Position #512320
IS Technical Services Consultant/Administrator
Information Security Governance, Risk, and Compliance Analyst
DMS/BISM

POSITION SUMMARY

Under the general supervision of the Chief Information Security Officer (CISO), this position supports the Department of Employee Trust Funds (ETF) and its partners in information security matters related to governance, risk, and compliance (GRC), and is intended to support the business side of information security. Technical knowledge is required for overall context but will comprise a small part of the duties associated with this position.

This position will develop and implement information security policy strategies, roadmaps and other instruments that ensure BISM's alignment with ETF's strategic objectives and industry best practice. This position will also lead and manage projects related to GRC on behalf of the CISO and key ETF stakeholders. This includes projects to develop, implement, maintain, and continuously improve an enterprise-wide information security risk management program using industry-standard guidance such as NIST 800-30 and ISO 27001. In addition, this position will also develop, document, seek approval for, implement, exercise, maintain and continuously improve the ETF Information Security Incident Response Plan (IRP).

The incumbent will lead business, change management, and project management activities for the BISM information risk management (IRM) program, working together with the BISM technical team and lead worker and the ETF Bureau of Information Technology Services (BITS) working groups, and support BISM's role in the development, testing and implementation of the ETF benefits and pension systems and other major platforms in the ETF application portfolio.

This position will oversee, manage, and consult on issues regarding federal and statutory compliance, internal audit, and third-party service providers.

This position requires the incumbent to develop, maintain and optimize professional, collaborative relationships with internal ETF groups, the Department of Administration (DOA), Division of Enterprise Technology (DET), and various contractors and vendors. It is also expected that the incumbent will "lead from the front" by setting an example for other ETF members in following applicable security practice, federal law, state statute, ETF policy, standards, procedures, and guidelines.

GOALS and WORKER ACTIVITIES

35% GOAL A: Development, management, and oversight of ETF management and business-related information security efforts

Worker Activity

- A1. Lead the selection, development, implementation, maintenance and continuous improvement of management and business-related information security controls.
- A2. Manage information security projects for BISM, to include communication, scheduling, facilitation and tracking of progress.
- A3. Oversee information security support for ETF contracting efforts, to include development, editing and negotiation of contract language.

A4. Plan, develop, communicate, obtain approval for, implement, and maintain an ETF-wide process for approving and implementing enterprise governance instruments such as strategies, policies, standards, procedures, and guidelines.

A5. Develop and maintain plans and strategies for the development, communication, approval, implementation and maintenance of information security policies and standards.

A6. Work to maintain and continuously improve ETF information security processes associated with HIPPA, Wisconsin statute and ETF's chosen information security frameworks.

A7. Lead BISM processes to maintain, track and report ETF workforce compliance with ETF policies, standards and required procedures.

A8. Provide communications intended for internal and external parties related to enhancing information security practices while encouraging input and participation.

A9. Oversee implementation, administration and report metrics for ETF's information security-related awareness, training, and drill efforts.

A10. Plan, develop, evaluate, and execute process modification strategies for new and changing business operational procedures.

A11. Lead problem resolution efforts with ETF staff as necessary while continuing to assure the security of ETF's information.

A12. Assist BISM technical personnel with evaluating, assessing, characterizing, and tracking information security related issues, vulnerabilities, and other threats to ETF's information.

30% GOAL B: Development, implementation, and maintenance ETF information security risk management program

Worker Activity

B1. Oversee development and implementation of business processes, policies, standards, procedures, forms, and other instruments designed to monitor, report, and continuously improve an ETF information security risk management program.

B2. Lead business and technical personnel in implementation of a metrics reporting program designed to monitor, report, and continuously improve the ETF information security risk management program.

B3. Initiate and maintain collaborative, productive working relationships with ETF business leaders and assist them in integrating the ETF information security risk management program into their business activities.

B4. Develop methods and processes for measuring and reporting ETF information security risk to the CISO and other key ETF stakeholders.

B5. Develop methods and processes for measuring and reporting on the effectiveness of current and planned information security controls.

B6. Lead risk-based analyses of ETF's identified and anticipated information security vulnerabilities and use this analysis to prioritize resource allocation designed to address those risks.

15% GOAL C: Development, implementation, and maintenance of the ETF information security incident response plan (IRP)

Worker Activity

C1. Lead development, implementation and maintenance of the ETF IRP and all associated business processes, policies, standards, procedures, and business relationships.

C2. Lead exercises of the ETF IRP upon initial implementation and twice per year thereafter.

C3. Oversee thorough documentation of "lessons learned" from IRP exercises and lead implementation of targeted, continuous improvements to the plan.

15% GOAL D: Provision of assistance for information security activities for the continuity of operations plan (COOP)

Worker Activity

D1. Working with the agency's COOP team, lead planning, development and implementation of the information technology service and security portions of the ETF COOP and all associated business processes, policies, standards, procedures, and business relationships.

D2. Lead information technology service and security portions of ETF COOP exercises.

D3. Oversee thorough documentation of "lessons learned" from COOP exercises and lead the implementation of targeted, continuous improvements to the plan as they pertain to information security.

5% GOAL E: Professional education and development

Worker Activity

E1. Continue education through academic, professional, and informal means, to include obtaining information security-related certifications.

E2. Maintain situational awareness of information security-related global, national news, trends, events, concerns and share such awareness with relevant stakeholders in ETF and other state agencies.

E3. Practice, advocate for, and maintain personal commitment to ETF core values and maintain a focus on customer service.

Knowledge, Skills, and Abilities:

1. Knowledge of information security guidance such as NIST 800-53 and the CIS Critical Security Controls for Effective Cyber Defense.
2. Ability to maintain confidential information in accordance with policies, guidelines, and direction from manager.
3. Ability to regularly demonstrate a high degree of professional integrity.
4. Thorough knowledge and understanding of information security processes, controls, technologies, and strategies.
5. Ability to work effectively with business partners and customers to solve business challenges while balancing the need for confidentiality, integrity, and availability.
6. Ability to demonstrate a commitment to fostering a diverse working environment.
7. Solid understanding of common and emerging information security attack vectors, penetration methods and countermeasures.
8. Ability to work independently, as part of a team of peers, and also to support and contribute to a multidiscipline team environment.
9. Knowledge of conflict resolution and incident escalation.
10. Excellent oral and written communications skills and skill in developing and maintaining effective working relationships with senior management, staff, and customers internal and external to the organization in order to clearly and effectively facilitate meetings, elicit information, present ideas/concepts/information, and coordinate security efforts.
11. Expert ability to identify, manage, and resolve problems.
12. Highly skilled in effective time management, organization, and priority-setting; high attention to detail.
13. Ability to explain and summarize highly complex technical information in a manner easily understood by others with varying degrees of knowledge or understanding and using plain language techniques.
14. Ability to analyze facts and apply sound judgement in decision making.
15. Understanding of technical concepts and technologies such as application security, secure coding concepts, endpoint security, edge technologies, enterprise management platforms and malware defenses.
16. Knowledge of project management principles, methods, and practices.
17. Knowledge of state, department, and industry activities, goals, objectives, priorities, and policies that may affect or be affected by development standards.
18. Advanced skills with PCs and software such as Microsoft Office (e.g., Excel, Word, Visio, etc.).
19. Ability to take the initiative to assertively represent business needs, to stand firm when necessary and to compromise when possible, to diplomatically challenge assumptions, and to make recommendations to business and technical staff at all levels of responsibility and authority throughout the organization.