**DETAIL REKOMENDASI HASIL *REVIEW***

|  |  |  |
| --- | --- | --- |
| **No** | **Kondisi, Dampak, dan Kriteria** | **Rekomendasi dan Tanggapan *Auditee*** |
| **1.** | ***Business Requirement Document* dan *System Design* Fitur *Frictionless Transaction with* VCAS via OCTO Mobile Belum Mencakup Seluruh *User Requirement***  **Kondisi**  Berdasarkan *review* dokumen *User Requirement* (UR) Frictionless Transaction with VCAS via Octo Mobile v1 diketahui pada bagian 4.3. *Integration Requirement* terdapat *requirement* untuk *setup* SFTP pada ITM untuk pengiriman *file* ke ALTO. Data *file* tersebut akan berisi informasi nomor kartu dan nomor *handphone*. File tersebut akan digunakan apabila dibutuhkan pengiriman SMS OTP, namun ESB tidak dapat diakses atau *time-out*. Akan tetapi, hal ini tidak tercantum pada *Business* *Requirement Document* (BRD) dan dokumen System Design (SD), serta belum masuk ke dalam pengembangan yang telah dilakukan. Tidak adanya informasi di dalam dokumen kebutuhan dan desain menyebabkan adanya *user requirement* yang tidak dikembangkan.  **Kriteria**  H.02.P.01.01 SOP IT *Project Development Life Cycle* Versi: 14.03.2024   * Poin 4.3.7 BRD adalah dokumentasi yang disusun oleh IT Business Analyst atau dikoordinasikan oleh PM (Infrastructure Technology) yang mencakup uraian terperinci untuk solusi *end-to-end* dari suatu sistem/ infrastruktur yang akan dibuat untuk memenuhi kebutuhan bisnis sesuai dengan *User Requirement* (UR) yang disusun oleh Business Project Manager untuk pengajuan Proyek dan *Change Request* (CR).   **Penyebab**  TBD | **Rekomendasi**  Tim Proyek agar menambahan requirement tersebut pada BRD dan SD, mengembangkan, serta melakukan pengujian atas *requirement* ini.  **Tanggapan *Auditee***  xxx (mohon untuk diisi)  **PIC**   * Process Improvement & System Control Head * Digital Channel Development Project, Strategy & Availability Head   ***Target Date* (Status)**  dd-mm-yy (*Open*) |
| **2.** | ***Business Requirement Document* (BRD) Belum Mencerminkan Kondisi Terkini Proyek**  **Kondisi**  Pada BRD *Frictionless Transaction with* VCAS via OCTO Mobile versi 1.6, terdapat empat poin *requirement* yang perlu dilengkapi atau disesuaikan dengan kondisi pengembangan terkini. Keempat poin tersebut perlu ditambahkan untuk memastikan informasi pada dokumen BRD sudah sesuai dengan sistem yang dikembangkan. Kondisi ini disebabkan karena adanya informasi terkait sistem yang baru diketahui atau ditentukan pada saat sistem dikembangkan. **Detail dapat dilihat pada Lampiran 1.**  Terdapat tujuh poin *requirement* yang belum tersedia pada BRD *Frictionless Transaction with* VCAS via OCTO Mobile versi 1.6. Ketujuh poin *requirement* tersebut saat ini sudah dikembangkan pada sistem yang dibangun, namun belum didokumentasikan pada BRD. Ketujuh poin *requirement* tersebut yaitu:  Aktivitas *sync* data nasabah kartu kredit apabila mengganti nomor *handphone* nasabah.  *Handling* apabila status transaksi *online merchant* dengan OOB adalah ‘*In Progress*’. Pada proses *existing*, nasabah perlu melakukan pengecekan sukses/tidak-nya transaksi melalui mutasi rekening secara berkala. Mengingat status transaksi pada *online merchant* hanya“*Success*” atau “*Failed*”, maka perlu di-*consider* agar transaksi digagalkan apabila status ‘*In Progress*’ sehingga tidak terdapat *dispute* antara Bank, *Merchant*, dan nasabah.  *Handling* apabila sistem internal Bank (ESB atau OCTO Mobile) mengalami *time-out* saat ALTO inisiasi pembuatan *push* notifikasi OOB ke ESB.  *Handling* apabila nasabah menutup atau *cancel* transaksi pada layar *merchant* saat *push* notifikasi sudah terkirim atau di-*approve* oleh nasabah.  *Handling* apabila nasabah NTB kartu kredit atau debit melakukan transaksi *eCommerce* namun informasi nomor *handphone* nasabah belum tersedia pada FTP *folder* untuk pengiriman OTP.  *Requirement* bahwa nasabah dapat menerima lebih dari satu OOB selama kriteria validasi *challenge* dengan OOB terpenuhi seluruhnya.  Pada subbab ‘3.3.3. Format Notifikasi’ belum terdapat format notifikasi untuk *push notification* verifikasi transaksi yang akan muncul pada *device* nasabah sesuai *requirement* 3.3.1. Saat ini format notifikasi yang disediakan hanya informasi transaksi sukses atau *failed* setelah verifikasi selesai dilakukan.  Informasi *requirement* yang tidak akurat dapat menyebabkan ketidaksesuaian desain sistem dan *deliverable* produk yang dibangun.  **Kriteria**  H.02 - Kebijakan Pengembangan Sistem TI versi 20.07.2023   * Poin 4.14 - Setiap pengembangan dan pengadaan sistem wajib memiliki dokumentasi *requirement* yang dibuat harus lengkap, jelas, dan merinci kebutuhan *input*, proses, dan *output* yang dibutuhkan. * Poin 5.1.1 - Dokumentasi kebutuhan harus didefinisikan dengan jelas dengan mencakup namun tidak terbatas pada *user* *requirement*, batasan, regulasi, infrastruktur dan keamanan informasi.   SOP H.02.P.01.01 - IT *Project Development Life Cycle* versi 14.03.2024   * Poin 4.3.7 - BRD adalah dokumentasi yang disusun oleh IT Business Analystatau dikoordinasikan oleh PM (*Infrastructure Technology*) yang mencakup uraian terperinci untuk solusi *end to end* dari suatu sistem/ infrastruktur yang akan dibuat untuk memenuhi kebutuhan bisnis sesuai dengan *User Requirement* (UR) yang disusun oleh *Business Project Manager* untuk pengajuan Proyek dan *Change Request* (CR). * Poin 4.3.13 - Dalam hal terjadi perubahan ruang lingkup, wajib dilakukan penyesuaian dokumen kebutuhan dan desain yang disetujui dan disosialisasikan ke pihak terkait.   **Penyebab**  Kurangnya *review* secara menyeluruh terhadap perkembangan dan dokumentasi proyek. | **Rekomendasi**  Agar tim proyek melakukan pengkinian BRD sesuai kondisi yang ditemukan dan memastikan *addendum* BRD telah mendapatkan *approval* dari seluruh PIC yang terkait.  **Tanggapan *Auditee***  xxx (mohon untuk diisi)  **PIC**  Digital Channel Development Project, Strategy & Availability Head  ***Target Date (Status)***  dd-mm-yy (*Open*) |
| **3.** | **Belum Dilakukan Finalisasi Hasil *Pre-Assessment* Produk Bank Baru, Hasil Analisa Risiko Materialitas Produk, dan Kertas Kerja *Self-Assessment* Bank Indonesia**  **Kondisi**  Sampai dengan Maret 2025 (fase UAT dengan kartu tipe Mastercard), tim proyek *Frictionless Transcation with* VCAS via OCTO Mobile belum melakukan finalisasi atas:   1. *Pre-Assessment Form* Produk Bank Baru   Tim proyek belum melakukan analisa *pre-assessment form* produk bank baru untuk memastikan produk yang diajukan memenuhi definisi sebagai produk bank baru atau tidak. Informasi tersebut dibutuhkan untuk menentukan pembuatan *New Product Assessment* (NPA) atau *Significant Changes Assessment Process* (SCAP). Hal ini sudah disampaikan saat *meeting* November 2024 oleh ORM, namun belum selesai ditindaklanjuti tim proyek sampai dengan 21 Maret 2025.  Kondisi ini mengakibatkan proyek *Frictionless Transaction with VCAS via* OCTO Mobile belum dapat diidentifikasi sebagai produk bank dasar/lanjutan baru atau bukan produk baru, serta belum diputuskan untuk dibuat NPA atau SCAP. Belum adanya NPA atau SCAP menyebabkan adanya potensi risiko yang tidak teridentifikasi karena pengembangan belum di-*assess* oleh *mandatory reviewer* atau SME terkait.   1. Hasil Analisa Risiko Materialitas Produk dan Kertas Kerja *Self-Assessment* Bank Indonesia   Tim proyek telah melakukan *self-assessment* analisa risiko materialitas produk dengan hasil ‘*Low to Moderate*’ dan kertas kerja *self-assessment* BI dengan hasil ‘*High*’. Hasil *self-assessment* awal telah dikirimkan kepada seluruh *mandatory reviewer* pada 4 Desember 2024, akan tetapi sampai dengan 21 Maret 2025 belum di-*follow up* lebih lanjut karena terdapat perubahan pada inisiatif yang diajukan. Kondisi ini mengakibatkan belum dapat dipastikan tingkat materialitas risiko proyek dan apakah diperlukan perijinan ke regulator*.*  **Kriteria**  B.04.06 - Kebijakan Produk dan Aktivitas Baru versi Agustus 2019   * Poin 5.1.1 - *Product*/*Activity* *Owner* wajib melakukan analisa (*assessment*) untuk memastikan apakah produk/aktivitas yang diajukan adalah baru sesuai dengan definisi Produk/Aktivitas Baru.   E.01.K01 - Kebijakan Manajemen Proyek dan CAPEX Rutin versi 12.2018   * Poin 3.3.3 - PO/PM bertanggung jawab atas pembuatan pelaporan, permohonan persetujuan dan/atau laporan realisasi ke pihak regulator dengan persetujuan Direksi terkait dan disampaikan secara benar, lengkap dan tepat waktu.   **Penyebab**  *To be confirmed* with Tim Proyek | **Rekomendasi**  Tim proyek agar:   1. Melakukan analisa *Pre-Assessment Form* Produk Bank Baru dan mendistribusikan hasil analisa tersebut kepada pihak *reviewer* terkait sampai mendapatkan *final feedback/approval*. 2. Menindaklanjuti *feedback* dari unit kerja Compliance dan ORM, mendistribusikan kembali Hasil Analisa Risiko Materialitas Produk dan Kertas Kerja *Self-Assessment* Bank Indonesia yang sudah disesuaikan kepada seluruh *mandatory reviewer* untuk mendapatkan dan menindaklanjuti poin-poin tambahannya.   **Tanggapan Auditee**   1. [Respon tanggapan] 2. [Respon tanggapan]   **PIC**  Process Improvement & System Control Head  **Target Date (Status)**   1. dd-mm-yy (*Open*) 2. dd-mm-yy (*Open*) |
