



The eMPF Platform Company Limited (eMPF Company) is a wholly owned subsidiary of the Mandatory Provident Fund Schemes Authority (MPFA) responsible for building and operating the eMPF Platform (eMPF). The eMPF Platform is a major public utility which aims to standardize, streamline and automate the existing MPF scheme administration processes. It is the most significant reform of the MPF System since its introduction in December 2000.

For background and details of the eMPF Platform, please go to our website <https://www.empf.org.hk>

We are looking for high calibre and passionate individuals to join us to undertake this transformation initiative that is leading the MPF ecosystem to a new era and is creating a positive impact on the working population of Hong Kong.

## **Manager – Risk Management**

### **(Job reference no.: eMPF011/2026)**

#### **Key Accountabilities**

Assist the Team Lead / Senior Manager in the following duties:

- Executing and refining the monitoring framework and mechanism in respect of technology risks and information security management for managing the eMPF platform (the Platform) which is developed, administered and operated by a third party delivery partner (the “Delivery Partner”);
- Executing and refining the governance framework of technology risk management and information security to ensure adherence to relevant regulatory requirements and best practices for benchmarking the Delivery Partner’s deliverables;
- Ensuring policies and procedures are properly enforced and monitored in actual practice to achieve relevant governance goals;
- Working closely with the Delivery Partner to review and approve deliverables, including but not limited to the completeness and reasonableness of the detailed work submitted by the Delivery Partner comparing with market practice, e.g. maintenance of a fit and proper technology risk management framework, up-to-date security measures for detecting, preventing, managing and monitoring attempted cyber intrusions or financial crimes against the Platform, tools for reporting and monitoring issues, incidents and risks, and promote information and technology security awareness across all relevant personnel supporting the Platform etc.;
- Establishing and providing oversight on technology risk and information security related work by the Delivery Partner, including but not limited to working with the Delivery Partner to develop and refine reporting metric (such as risk indicators), risk controls assessments, incidents and risk register to record and monitor all potential risks being identified, and ensuring proper monitor and follow up on the identified risks through the implementation of rectification;
- Overseeing the Delivery Partner’s operations and management of technology risk management and information security related initiatives;
- Ensure proper response and handling, escalation and reporting of system security incidents;
- Ensuring the implementation of initiatives adhere to strategic architecture, governance model and up to market standards;
- Leading and driving the security risk assessments, red team security tests, and compliance assessments on information security and technology risk; and

- Providing regular and ad hoc reporting to management on work progress and potential issues. For issues handling, collaborating with the Delivery Partner, Risk Management Team, Digital & IT Team, Data Assurance Team and other relevant teams, as appropriate, on root cause analysis as well as review and monitoring of remediation plans and implementation.

### **Skills and Qualification**

- Degree holder in Computer Science / Information Security or related disciplines;
- Minimum 8 years of relevant experience in multiple areas including technology risk, information security, cyber security, regulatory compliance in a financial services and/or public sector environment;
- Relevant security management and IT audit qualifications, e.g. CISM, CISSP, CISA, CRISC or equivalent;
- Extensive knowledge on information security and technology risk management principles and best practices;
- Hands-on experience in configuring security devices, SIEM monitoring, penetration test, red team security test, risk controls implementation is preferred;
- Knowledge of PDPO, ISO 27001 and general compliance as well as infrastructure and applications;
- Good vendor management experience for large-scale projects;
- Proactive, responsible, strong sense of work ownership, good problem solving, communication and interpersonal skills, independent and yet a good team player with strong market sense and analytical thinking;
- Can work under pressure and meet tight schedule; and
- Good command of both spoken and written Chinese and English.

### **Remuneration Package**

Rank and salary will be commensurate with qualification and experience. The initial appointment will be made on a fixed-term contract. A competitive remuneration and benefits package including discretionary performance-linked variable pay, annual leave, medical, dental and life insurance coverage, and MPF will be offered.

### **To Apply**

Interested candidates are invited to apply via our [online application](#). The closing date for application is **11 June 2026**. Applicants not contacted for follow-up within 3 months after the closing date for application may assume that their applications are not successful. Applications not selected for further processing may be considered for other relevant openings in the future but their applications will not be retained for more than a period of two years after the closing date.

The information provided will be kept confidential and only be used for those purposes relating to your application. Please visit our website for the details of the MPFA's Personal Information Collection Statement at <https://www.mpfa.org.hk/en/mpfa/joining-mpfa/job-vacancies/personal-information-collection-statement>. The MPFA and its subsidiary are equal opportunities employers and welcome applications from all qualified candidates.

(如欲索取中文版本，請電郵至 [eMPFHR@empf.org.hk](mailto:eMPFHR@empf.org.hk))