Annex

Good practices for managing third-party IT solutions

1. Third-party Risk Assessment

- Reviewing and enhancing risk assessment processes - Throughout the third-party life cycle management, assess the risk associated with third-party software updates:
  - Understanding the system privilege permissions required by the software for normal operations and evaluating the operational and security impact in case of software failure or malfunction.
  - Assessing the software vendor's update deployment processes to understand how different types of updates (e.g. security patches, feature updates) are delivered and installed, and their implications on the bank's ability to control, schedule, and monitor the software update process.
  - Enhancing the bank's control over receiving and deploying such updates (e.g. ability to deploy updates to a smaller set of devices/systems, selective updates) following a risk-based approach.
  - Evaluating the testing process conducted by the software vendor prior to releasing updates.
  - Ensuring that any changes to the software update model and their implications are thoroughly communicated to the bank.

2. IT Change / Patch Management

- Evaluating software update scheduling and monitoring processes - Assessing the bank's processes for scheduling, controlling, and monitoring software updates from third-party vendors, while enhancing the framework and processes to accommodate automated software updates (e.g. utilising a centralised internal server or proxy instead of updating directly from vendors' servers to the endpoints to exert greater control over update frequency and release schedule).
- Implementing testing and rollback procedures - Ensuring that appropriate testing and rollback procedures are in place to mitigate the risk of faulty updates.
- Adopting gradual deployment strategies - Implementing a gradual approach (e.g., pilot testing, phased rollout, use of "N-1" version) to deploy updates where feasible to reduce potential disruptions.

3. Privileged Access Management

- Managing privileged access - Ensuring that the software is installed and configured in adherence to the least-privilege principles and on a need-to-have basis to minimise unnecessary risk exposure.

4. Preparedness and Recovery Capabilities for IT Incidents

- Defining communication and escalating protocol for large scale outage of common IT infrastructure - Implementing a robust communication and escalation protocol to ensure swift response and effective collaboration among the bank, vendors and other relevant stakeholders.
- Identifying critical interdependencies - Identifying and addressing critical interdependencies necessary for recovery such as enabling IT team's access to troubleshooting tools, retrieval of cryptographic keys, and third-party support.
- Ensuring robustness of system backups - Enhancing the robustness of system backups to facilitate prompt restoration of services in the event of an incident.

As the third-party risk landscape continues to evolve, your institution should implement an effective mechanism for managing the risks associated with third-party dependencies, taking into account the good practices shared above.