| **4.** | **Belum dilakukan *Review* Kecukupan *Legal Documents* Bank dengan PT ALTO Network Terkait Penggunaan VISA *Customer Authentication Service* (VCAS) yang Disediakan oleh VISA.**  **Kondisi**  Tim proyek belum melakukan *review* untuk memastikan apakah *legal documents* Bank dengan PT ALTO Network telah mencakup skema kerja sama antara Bank, PT ALTO Network dan VISA. Kedua vendor tersebut mengintegrasikan solusi SaaS dengan fungsionalitas yang berbeda. Adapun keterlibatan masing – masing vendor dalam proyek *Frictionless* VCAS via OCTO Mobile adalah sebagai berikut.   * PT ALTO Network sebagai penyedia layanan ALTO *Online Secure* (AOS) berbasis *Software-as-a-Service* (SaaS) untuk memfasilitasi metode otentikasi transaksi *online* (*challenge*) via *one-time password* (OTP) dan *out-of-band* (OOB). * VISA sebagai penyedia *engine* VCAS berbasis SaaS yang akan memproses data transaksi *online* untuk memperoleh *risk score* sebagai penentu metode otentikasi transaksi (*auto-approve/frictionless*, *challenge* atau *reject*). Pemrosesan tersebut akan dilakukan berdasarkan kombinasi antara *risk score* yang dihasilkan VISA serta parameter lain yang ditetapkan oleh Bank*.* Dalam hal ini, *connection* antara VISA dan Bank akan melalui jaringan ALTO.   Saat ini, Bank telah memiliki *legal document* dengan PT ALTO Network berupa *Master Agreement*, *Work Order Document* (WOD) dan *Non-Disclosure Agreement* (NDA) *Company*. Akan tetapi, Tim Proyek belum melakukan *review* untuk memastikan apakah *legal document* yang ada telah mencakup skema kerja sama antara Bank, PT ALTO Network dan VISA dalam proyek *Frictionless* VCAS via OCTO Mobile. Selain itu, belum terdapat klausa jaminan atas keamanan pemrosesan data dari VISA, ketersediaan dan keandalan layanan serta kewajiban hukum jika Bank mengalami kerugian akibat layanan yang disediakan oleh PT ALTO Network maupun VISA.  Kondisi ini dapat berdampak pada lemahnya posisi Bank secara hukum apabila terjadi insiden operasional ataupun kebocoran data yang disebabkan oleh VISA.  **Kriteria**  E.03.01 – Kebijakan Pengadaan Barang dan Jasa Versi 2023   * Poin 6.1. - Layanan yang diberikan oleh Vendor harus didokumentasikan dengan tepat melalui perjanjian, di mana peran dan tanggung jawab yang ditetapkan untuk Vendor harus sesuai dengan standar bisnis Bank dan sesuai dengan persyaratan hukum dan peraturan yang berlaku. Perjanjian adalah kesepakatan antara Bank dan Vendor mengenai hal tertentu/ kerjasama/ pengadaan dalam waktu tertentu dengan nilai tertentu yang disetujui bersama sebagai para pihak dan dituangkan secara tertulis. Bentuk-bentuk kesepakatan secara tertulis yang dipergunakan antara lain:  1. Perjanjian Kerjasama/*Master Agreement* (PKS) 2. *Work Order Document* (WOD) 3. *Confidentiality Agreement*/*Non Disclosure Agreement* (NDA) 4. *Addendum* 5. *Novation Deed* 6. Surat Perjanjian Kerja (SPK) 7. Surat Pemesanan Pembelian (SPP)/*Purchase Order* (PO)  * Poin 6.2.3. - Template Perjanjian Kerjasama (PKS)/ *Master Agreement* harus di-*review* oleh bagian Legal sesuai pembagian kewenangan sebagaimana diatur dalam Kebijakan Hukum.   E.03.01.P.02 – SOP Manajemen Pihak Ketiga Versi 07.2021   * Poin 2.5. - Perubahan Ruang Lingkup Kerjasama Pihak Ketiga   Untuk perubahan ruang lingkup kerjasama pihak ketiga yang telah berjalan, mengacu pada Lampiran 2: Matriks Tata Kelola Pihak Ketiga, BU/SU melengkapi dokumen pendukung untuk mendapatkan opini dan konfirmasi dari *reviewer* dan/atau pihak yang terkait dan mendapatkan persetujuan dari pemegang otoritas pemberi persetujuan kerjasama pihak ketiga jika diperlukan.  **Penyebab**  Kurangnya *review dan assessment* atas kecukupan dan kelengkapan dokumen perjanjianoleh tim Legal sebagai *Subject Matter Expert.