



## PR/096946 | Technical Information Security Officer

### 募集職種

#### 人材紹介会社

ジェイエイシーリクルートメントシンガポール

#### 求人ID

1599606

#### 業種

ITコンサルティング

#### 雇用形態

正社員

#### 勤務地

シンガポール

#### 給与

経験考慮の上、応相談

#### 更新日

2026年06月26日 11:49

### 応募必要条件

#### 職務経験

6年以上

#### キャリアレベル

中途経験者レベル

#### 英語レベル

ネイティブ

#### 日本語レベル

無し

#### 最終学歴

短大卒：準学士号

#### 現在のビザ

日本での就労許可は必要ありません

### 募集要項

#### Company Overview

My client is a leading Japanese trust bank with a strong global footprint, offering a broad range of financial and fiduciary services. The bank places strong emphasis on technology risk management, cybersecurity, and regulatory compliance to safeguard its systems, data, and clients.

#### Role & Responsibilities

- Technology Risk, Security & Governance
  - Provide independent second-line technical oversight of information security and technology risks as part of the Technology Risk Management (TRM) team.
- Support the maintenance and continuous strengthening of a robust technology risk and information security governance framework.
- Contribute technical expertise to the drafting, review, and ongoing maintenance of technology and information security policies, standards, and procedures, ensuring alignment with regulatory and internal requirements.
- Maintain strong familiarity with MAS and other applicable regulatory requirements, internal security policies, and industry best practices.

#### Regulatory Compliance & Security Oversight

- Perform and lead in-depth gap assessments of policies, procedures, and controls against regulatory technology risk management and cybersecurity requirements.
- Monitor regulatory developments and supervisory expectations, assess their impact, and recommend enhancements to the technology risk and cybersecurity framework.
- Provide independent technical validation of implemented security controls to assess design adequacy, operating effectiveness, and compliance.

#### Incident Oversight & Control Validation

- Represent the TRM function in collaboration with First Line of Defence teams on security incidents, including oversight of root cause analysis and validation of remediation actions.
- Review technical incident reports and post-incident assessments, providing independent challenge, risk-based observations, and recommendations to address underlying control gaps.

#### Risk Register, Reporting & Security Exercises

- Oversee the Technology Risk Register, monitor risk treatment plans, and engage risk owners to ensure remediation actions are executed effectively and within agreed timelines.
- Review security assessment, testing, and assurance reports, providing independent technical commentary and risk perspectives.
- Plan, coordinate, and oversee adversarial attack simulation exercises (e.g. Purple Teaming) to evaluate the effectiveness of security controls and detection capabilities.

#### Advisory, Stakeholder Engagement & Continuous Improvement

- Provide technical security advisory input and technology risk guidance to management and relevant stakeholders.
- Stay abreast of emerging cyber threats, technologies, and regulatory expectations, and share timely insights with local management and Head Office stakeholders.
- Support and participate in additional technology risk management and cybersecurity initiatives as required.

#### Requirements / Qualifications Education & Professional Certification

- Bachelor's degree in Cybersecurity, Information Technology, Computer Science, Engineering, or a related discipline.
- At least one recognised information security certification such as CISSP, CRISC, or an equivalent qualification.

#### Experience & Technical Expertise

- Minimum of 7 years' experience in information security, including at least 3 years in security operations or hands-on technical security roles.
- Strong understanding of the cyber threat landscape, attack techniques, and defensive security controls.
- Proven experience with security assessments, security architecture reviews, control validation, and remediation planning.
- Good working knowledge of public cloud environments (e.g. AWS, Azure), including associated security controls, risks, and governance considerations.

#### Skills & Competencies

- Strong analytical and problem-solving abilities, with the capability to translate technical security requirements into regulatory and business contexts.
- Sound technical judgment when assessing security incidents, vulnerabilities, and control effectiveness.
- Effective communication and influencing skills, enabling engagement with both technical and non-technical stakeholders.
- Detail-oriented, resilient, and able to think strategically when identifying, assessing, and mitigating technology and cybersecurity risks.

#### Additional Advantage

- Exposure to data governance concepts, including data classification, information asset classification, and system criticality frameworks, is an advantage.

**Notice:** By submitting an application for this position, you acknowledge and consent to the disclosure of your personal information to the Privacy Policy and Terms and Conditions, for the purpose of recruitment and candidate evaluation.

Privacy Policy Link: <https://www.jac-recruitment.sg/privacy-policy>

Terms and Conditions Link: <https://www.jac-recruitment.sg/terms-of-use>

---

