BC PENSION CORPORATION

JOB DESCRIPTION

JOB DETAILS

Job Title: Enterprise Security Architect

Job ID: IS3033

Classification: Information Systems R30

Classification Date: (MM/DD/YYYY)

Branch: Information Technology Services

Unit: TIS-IT Security

Reports to: Assistant Director, IT Security

Security Screening: Yes

Union/Excluded: BCGEU

BRANCH DESCRIPTION

The Information Technology Services branch (ITS) provides the IT services to the BC Pension Corporation including; IT Operations, Application Development & Maintenance, Quality Assurance, Deployment and Mid-tier, and Service Management. Services are delivered from a team of dedicated contributors who provide ongoing support and transformational services to facilitate the execution of the 12/21 corporate strategy. This is an excellent opportunity for those interested in working with a team of professionals who enjoy a challenging and rewarding environment.

JOB SUMMARY

As part of the IT security team in the ITS branch, the Enterprise Security Architect leads the development, support and maintenance of the security architecture that meets the corporation's objectives. The Enterprise Security Architect works with various stakeholders to design the security architecture of the corporation's line-of-business applications, supporting infrastructure and create related policies, standards, processes and procedures. The Enterprise Security Architect manages IT security projects and provides information security expertise for architecture issues and advice regarding security risks and mitigation approaches. The Enterprise Security Architect leads, performs or oversees security risk assessments and vulnerability assessments. Other duties include managing IT security resources including contractors to meet project deliverables and objectives and developing and presenting security documents, reports, and briefing notes on issues impacting security technologies that protect corporation's infrastructure and information systems. The Enterprise Security Architect also responds to security incidents and conducts security investigations, and provides support and maintenance of the operational security capabilities.

This position handles confidential and sensitive matters and suitable for someone with strong leadership and communication skills and the ability to influence others.

JOB RESPONSIBILITIES

• Plans, develops, and implements the corporation's application security architecture, standards, solutions and framework, and incorporates them into the systems development life cycle.
• Develops the application security strategic direction within the corporation with business partners, and develops standards and procedures for responding to security incidents.

• Participates in strategic and operational security planning to achieve business goals by prioritizing initiatives and coordinates the evaluation, deployment, and management of current and future security technologies.
• Provides authoritative advice and subject matter expertise to internal and external stakeholders on security threats, regulatory requirements and technology changes that may affect the security of line-of-business applications and supporting infrastructure.

• Provides direction, expertise, guidance and support to staff, project teams and suppliers who are designing, developing, enhancing and maintaining business critical application systems and accessing the information assets of the corporation to ensure adherence to security standards and consistency with policies and best practices.
• Develops, recommends, maintains, and oversees enforcement of new or enhanced information security policies, standards, processes, and guidelines and evaluates new and emerging security technologies, tools and industry trends for applicability to the corporation.
• Provides information security expertise to application architecture issues, strategic corporation projects, security investigations and governance initiatives, and recommends revised approaches and new concepts to effect change.
• Plans and conducts or oversees various security assessments including vulnerability assessments, security audits, Security Threat and Risk Assessments (STRAs), assists with Privacy Impact Assessments (PIAs) for projects, systems, applications, develops and leads the implementation of mitigation plans to address risks and gaps found by assessments and audits, and tracks the mitigation action items and report on the mitigation work and ensure that systems

comply with audit requirements, quality assurance plans and security policies and standards.
• Develops and presents application security documents, reports, and briefing notes on issues impacting security policies, standards, procedures, and technologies protecting the corporation's line-of-business applications and supporting infrastructure, security risks and associated mitigation strategies, new or enhanced security standards to the Information Security Risk Committee (ISRC) or Technical Risk and Governance Committee (TRGC).

• Proposes and manages IT security projects, by developing concept and project proposals, business cases and charters; applying standard project management techniques, scheduling and prioritizing tasks and resources in accordance with the corporation's project management standards and processes; applying consistent quality assurance and change management practices; conducting post-implementation reviews for lessons learned and realization of benefits; and where applicable, participate in procurement activities in alignment with corporate policies and processes.
• Responds to escalated incident alerts and threats reported by the managed security service provider, the corporation's staff or other allies.

• Oversees the administration and maintenance of all security technologies and their associated software and provides support and maintenance of the internally managed operational security capabilities.
• Develops standards and monitors compliance of outsourced service provider(s) to the corporation's standards.
• Develops, leads and participates in the information security community of practice.
• Collaborates with other architects and solution engineers to develop solutions and ensure alignment of security architecture across all architecture domains and alignment with strategic goals.
• Liaises with vendors and other external security subject matter experts to update and advise the corporation on the most efficient and effective way to use standard methods, tools and best practices for securing information.
• As required, provides assistance and IT Security advice in the preparation and review of RFPs, RFQs and vendor responses.
• As required, supervises staff including assignment of work, mentoring, coaching, development and evaluation of performance plans and approval of leave.
• As required, manages resources and project teams to meet project deliverables and objectives, and procures, negotiates with, and manages contractors.
• As required, assists in developing security awareness and corporate training initiatives.
• Performs other related duties as required.

EDUCATION

Degree/Diploma Obtained	Program of Study

• Degree in computer science or related field and five years of information technology related experience; OR Diploma in computer science or related field and seven years of information technology experience; OR ten years of information technology experience.
• Professional designation as a Certified Information Systems Security Professional or Certified Information Security Manager, or equivalent.

