Arrangement for Generative A.I. Sandbox++ ("Sandbox")

Objectives

- The Sandbox is intended to:
    - support the development, testing, and pilot of innovative Artificial Intelligence (A.I.) and Generative A.I. (GenA.I)-based solutions in the financial industry; and
    - provide early targeted supervisory feedback to participants in the Sandbox and share good practices in the adoption of A.I. and GenA.I, drawing on insights gained from Sandbox trials.

Focused Areas and Example Use Cases

- The Sandbox use cases are expected to focus primarily on enhancing risk management, anti-fraud measures and customer experience. Some non-exhaustive examples are shared below to inspire innovative ideas:
    - **Risk management** – Optimise risk management processes across the full range of risk disciplines, including evaluation of creditworthiness by analysing financial statements and other unstructured data of borrowers to enhance loan approval efficiency, assessing the compliance of suitability requirements when distributing investment products, identifying deficiencies in listing documents of new listing applicants prepared by sponsors, the improvement of underwriting decisions through the analysis of structured and unstructured data, and the forecasting of claims to support informed decision-making;
    - **Anti-fraud measures** – Detect and prevent fraudulent activities, including "deepfake" scams; review websites, emails, and message contents to automatically identify fraudulent messages and devise timely responses; identify forged documents submitted during the client onboarding process; and review claim documents and communications to identify anomalies; and
    - **Customer experience** – Elevate customer engagement through more advanced customer service chatbots capable of generating personalised responses based on individual customer background, transaction records, and past interactions, as well as providing real-time updates on claims status.
- The themes are not intended to be exhaustive. Use cases that extend beyond these areas and deliver broader societal and economic benefits are also encouraged. This may include innovations that strengthen financial resilience, promote sustainable development and enhance public well-being, for example leveraging A.I. to improve climate risk assessment, expanding access to financial services for underserved communities, advancing health protection and supporting more effective long-term financial and retirement planning.

- All Sandbox use cases should incorporate components of A.I. safety and risk management, including but not limited to bias detection and mitigation, explainable A.I., and frameworks for A.I. output monitoring and evaluation.
- Participants are encouraged to explore "A.I. vs. A.I." strategies as part of their trials, by leveraging A.I. to validate, safeguard, and enhance the accuracy and robustness of A.I. outputs.

General Principles

- The focus of the Sandbox is on solutions that demonstrate a significant level of innovation and potential for substantial impact. Priority will be given to solutions that align with these criteria.
- Adhering to the principle of data minimisation, participants are encouraged to adopt data sanitisation techniques such as data masking or tokenisation on their training data, where applicable, to minimise the risk of data leakage. Participants may leverage public data, anonymised data, or synthetic data where appropriate, with a focus on validating workflows, methodologies, and risk controls, while ensuring that A.I. solutions are trained and tested under realistic conditions.
- A secure data transfer and access mechanism will be made available to ensure the confidentiality and integrity of data used within the Sandbox. Participants are expected to review and implement adequate data security controls, including encryption and access controls where necessary.
- The level of A.I. or GenA.I.-specific risk mitigations associated with proposed solutions will be a key factor in project selection. Priority will be given to projects that explore and test a wide range of GenA.I.-driven risk mitigation strategies over simpler or commonly adopted cases, which may offer less learning or impact.

Key Factors for Consideration in Evaluating Applications

- **Level of innovation** – The extent to which the proposed solution introduces novel or alternative ideas, methodologies or models that have the potential to create new digitalisation opportunities;
- **Complexity of the solutions** – The technical sophistication and intricacy of the proposed solutions to promote advancement and added value;
- **Expected contribution to the industry** – The potential for the proposed solution to make a meaningful impact on the financial services sector, such as by addressing industry-wide challenges or by formulating new solutions replicable and scalable by different institutions; and
- **Adherence to the principle of fair use** – The degree to which the proposed solution is designed to be used in a fair, responsible, and ethical manner, avoiding harm to others or misuse of computing power.

