tasks and perform your job.

D6. Carry out special assignments as directed.

(Rev. 06/2019)

KNOWLEDGE, SKILLS, and ABILITIES

KNOWLEDGE OF:

- Information security control framework theory
- Individual security controls as outlined in the CIS Top 20 or equivalent framework
- Planning, selection, implementation, operations and maintenance of security-related systems across multiple platforms and applications software
- Security-related systems specific to end-user compute devices
- Security-related systems specific to network infrastructure
- Security-related systems specific to software products, such as Microsoft Office and Microsoft Active Directory

SKILLED IN:

- Information system security-related planning, selection, implementation, and documentation processes and best practices
- Information technology training methods and techniques
- Communicating technical information effectively, either orally or in writing, to technical and non-technical users, technical teams, and senior management
- Use of information technology operating systems
- Coordinating and providing expertise related to the security and maintenance of network infrastructure
- Analyzing system problems and developing solutions
- Working independently or collaboratively with a variety of persons at technical and non-technical peer, consultant, and manager levels
- Providing consistent quality customer service
- Coordinating or leading the work of IT professionals or project teams
- Providing expertise and problem resolution across multiple platforms and software

ABILITY TO:

- Perform advanced work on security controls, with immediate impact or potential impact on ETF systems
- Coordinate the delivery of ETF security services to customers
- Coordinate and lead teams in planning and implementation of security controls, including testing and roll-back planning
- Provide technical direction for security systems and supporting technologies across multiple platforms
- Develop comprehensive operational procedures for documented, consistent use of security controls
- Work with end-users to remediate compliance issues related to security policies and practices
- Operate vulnerability scanning tools such as Qualys, Nessus, or equivalent
- Operate SIEM tools such as QRadar, Splunk, SolarWinds LEM, or equivalent
- Operate anti-malware tools such as Symantec, Norton, McAfee, or equivalent
- Operate web filter tools such as ZScaler, Forcepoint, Bluecoat, or equivalent

SPECIAL REQUIREMENT:

Due to the nature of this position, some non-standard work hours may be required.