CITY OF AURORA
JOB DESCRIPTION

JOB CODE: 237
SALARY GRADE: E17
EFFECTIVE/UPDATED: 12/18/2020

DIRECTOR CYBER & TECHNOLOGY RISK

Definition

Under direction of the Chief Information Officer (CIO), the Director Cyber & Technology Risk will develop and leverage a broad base of IT Risk Management, IT Security, IT Compliance, and Information Governance policies, standards and frameworks to address strategic business risks, issues, and questions impacting, underlying IT systems/platforms, business data/information and related business processes. Oversees an insourced Managed Security Services Provider delivering 24x7x365 Security Operations Center and Security Event Incident Management services whose primary objective is to oversee the front-line and reduce risk of intrusion. The position must understand the high-level strategy and direction of City initiatives stemming out groups such as IT, IT Security, Mayor/Alderman Offices, Public Safety, Public Information, Public Works, Development Services, Finance, Human Resources, City Clerk, Legal, etc. Responsible for supporting the mission and activities of the IT Project Management Office (PMO) as it relates to IT Security.

Equipment/Job Location

The noise level in the work environment is usually moderate. Performs duties in an office environment. Some travel may be required for field research, training, seminars and conferences. The employee frequently is required to sit. The employee must occasionally lift and/or move up to 100 pounds. The employee must be available for after hours and weekend on-call support.

Essential Functions of the Job

1. Anticipate, assess and mitigate operational, third party vendor, and compliance risks from current and changing business practices, systems, policies, procedures, regulations, and laws.

2. Research, define and articulate key elements of effective IT risk management, IT compliance, and information governance programs.

3. Develop and manage a team of IT risk management, IT compliance and information governance practitioners (full-time/contracted) capable of executing IT risk assessments and regulatory and compliance reviews.

4. Represent the organization to senior leadership through briefings and executive level reports (e.g., Board, Compliance, Audit, Risk Committees), planning sessions and other personal interactions.

5. Support and actively advise project teams to address risks, questions and issues and help interpret and outline effective IT risk management, IT compliance and information governance practices in coordination with IT Security, Legal and Internal Audit peers.

6. Lead a team to execute fit/gap assessments on current standards and policies to identify opportunities for policy refinement and enhancements.

7. Refine existing and develop new polices and standards outlining critical IT security and IT risk management practices (e.g., technical security controls, data security, data privacy, etc.).

8. Outline, define, and train roles and responsibilities on how to support and maintain effective IT risk management, IT compliance and information governance practices in the wider organization.

9. Coach peers and leaders to become more aware of the IT risk management discipline and to share best practices with stakeholders on new and existing initiatives and programs.

10. Budget ownership & planning responsibilities for the Cyber budget as part of the global Group Security budget.

11. Oversee the Group Security technology roadmap.

12. Oversees and reviews the performance of IT division personnel; examines current operational and performance levels.

13. Develops effective working relations with IT divisions and other city departments with whom work must be coordinated or interfaced.

14. Participates in the hiring, promotion, disciplinary action, termination recommendation, and salary adjustments of assigned staff.

15. Encourages appropriate training for employees and career path planning.

16. Helps build succession plans for critical IT employees.

17. Monitors network capacities, identifies potential weaknesses and coordinates this with the Director IT Operations and Infrastructure & Operation Teams.

18. Keeps current on computer industry trends and emerging software.

19. Performs other related special project duties as assigned.

Required Knowledge and Abilities

- Positive attitude under pressure
- Track record of delivering against deadlines
- Extremely proficient in evaluating urgency and dealing with multiple high priority issues simultaneously
- Process focused with the ability to think through solutions from concept, to engineering, to implementation, to support.
- Excel in collaborative, cross functional, and multi-cultural environments.
- Innovative thinking with an openness to accepting new ideas or thinking from others.
- Willingness to lead others with or without formalized reporting lines and directives.
- Project a positive and approachable attitude to those around you.
- Display and illustrate a high degree of thoroughness and dependability with strong ability to follow through to conclusions.
- Deep experience in core business, data and IT processes.
- Expresses high learning ability and interest in current and emerging technologies.
- Requires the ability to take a leadership role within the IT Division and oversee network and PC related activity.
- Requires the ability to implement strategy across multiple City departments and/or divisions.
- Requires the ability to supervise, support, and train staff in performing their daily responsibilities.
- Requires the ability to establish and maintain a good working relationship with all City departments, vendors, and outside agencies.
- Serves as the IRC who coordinates all cybersecurity incident response activities for the City. The IRC is responsible the staffing and resources of the SOC, the appropriate training of SOC personnel that have incident handling responsibilities and serves as the escalation point for incident response issues, and reporting lessons learned. The Incident Response Coordinator (IRC) is an extension of the CSIRT.

Qualifications for Hire

- Bachelor's Degree from an accredited college or university with course work in Computer Science, Business Administration, Accounting or related field.
- Requires at least ten (10) years of professional experience in IT risk management, IT security and compliance frameworks, information governance models and other operational risk capabilities.
- Strong ability to assess urgency and prioritization and make risk-based decisions based upon situational circumstances.
- Advanced skills and understanding of technologies and the underlying process surrounding data and information control.

- Demonstrated experience working with regulatory requirements, standards and frameworks including but not limited to (PCI-DSS, SOC, ISO, GDPR, NIST, HIPAA, CJIIS, etc.)
- Industry certifications (e.g., ISC2, CRISC, SCCP, ISSAP, CISSP, CISA, CISM, COBIT, etc.)
- Requires possession of a valid Illinois Driver's License.