* | **Rekomendasi**  Tim proyek agar berkoordinasi dengan tim Legal untuk melakukan *review* kecukupan *legal documents* dalam mendukung kerja sama antara Bank, PT ALTO Network dan VISA antara lain, namun tidak terbatas pada:   * Apakah *legal documents* Bank dan PT ALTO Network memiliki kekuatan hukum atas penggunaan *engine* VCAS oleh Bank. * Apakah *legal documents* Bank dan PT ALTO Network dapat digunakan sebagai basis pemberian jaminan pengamanan pemrosesan data, ketersediaan layanan, dan keandalan layanan yang disediakan oleh VISA. * Apakah *legal documents* Bank dan PT ALTO Network dapat digunakan sebagai basis *legal action* kepada PT ALTO Network dan VISA jika di kemudian hari terdapat kerugian yang disebabkan kegagalan pengamanan pemrosesan data, ketidaktersediaan layanan, dan ketidakandalan layanan yang disediakan oleh PT ALTO Network dan VISA. * Apakah diperlukan penyusunan *legal documents* lainnya antara Bank dengan VISA sebagai basis penjaminan atas keamanan pemrosesan data, ketersediaan layanan, dan keandalan layanan yang disediakan oleh VISA.   **Tanggapan *Auditee***  <Mohon diberikan tanggapan>  **PIC**  Process Improvement & System Control  ***Target Date* (Status)**  dd-mm-yy (*Open*) |
| **5.** | **Belum Dilakukan *Assessment* Validitas *Master Service Agreement* (MSA) dan *Work Order Document* (WOD) Antara Bank dengan PT ALTO Network untuk Proyek *Frictionless* VCASvia OCTO Mobile**  **Kondisi**  Belum terdapat *assessment* untuk memastikan kesesuaian ruang lingkup proyek *Frictionless* VCAS via OCTO Mobile dengan isi dari MSA dan WOD antara Bank dengan PT ALTO Network.  Proyek *Frictionless* VCAS via OCTO Mobile saat ini didukung oleh:  MSA No. F.094/CM/13062024 tanggal 21 Juni 2024: *Master agreement* antara Bank dan PT ALTO Network untuk penyediaan jasa sesuai WOD.  WOD No. 049/WOD/PISyC/VIII/2024 tanggal 7 Februari 2024: menggambarkan ruang lingkup penyediaan AOS-VCAS berbasis *Software-as-a-Service* (SaaS).  Akan tetapi, terdapat pasal pada MSA yang tidak relevan dengan solusi SaaS yang menjadi ruang lingkup proyek ini antara lain namun tidak terbatas pada:   |  | | --- | | Kepemilikan HAKI Atas *Deliverables*  8.4 Semua HAKI atas *deliverables* adalah kepunyaan dan milik Bank untuk dipergunakan secara terus menerus dan bersifat eksklusif. Vendor dengan ini telah mengalihkan HAKI atas *deliverables* kepada Bank. Dengan perjanjian ini vendor juga telah memastikan bahwa seluruh HAKI pihak ketiga yang terkait dengan *deliverables* telah dialihkan sepenuhnya kepada Bank. |   Pasal tersebut menjadi tidak relevan karena solusi yang disediakan vendor adalah berupa SaaS, dimana kepemilikan solusi SaaS tetap dimiliki oleh Vendor.  Ketidaksesuaian isi dokumen perjanjian kerja sama yang dapat menyebabkan *dispute* antara Bank dengan vendor penyedia jasa.  **Kriteria**  H.09 – Kebijakan Pengelolaan Penyedia Jasa TI Versi 15.09.2023   * Poin 4.6. - Rincian isi perjanjian harus sesuai dengan ruang lingkup pekerjaan. Tim proyek dan/atau unit kerja pengguna berkoordinasi dengan unit kerja yang bertanggung jawab atas pengelolaan kontrak TI dan unit kerja terkait termasuk Satuan Kerja Manajemen Risiko Hukum (SKMRH) melakukan *review* atas isi perjanjian.   **Penyebab**  Kurangnya *review dan assessment* atas validitas dokumen perjanjianoleh tim Legal sebagai *Subject Matter Expert.* | **Rekomendasi**   * Tim Proyek agar berkoordinasi dengan tim Legal untuk melakukan *review* atas keseluruhan informasi yang terdapat pada dokumen MSA antara Bank dengan PT ALTO Network. * Atas *review* MSA antara Bank dengan PT ALTO Network, agar tim proyek berkoordinasi dengan tim Legal untuk melakukan *review* dan *assessment* terkait kebutuhan penambahan poin dalam WOD yang menjelaskan bahwa terdapat pengecualian klausul MSA karena tidak dapat diterapkan pada jenis solusi SaaS.   **Tanggapan *Auditee***  <Mohon diberikan tanggapan>  **PIC**  Process Improvement & System Control  ***Target Date* (Status)**  dd-mm-yy (*Open*) |