Application Procedures

- Applicants are required to provide detailed information, including high-level design, applicable models, risk assessments of their proposals and information about their technology partners.
- Applicants may be contacted for additional information during the evaluation process. The processing time will vary depending on, inter alia, the complexity of the use case, the quality of information provided, and responsiveness to follow-up questions.
- Interested parties may submit their applications through the respective channels listed below and direct any inquiries to the contacts provided:

Type of Institution	**Channel**	**Contact**
Authorized Institutions under the Banking Ordinance (Cap. 155)	The HKMA's Survey Tool platform	GenAI_sandbox@hkma.gov.hk
Licensed Corporations under the Securities and Futures Ordinance (Cap. 571)	Via Email GenAI_sandbox@sfc.hk	GenAI_sandbox@sfc.hk; and please contact your case officer.
Authorized Insurers and Licensed Insurance Broker Companies under the Insurance Ordinance (Cap. 41)	Insurtech Facilitation Team	insurtech@ia.org.hk
MPF Approved Trustees and Principal Intermediaries under the Mandatory Provident Fund Schemes Ordinance (Cap. 485)	Via Email GenAI_Sandbox@mpfa.org.hk	GenAI_Sandbox@mpfa.org.hk
Stored Value Facility Licensees under the Payment Systems and Stored Value Facilities Ordinance (Cap. 584)	Via Email pssvfo@hkma.gov.hk	pssvfo@hkma.gov.hk

Expectations on Participants

Institutions accepted into the Sandbox are expected to:

- Allocate sufficient internal resources to manage their participation effectively, including project management, technical execution, and coordination with technology partners where applicable;
- Provide regular updates to their respective regulators on project progress as requested;
- Actively participate in Sandbox events and knowledge-sharing activities; and
- Submit a final report to their respective regulators upon conclusion of the Sandbox, detailing the outcomes of their trials and key learnings.

Arrangements for Sandbox Collaboratory and Facilitation Events

- Sandbox Collaboratory and other facilitation events will be organised to support the development and refinement of use cases.
- Interested institutions and technology vendors will be organised into dedicated sessions based on their interests, areas of expertise, and availability.
- During these workshops and events, institutions may identify and collaborate with technology partners to carry their use cases forward for further exploration and more comprehensive testing within the Sandbox following initial ideation.

Others

- Admission to the Sandbox does not indicate endorsement of the solution by the respective regulators.
- Sandbox participants intending to implement the solution after the Sandbox should adhere to the established procedures when adopting new technologies.
- Details of sandbox participation, including the identities of approved participants and their technology partners, may be publicly disclosed.
- Sandbox requirements may be modified as necessary, based on participants' proposals and testing.

Frequently Asked Questions

General Information

1. **Who can participate?**
   The GenA.I. Sandbox++ is open to the regulated entities listed above and their partnering technology firms. All applications must be submitted by regulated entities.

2. **Should institutions submit sector-specific or cross-sector use cases?**
   Both sector-specific and cross-sector use cases are welcome. The selection of use cases will be based on the evaluation criteria listed above.

3. **Is there a restricted list of technology vendors that institutions must partner with?**
   No. A catalogue of technology providers, including language model providers, GenA.I. solution providers and consultancy firms, is available through Cyberport for reference and consideration. Institutions may collaborate with any technology providers of their choice.

4. **Can an institution apply without partnering with a technology partner?**
   Yes, institutions may submit applications without partnering with third-party technology providers. However, collaboration with technology firms is strongly encouraged as they may contribute to better project outcomes through their specialised expertise and practical experience.

5. **Can an institution submit more than one use case?**
   Yes, institutions may submit multiple use cases. However, institutions are advised to prioritise internally, focusing on high-impact proposals rather than submitting a large volume of use cases.

6. **What is the cost of participation?**
   Participation in the Sandbox is free of charge. Participants are responsible for any internal costs they may incur, such as staff resources or commercial engagements with technology partners.

Technical and Operational Details

7. **Where are trials conducted?**
   Trials will be conducted within a secure environment at the A.I. Supercomputing Centre operated by Cyberport.

8. **What support will participants receive?**
   Participants will receive technical support, supervisory guidance, networking opportunities, and access to Cyberport's A.I. Supercomputing infrastructure.

9. **What are the expected scale and computational requirements for Sandbox trials?**
   Trials should be appropriately sized for a sandbox environment and designed as exploratory, time-bound initiatives. The Sandbox is intended to support experimentation, learning, and early validation, rather than large-scale or production-grade deployment.

10. **How long does the Sandbox run?**
    The Sandbox, including preparation work and final report writing, generally lasts six to eight months following the announcement of selection results. Extensions may be granted on a case-by-case basis.