Advisory on IT Change Management Best Practices

November 2023

Contents

1. Background

1.1 Financial and Insurance Institutions ("Institutions") in Singapore have undergone significant digital transformation in the past few years and the pandemic has further accelerated such transformation.

1.2 Digital transformation inevitably means more systems and changes, and this increases institutions' exposure to technology failures. This supports the industry's observation of an upward trend in the number of IT incidents in Singapore since 2019, which have caused considerable amount of impact to the institutions and their consumers.

1.3 Further analysis shows that a large number of institutions' IT incident were due to change management. As such, there is a need to address this gap and focus on improving current practices to reduce the number of incidents.

1.4 A joint working group with representatives from the ABS Standing Committee on Cyber Security (SCCS) and Insurance SCCS was formed. This advisory is the working group's collective effort to gather, analyse and share the best practices related to change management, "from" the industry and "for" the industry.

1.5 This advisory provides best practices and recommendations for the financial institutions in Singapore to strengthen their change management process based on the nature, size and complexity of their business.

2. Best Practices Recommendations

2.1 Change Governance and Oversight

2.1.1 The institutions should ensure that there is comprehensive change management strategy, policy, standard, and procedure ("documents") in place, aligned to the institution's size and operations, communicated to and accessible by all the stakeholders. These "documents" should be reviewed, tested, and updated as needed on a periodic basis. Knowledge base accumulated could be embedded into the procedure or maintained separately, for standardised adoption.

2.1.2 The institutions should ensure that the roles & responsibility matrix, or equivalent, is clearly defined, reviewed, and updated regularly for the stakeholders involved in the change management process.

2.1.3 The institutions should have clear definition and criteria of change success and failure.

2.1.4 For the emergency changes, the institutions should put in place a clearly defined criteria for what is permitted as an emergency change. Emergency changes, despite the short notice, still need to have adequate testing completed and authorized by appropriate approvers.

2.1.5 For the retrospective changes, proper recording, approval, and testing should still also be conducted.

2.1.6 For the changes related to critical initiatives or major migrations, they should not be classified under emergency changes.

2.1.7 The institutions could consider having higher level approval requirement for changes that need to happen during the change freeze periods.

2.1.8 Besides establishing pre-production change controls, the institutions should also consider instituting post-production controls, including change completion validation, rolling back plan, etc.

2.1.9 The institutions should establish standard practice to ensure that any impact to upstream, downstream, and cross-stream systems introduced by the change is adequately assessed and communicated to the stakeholders.

2.1.10 Regular incidents and knowledge sharing among the relevant teams and stakeholders are recommended.

2.2 Change Request Log and Review

2.2.1 The institutions should implement proper system(s) to implement the defined change management policy/standard/procedure. System(s) should be configured to control all the change requests with pre-defined criteria. Fields in the system(s) could be set as mandatory or optional as per the company's "documents" and external notification requirements.

2.2.2 The institutions could consider enhancing the overall change management process by using the automation to minimize the human intervention. For processes that could not be automated, based on the criticality and associated risks, continuous improvements to mitigate human error like training, scorecard tracking, etc. might be considered to align with institution's risk appetite, where necessary.

2.2.3 The institutions should ensure that there is complete inventory tracking of change cases or tickets including all the types of changes even including those emergency changes.

2.2.4 The institutions could consider the implementation of peer review including maker and check arrangements for high-risk activities in the change process.

2.2.5 The institutions with high volume of Change Requests could consider having higher frequency for Change Advisory Board (CAB) review meeting to allow for deployment flexibility / agility.

2.3 Change Assessment and Communication

2.3.1 Change Impact assessment should include all the data about scheduled downtime and impacted systems (upstream/downstream) to be reviewed by Change Advisory Board ("CAB") members to assess the proposed change and authorise the change planning. If required, higher levels of authority (e.g. IT management) are involved in the authorisation process, for instance, when the planned schedule is during the freeze period.

2.3.2 The institutions should ensure that the process of communication to relevant stakeholders (not limited to IT but including business and other functions as needed) is in place across various change types, where necessary.

2.4 Change Scheduling

2.4.1 The institutions could consider the appropriate change frequency planning to minimize the potential impact. The institutions could consider forward looking schedule planning to allow sufficient time for preparation and to lower chance of conflicting schedule.