| **6.** | **Perlu Dilakukan Penyesuaian Informasi pada Dokumen *System Design* (SD) Proyek *Frictionless Transaction with VCAS via OCTO Mobile***  **Kondisi**  Perlu dilakukan penyesuaian informasi yang ada di dalam dokumen SD aplikasi.   1. OCTO Mobile (SD *Frictionless Transaction with* VCAS via OCTO Mobile, 2025 versi 1.0)   Terdapat empat poin pada dokumentasi desain sistem yang perlu disesuaikan berdasarkan kondisi terkini.   |  |  |  | | --- | --- | --- | | **No** | **Subbab** | **Keterangan** | | 1. | 2.2 *Validate Push Notification Status* | Ketidaksesuaian informasi aplikasi yang men-*trigger* pengecekan kriteria OOB/OTP pada *System Design*. Pada *flow* SD, pengecekan di-*trigger* oleh *front-end* aplikasi OCTO Mobile, seharusnya dilakukan oleh ESB. | | 2. | 2.3 *Detail Confirmation* | Terdapat kesalahan penulisan alternatif *flow* setelah aktivitas ‘*validate detail customer with confirmationId is expired*’. *Flow* tersebut ditulis untuk kondisi ‘*when confirmation id not same with request’*, seharusnya ‘*when confirmation id is expired*’. | | 3. | 2.4 A*pprove Confirmation*  2.5 *Reject Confirmation* | Belum terdapat dokumentasi *flow* proses ke *front-end* setelah OCTO Mobile menerima *update callback status & response*’ dari ESB terkait sukses atau tidaknya transaksi. | | 4. | 2.5 *Reject Confirmation* | Terdapat kesalahan informasi pada *flow process* aktivitas *reject confirmation.* Pada SD, terdapat *flow* untuk *input* mPIN OCTO Mobile, seharusnya nasabah tidak perlu melakukan *input* mPIN untuk menolak konfirmasi. |  1. ESB (SD *Transaction with* VCAS via OCTO Mobile, November 2024 versi 1.0)   Terdapat lima poin pada dokumentasi desain sistem yang perlu disesuaikan berdasarkan kondisi terkini.   |  |  |  | | --- | --- | --- | | **No** | **Subbab** | **Keterangan** | | 1. | 2.1 *Design* OOB *Validation* – VCAS 1.0.2  2.2 *Design* OOB *Confirmation* – VCAS 1.0.1 | Terdapat dua *service* ESB yang merupakan orkestrasi atau *multi provider*, namun pada SD diidentifikasi bukan merupakan *service* dengan orkestrasi. | | 2. | 2.1 *Design* OOB *Validation* – VCAS 1.0.2 | Terdapat ketidaklengkapan informasi pada *flow chart* untuk kondisi ‘*if card\_type not null*’ dimana setelah *flow* ‘*Call ITM atomic DebitCardInfo* 2.0’ seharusnya dilanjutkanke *process* ‘*Call Octo Mobile atomic MFAPushNotification* 2.0’. | | 3. | Terdapat ketidaklengkapan informasi pada *flow chart* untuk kondisi ‘*if card\_type = null*’ dimana setelah pengecekan ‘*status code 5F?*’ seharusnya terdapat *flow* validasi:   * apabila status sukses (00) = ‘*Yes*’ maka dilanjutkan ke ‘*Call Octo Mobile atomic MFAPushNotification* 2.0’ * apabila status ‘*other*’ maka dilanjutkan ke ‘*Send response to channel*’ untuk memunculkan *error respond*. | | 4. | 2.2 *Design* OOB *Confirmation* – VCAS 1.0.1 | Terdapat ketidaklengkapan informasi pada *flow chart* untuk kondisi ‘*if card\_type not null*’ dimana setelah *flow* ‘*Call ITM atomic DebitCardInfo 2.0*’ seharusnya dilanjutkan ke *flow* ‘*Call Octo Mobile atomic GenerateConfirmation* 2.0’. | | 5. | Terdapat ketidaklengkapan informasi pada *flow chart* untuk kondisi ‘*if card\_type = null*’ dimana setelah pengecekan ‘*status code 5F?*’ seharusnya terdapat *flow* validasi:   * apabila status sukses (00) = ‘*Yes*’ maka dilanjutkan ke ‘*Call Octo Mobile atomic GenerateConfirmation* 2.0’ * apabila status ‘*other*’ maka dilanjutkan ke ‘*Send response to channel*’ untuk memunculkan *error respond*. |  1. ASCCEND (SD *Frictionless Transaction with* VCAS via OCTO Mobile, Oktober 2024 versi 1.1)   Terdapat informasi pada dokumen *System Design* ASCCEND yang perlu disesuaikan karena adanya perubahan rencana pengembangan.  Sebelumnya, tim *developer* ASCCEND berencanauntuk membuat *file online* baru CMBOLSH2L (*batch file* CMBOLSHP) sebagai pengganti *existing file* SCMOLSH2L (*batch file* SCMOLSHP). *File* tersebut digunakan oleh program CMBES08S untuk *inquiry* data nasabah.  Atas rencana tersebut, tim *developer* menggunakan *batch file* CMBOLSH2L saat penyusunan SD *frictionless transaction with* VCAS via OCTO Mobile. Saat sistem dikembangkan, pembuatan file CMBOLSH2L tidak jadi diimplementasi sehingga tim *developer* kembali menggunakan *file existing* SCMOLSH2L. Hal ini menyebabkan informasi pada SD tidak sesuai dengan kondisi terkini.    Informasi desain sistem yang belum didokumentasikan atau tidak sesuai berisiko terdapat *requirement* yang tidak tercakup dalam fase pengujian, fungsi aplikasi tidak berjalan atau tidak sesuai dengan kebutuhan *user*, dan adanya komplain nasabah.  **Kriteria**  H.02.P.01.01 - SOP IT *Project Development Life Cycle* Versi: 14.03.2024.   * 4.3.10 Dokumen desain yang dibuat wajib mencakup seluruh poin-poin kebutuhan yang tertuang dalam dokumen kebutuhan.   **Penyebab**   * Terdapat *requirement* yang belum diidentifikasi pada saat pembuatan BRD sehingga tidak ter-*capture* pada dokumen *System Design*. * Terdapat perubahan kondisi pada saat pengembangan sistem dilakukan yang belum direfleksikan pada dokumen *System Design*. | **Rekomendasi**  Agar *developer* aplikasi melakukan penyesuaian informasi pada dokumen *System Design* sesuai kondisi pengembangan yang dilakukan serta memastikan perubahan telah diketahui dan disetujui oleh pihakterkait.  **Tanggapan Auditee**   1. <<Mohon diberikan tanggapan>> 2. <<Mohon diberikan tanggapan>> 3. <<Mohon diberikan tanggapan>>   **PIC**   1. Gilang Kusuma Jati, Application DevOps Head - Mobile & Internet Banking 2. Yunita Kusuma Dewi, Enterprise Gateway Apps Head 3. Ferry Parlindungan, Application Development Head - Credit Card Products   **Target Date**   1. dd-mm-yyyy (*Open*) 2. dd-mm-yyyy (*Open*) 3. dd-mm-yyyy (*Open*) |
| **7.** | **Pengiriman Data Yang Tidak Diperlukan Dari ITM ke ESB**  **Kondisi**  Terdapat data nasabah yang dikirimkan dari ITM ke ESB, namun data tersebut tidak digunakan atau diperlukan. *Service ‘*DebitCardInfo2.0’ yang digunakan dalam proses *OOBValidation* dan *OOBConfirmation* mengirimkan data CIF, *phone number*, *short name*, *card type description*, dan *card expired date* dari ITM ke ESB. Dari keseluruhan data yang dikirimkan, informasi mengenai tanggal kedaluwarsa kartu tidak diperlukan karena ESB telah memperoleh data tersebut dari ALTO. Hal ini tidak sejalan dengan prinsip *need-to-know* dalam pemberian data di lingkungan internal Bank, serta dapat meningkatkan jumlah *data point* yang berisiko terekspos secara tidak perlu apabila terjadi insiden keamanan yang melibatkan ITM atau ESB.  **Kriteria**  E.01.K.02 - Kebijakan Manajemen Data Versi. 03.2025   * 8.3.3.1 Ketentuan Pembagian atau Pemberian Data   + Pembagian Pembagian atau Pemberian Data, baik di lingkup internal Bank maupun kepada pihak di luar Bank wajib mengikuti ketentuan keamanan Data yang diatur pada Kebijakan Keamanan Informasi sesuai klasifikasinya dan dilaksanakan berdasarkan     - Prinsip *need-to-know basis*;     - Prinsip pembagian tugas, wewenang, dan fungsi; dan     - Tidak melanggar Undang-Undang dan Peraturan yang berlaku.   H.02.P.01.01 - SOP IT *Project Development Life Cycle* Versi: 14.03.2024.   * 4.3.10 Dokumen desain yang dibuat wajib mencakup seluruh poin-poin kebutuhan yang tertuang dalam dokumen kebutuhan.   **Penyebab**  Tidak teridentifikasinya *data point* yang sebenarnya telah tersedia pada sistem lain saat proses desain sistem. | **Rekomendasi**  Agar *developer* aplikasi ITM melakukan evaluasi dan penyesuaian pada desain sistem terkait pengiriman data *card expired date* yang tidak digunakan dari ITM ke ESB.  **Tanggapan Auditee**  <<Mohon diberikan tanggapan>>  **PIC**  Afandi Ahmad, Application Development Head - Middleware  **Target Date**  <<Mohon diberikan tanggapan>> |
| **9.** | **Fungsi *Issuer Rules Set* pada Layanan VISA *Consumer Authentication System* (VCAS) Belum Diuji Secara Menyeluruh**  **Kondisi**  Tim proyek belum melakukan pengujian atas kesesuaian antara parameter *issuer rules set* VCAS yang di-*setting* dengan hasilnya secara menyeluruh. Pengujian dilakukan untuk memastikan *engine* VCAS mampu menentukan metode otentikasi dengan *auto-approve*, *auto-reject*, ataupun *challenge* (OOB/OTP) telah sesuai dengan parameter yang di-*setting*. Tim proyek saat ini baru menguji parameter terkait nominal transaksi dan nomor kartu spesifik yang didaftarkan (*plain vanilla*). Tim proyek perlu memastikan parameter berfungsi dengan baik untuk untuk kondisi lainnya. Apabila parameter lain tidak dilakukan pengujian, maka berpotensi adanya kelemahan sistem vendor yang tidak teridentifikasi lebih awal.  **Kriteria**  H.02. – Kebijakan Pengembangan Sistem TI Versi: 04.2025   * Poin 5.4.17. Pengujian harus dilakukan untuk memastikan fungsionalitas, desain dan keandalan seluruh sistem aplikasi sesuai dengan kebutuhan yang telah disetujui oleh pengguna;   **Penyebab**  Belum terdapat prosedur spesifik yang mengatur terkait pengujian atas servis SaaS yang digunakan oleh internal Bank. | **Rekomendasi**  Agar tim PISC melakukan pengujian atas kesesuaian setting parameter dengan hasil issuer rules set pada lingkungan UAT VISA dan mendokumentasikan hasilnya.  **Tanggapan *Auditee***  <Mohon diberikan tanggapan>  **PIC**  Process Improvement & System Control Head dan Digital Channel Development Project Head - Growth & Ecosystem  ***Target Date (Status)***  dd-mm-yy (mohon untuk diisi) (*Open*) |