EXPERIENCE

Years of Experience	Type of Experience

• Minimum of three years of experience developing security architecture in a large, complex organization.
• Minimum of three years of experience conducting security threat risk assessments.
• Preferred Qualifications include:
o Experience with configuring, running, validating and contextualizing the findings of vulnerability discovery tools such as NMAP, Burp Suite, or Open Web Application Security Project Zed Attack Proxy (OWASP ZAP).
o Experience working in software development, securing Application Programming Interfaces (APIs), working with continuous integration tools (e.g., Jenkins).
o Experience performing code reviews and/or using static analysis tools and participating in agile development projects in a DevOps environment.
o Experience working in security within the insurance, financial, pension administration sector.
o Professional designation/certification in any of the following:
Global Information Assurance Certification Penetration Tester (GPEN)
Global Information Assurance Certification Web Application Penetration Tester (GWAPT)
Global Information Assurance Certification Defensible Security Architecture (GDSA)
Sherwood Applied Business Security Architecture (SABSA) Chartered Security Architect
IT Infrastructure Library (ITIL) certifications
• Minimum of one year of experience supervising IT professionals.

KNOWLEDGE, SKILLS & ABILITIES

o Talent for establishing, maintaining and promoting effective collegial relationships with a variety of groups or individuals to meet program objectives, complete projects, or to influence outcomes.
o Knowledge of change management processes and project management methodologies.
o Knowledge of architecture development processes, information management technologies and security foundations.
o Knowledge of secure application design and development life cycle.
o Knowledge of identity access management, common web application security risks and prevention/mitigation techniques.
o Knowledge of all aspects of IT security including current technologies and best practices and relevant standards from organizations like the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and the Committee of Sponsoring Organizations of the

Treadway Commission (COSO), the American Institute of Certified Public Accountants (AICPA).
o Knowledge of NIST Framework for Improving Critical Infrastructure Cybersecurity, ISO/IEC 27002 and System and Organization Control (SOC) Reports
o Knowledge of computer hardware, software, networks, communications, connectivity, security appliances (e.g., firewalls, routers, etc.) and communication protocols as they relate to networking.
o Ability to handle confidential issues with tact and diplomacy.
o Ability to continuously learn ever-changing information security-related developments including vulnerabilities and testing methodologies.
o Ability to balance security requirements and designs with business drivers and needs.
o Ability to work as part of a team or independently, and to exercise judgement in resolving problems.
o Demonstrated good written and verbal communication skills with excellent attention to detail when communicating both verbally and in writing

CORE COMPETENCIES

Navigating Change L2
Supporting self and others through change and transition and enabling successful transformation in work products and processes.

- Invites input and feedback on proposed changes.
- Supports others in generating new and innovative approaches.
- Builds support for new approaches and initiatives.
- Shares information on change in a timely manner.
- Identifies innovative approaches to deal with situations for which no known precedent exists.
- Eliminates unnecessary work activities.

Embracing Learning L2
Contributing to a learning culture by developing self and supporting others to acquire skills and improve performance.

- Gathers feedback from various sources to identify own strengths and weaknesses.
- Pursues challenging experiences beyond current position to add value in own area.
- Helps others identify learning needs to meet current job requirements.
- Provides honest, timely, clear and specific feedback to others.
- Ensures people are provided appropriate training within available budget and resources.
- Encourages people to reach their full potential.

Client Orientation L3
Making it easy for our external and internal clients - seeing things through their eyes.

- Balances client needs with business realities.
- Represents client needs to more senior management.
- Provides advice on complex problems and initiatives.

Accountability L2
Holding self and others accountable to deliver on commitments and to achieve desired results.

- Sets challenging but realistic goals for own area of responsibility.
- Helps people improve performance to maximize results.
- Holds people accountable for meeting established expectations.
- Evaluates progress against established goals and objectives.

Inspiring Trust L3
Inspiring confidence by demonstrating integrity and building credibility.

- Brokers healthy relationships across the organization to further the achievement of business goals.
- Promotes dialogue and shared understanding on business issues.
- Communicates complex issues clearly and credibly with varied audiences.
- Confidently and effectively expresses contrary opinions and own perspectives.
- Accepts alternate perspectives in support of business interests.
- Models trust in others to do their jobs.

Decision Making L2
Enabling progress by resolving issues and supporting others in taking calculated risks and making decisions.

- Involves the right people in the decision making process.
- Makes decisions by weighing several factors, some of which are partially defined with missing pieces of information.
- Uses sound business sense to make decisions.
- Considers risks when identifying or recommending options.
- Provides context and rationale for decisions.
- Provides information to others to support decision making on complex issues.

Organizational Focus L3
Aligning work priorities, processes and practices to achieve the strategic direction.

- Demonstrates an understanding of interdependencies across the organization (i.e. systems thinking).
- Responds to emerging trends with initiatives that are aligned with the organization's strategy.
- Translates strategic goals into specific operational initiatives.
- Ensures work unit objectives are aligned with the strategic goals.
- Balances short term needs of the organization and its people with the achievement of longer-term goals and strategies.
- Applies understanding of organizational context in dealing with complex issues.
- Aligns business operations across the organization.