2.4.2 The institutions should plan the change implementation calendar advisable to be outside the critical business periods or peak processing times to minimize risk and impact to business and customers.

2.5 Testing of Change

2.5.1 The institutions should establish Test Strategy standards that details testing methodology/framework as a standard practice for software releases to cover various change categories.

2.5.2 The institutions could consider comprehensive software test plan including regression test, system rollback [1], etc. with the stakeholders including business analysts, developers, technical leads, testers, etc.

2.5.3 Testing environment set up should mirror as close to production environments (in terms of configurations, interconnected systems, capacity, etc) to facilitate full end to end integration testing.

2.5.4 Testing environment should be updated timely after introduction of new functions or features of the software.

2.5.5 The institutions could perform post implementation verification testing to ascertain that implementation is successful. Duration for completion of post implementation review to be defined and all artefacts to be captured as evidence for record purpose to improve accuracy and facilitate timeliness of closure status reporting.

2.6 Changes Outside Singapore but Impacting Singapore

For the changes deployed outside of Singapore but support Singapore businesses or customers, based on the criticality of involved systems/services.

2.6.1 Necessary impact analysis could be done by the change manager, or global / local delegate, before the change. The institution could have the appropriate Singapore entity representative, or global / local delegate, to review the impact analysis as needed.

2.6.2 To enable the impact analysis, there could be a central repository containing change requests, associated document, change schedules, etc. This change repository should be easily accessible by the Singapore entity representative, or global / local delegate, as needed.

[1] System rollback plan is a recovery plan that aims at returning the system to its last known good state. It may be a tape restore or a reload of a configuration file. The rollback plan is the emergency escape plan to get the system back up before the prescribed amount of time elapses.

2.6.3 There could be a central change request review workflow, that enables the Singapore entity representative, or global / local delegate, to feedback / escalate, as needed, when there is material impact on Singapore businesses or customers.

2.7 Changes Related to Software Management

2.7.1 The institutions should ensure robust capacity planning and monitoring in place when developing or deploying the software. The institutions could consider building close-to-Production environments (in terms of configurations, interconnected systems, capacity, etc.) to verify capacity thresholds.

2.7.2 The institutions could have workflows-based build quality control such as code review, security code scanning, etc.

2.7.3 The organisations' cross-functional teams should be involved to review the performance readiness of changes planned.

2.8 Changes Related to Third Party Software or Hardware

2.8.1 The institutions could conduct the appropriate test of third-party software or hardware before onboarding or integrating them. Test results should be documented centrally and presented to the Change Advisory Board, or other appropriate committee, based on criticality of software or hardware for the institution's operation.

2.8.2 Stability monitoring on the third-party software or hardware should be in place both in production and back-up sites post onboarding or integration.

2.8.3 The institutions could establish the framework and implementable procedure to contractually obligate the third party to the Service Level Agreement ("SLA") and/or Performance Level Agreement ("PLA") if possible.

2.9 Changes Related to Security Vulnerability Management

For security vulnerability related to third-party products and open-source systems,

2.9.1 The institutions should prioritize the remediation based on the security vulnerabilities criticality and impact to the business.

2.9.2 The change requestor, or appropriate personnel, should provide necessary information about the vulnerability including test results and acceptance criteria for the vulnerability fixes aligning to security policy of the institution.

2.9.3 Institution could conduct adequate IT Security mitigation measures.

3. Acknowledgement

This advisory is developed by the IT incidents working group members from:

a) Financial Institutions
   1. DBS Bank Ltd (Working Group Lead)
   2. UBS AG (Working Group Lead)
   3. BNP Paribas
   4. Credit Suisse AG
   5. HSBC Bank (Singapore) Limited
   6. Maybank Singapore Limited
   7. MUFG Bank Ltd
   8. OCBC Bank
   9. SGX
   10. United Overseas Bank Limited

b) Insurance Institutions
   1. AIA Singapore
   2. Allianz Insurance Singapore
   3. Great Eastern Life Assurance
   4. MSIG Singapore
   5. Singlife

In addition, the paper was completed with the guidance and support of:

   1. ABS Standing Committee on Cyber Security (SCCS)
   2. Monetary Authority of Singapore (MAS)