| **10.** | **Belum Dilakukan Pengujian atas Kartu Debit dan Kredit *Principal* selain VISA dan Skenario Pengujian Terkait Fungsional VCAS Perlu Ditambahkan**  **Kondisi**   1. Pengujian untuk memastikan fungsionalitas kontrol layanan “*Frictionless Transaction with* VCAS via OCTO Mobile” untuk tipe kartu debit dan kartu kredit dari *principal* selain VISA belum dilakukan. Saat ini tim proyek telah melakukan pengujian SIT maupun UAT namun hanya menggunakan tipe kartu kredit dari *principal* VISA. Kondisi ini berpotensi menyebabkan adanya kelemahan fitur yang tidak teridentifikasi untuk pengembangan yang dilakukan pada produk kartu debit ataupun kartu kredit dari *principal* lainnya. 2. Skenario pengujian untuk memastikan kontrol tetap berjalan dalam kondisi alur atau proses yang tidak wajar sudah tersedia namun perlu ditambahkan tiga skenario lainnya, yaitu:  * Nasabah mengubah nomor *handphone* via OMO, kemudian melakukan transaksi *online* menggunakan kartu kredit untuk memastikan nasabah dapat tetap bertransaksi atau tidak dalam kondisi tersebut. * Nasabah mengakses OOB melalu menu OMO, tidak melalui *push notification* untuk memastikan OOB dapat diakses secara langsung di menu sesuai BRD*.* * Nasabah menggunakan satu kartu yang sama untuk melakukan lebih dari satu transaksi *online* dan keduanya membutuhkan metode otentikasi OOB via OMO*.*   **Kriteria**  H.02.P.01.01 – SOP IT *Project Development Life Cycle* Versi: 14.03.2024   * Poin 4.3.19. *Test Script* yang dibuat harus mencakup seluruh poin-poin kebutuhan, seperti yang tertuang pada dokumen kebutuhan, dokumen desain, maupun dokumen lainnya, serta memiliki skenario pengujian abnormal (*negative test*).   **Penyebab**   * TBC with Auditee * *Review* terhadap kebutuhan skenario pengujian belum dilakukan secara menyeluruh, khususnya terkait dengan pengujian atas *requirement* yang berubah atau bertambah seiring perkembangan lingkup proyek. | **Rekomendasi**   1. Agar tim PISC dan Digital Channel Development Project melakukan pengujian untuk tipe kartu debit dan kredit dari *principal* selain VISA. 2. Agar melakukan penambahan skenario pengujian, minimum sesuai dengan rekomendasi, untuk memastikan pengujian telah mencakup kondisi alur atau proses yang tidak wajar.   **Tanggapan *Auditee***  <Mohon diberikan tanggapan>  **PIC**   1. Process Improvement & System Control Head dan Digital Channel Development Project Head - Growth & Ecosystem 2. Gilang Kusuma Jati, Application DevOps Head - Mobile & Internet Banking   ***Target Date (Status)***   1. dd-mm-yy (mohon untuk diisi) (*Open*) 2. dd-mm-yy (mohon untuk diisi) (*Open*) |
| **11.** | **Dokumentasi UAT Perlu Dilengkapi atau Diperbaiki**  **Kondisi**  Terdapat lima dokumentasi hasil pengujian UAT yang belum menjawab tujuan dari skenario pengujian yang ditentukan. Dalam hal ini, hasil pengujian disajikan secara tidak lengkap sehingga belum dapat memberikan konklusi apakah pengujian telah dilakukan secara memadai, sebagai berikut.   |  |  |  | | --- | --- | --- | | **No** | **Test Script UAT** | **Keterangan** | | 1. | TS\_*NEG*\_*PASS*-210\_*Frictionless Transaction with* VCAS *via* OCTO Mobile\_Android\_1.1 | Dokumentasi telah menunjukkan *screenshot* adanya menu *input* OTP, namun tidak menunjukkan bukti bahwa nomor *handphone* tidak terdaftar sebagai pengguna OMO dan metode otentikasi harus melalui OTP. | | 2. | TS\_*NEG\_PASS*-210\_*Frictionless Transaction* *with* VCAS *via* OCTO Mobile\_IOS\_1.1 | | 3. | TS\_*NEG*\_*PASS*-210\_*Frictionless Transaction with* VCAS *via* OCTO Mobile\_Android\_1.2 | Dokumentasi belum menunjukkan *screenshot* adanya menu *input* OTP, dan tidak menunjukkan bahwa otentikasi transaksi perlu melalui OTP. | | 4. | TS\_NEG\_PASS-210\_*Frictionless* *Transaction* *with* VCAS via OCTO Mobile\_Android\_1.9, | Dokumentasi belum menunjukkan bahwa transaksi gagal karena *timeout* ESB. | | 5. | TS\_*NEG*\_*PASS* -210\_*Frictionless* *Transaction* *with* VCAS *via* OCTO Mobile\_IOS\_1.10 |   **Kriteria**  H.02.P.01.01 – SOP IT *Project Development Life Cycle* Versi: 14.03.2024   * Poin 4.1.28.   Setiap skenario yang teridentifikasi tidak dapat dilakukan pengujian dan diluar dari kontrol Bank perlu dideklarasikan/didokumentasikan.  Pendeklarasian/pendokumentasian dapat berupa:   1. Dokumen (misal sebagai bagian/lampiran dari Berita Acara UAT) yang disetujui oleh *Business Project Manager*, *Business/Project Owner*, dan TPM (D-2) jika diperlukan. 2. Memo atau MoM persetujuan dari PSC.  * Poin 4.1.29.   Pendokumentasian sebagaimana yang dimaksud pada butir 28 di atas memuat hal-hal berikut ini:   1. Deskripsi dari skenario yang tidak dapat diuji. 2. Penjelasan detail mengenai alasan mengapa skenario tersebut tidak dapat diuji. 3. Risiko yang dapat terjadi dengan tidak dapat diujinya skenario tersebut. 4. *Mitigating control* yang dapat dilakukan untuk menutup/mengurangi risiko tersebut (jika ada). 5. Tindak lanjut (misal jika diperlukan pengembangan sistem/aplikasi, tetap akan dilakukan pengujian pada lingkungan produksi, atau akan diterbitkan CIM serta target penyelesaian). 6. Lampiran MoM pembahasan (jika ada).  * Poin 4.3.19.   *Test Script* yang dibuat harus mencakup seluruh poin-poin kebutuhan, seperti yang tertuang pada dokumen kebutuhan, dokumen desain, maupun dokumen lainnya, serta memiliki skenario pengujian abnormal (*negative test*).  **Penyebab**  *Review* terhadap dokumentasi pengujian belum dilakukan dengan menyeluruh, untuk memastikan hasil pengujian disajikan secara lengkap dan memadai. | **Rekomendasi**  Agar melakukan perbaikan dokumentasi hasil pengujian, minimum sesuai dengan rekomendasi, untuk memastikan pengujian kelengkapan dan akurasi dari hasil pengujian yang ada.  **Tanggapan *Auditee***  <Mohon diberikan tanggapan>  **PIC**  Gilang Kusuma Jati, Application DevOps Head - Mobile & Internet Banking  ***Target Date (Status)***  dd-mm-yy (mohon untuk diisi) (*Open*) |
| **12.** | **Informasi pada *Frequent Asked Question* (FAQ) Perlu Dilengkapi**  **Kondisi**  Tim proyek sudah memiliki FAQ terkait transaksi *E-Commerce* tanpa OTP menggunakan Kartu Kredit Mastercard, namun belum dikinikan dengan rencana penerapan *frictionless transaction* menggunakan VCAS dan MFA pada OMO. Ketidaklengkapan atau ketidaksesuaian informasi pada FAQ dapat mengakibatkan *user experience* yang kurang baik karena Bank tidak memberikan informasi yang jelas kepada nasabah terkait layanan yang diberikan.  Beberapa contoh informasi yang perlu dikinikan pada FAQ, sebagai berikut.   1. Pada pertanyaan pertama terkait mengapa nasabah tidak menerima OTP, belum terdapat opsi jawaban sesuai pengembangan yang dilakukan. Jawaban pada FAQ saat ini hanya mencakup transaksi *auto-approve*, sedangkan terdapat kemungkinan nasabah menerima *push notification*/MFA untuk otorisasi transaksi, serta kondisi adanya gangguan/*time out* pada sistem internal Bank. 2. Pada pertanyaan ketiga terkait apakah seluruh transaksi *online* nasabah tidak akan menerima OTP kedepannya, belum terdapat penjelasan terkait opsi metode otentikasi lainnya menggunakan OOB/MFA melalui OMO. Jawaban pada FAQ saat ini hanya menjelaskan OTP sebagai salah satu metode otentikasi.   Selain ketiga penyesuaian di atas, terdapat enam rekomendasi kondisi yang perlu untuk ditambahkan menjadi pertanyaan pada FAQ sehingga Bank dapat memberikan informasi yang jelas kepada nasabah terkait dengan servis yang diberikan. Adapun rekomendasi yang diberikan tidak terbatas pada:   1. Nasabah tidak menerima OTP dengan kondisi no HP belum dilakukan batching ke FTP. 2. Nasabah tidak melakukan transaksi tetapi mendapat informasi/notifikasi transaksi berhasil/sukses. 3. Transaksi yang direject sebelum dapat menginput OTP/OOB (dimana kondisi transaksi auto reject atas engine yang dilakukan oleh VCAS). 4. Nasabah menanyakan agar proses otentikasi yang dilakukan dengan metode *frictionless*. 5. Kondisi transaksi yang tidak konsisten dalam memberikan metode otentikasi pada beberapa transaksi yang telah dilakukan (*frictionless*/OTP/OOB). 6. Kondisi Nasabah mengabaikan/menonaktifkan *push notification* pada *device* nasabah dan tetap ingin melanjutkan transaksi yang sedang dilakukan.   **Kriteria**  E.04.C.00.P.51 – SOP OCTO Mobile versi 17.08.2024   * Poin 2.6.5: “Unit kerja Mobile Banking Business Development, Customer Service dan Contact Center Officer wajib memberikan edukasi kepada Nasabah pengguna layanan OCTO Mobile tentang risiko-risiko Layanan OCTO Mobile dan cara-cara memitigasinya.” * Poin 3.6.3: “Membuat dan memperbarui dari waktu ke waktu user manual layanan OCTO Mobile serta mendistribusikan dan mensosialisasikannya sesuai ketentuan.” * Poin 3.7.2: “Membuat dan mengeksekusi program-program edukasi layanan OCTO Mobile dengan mengajukan persetujuan sesuai DOA.”   H.02 - Kebijakan Pengembangan Sistem TI versi 15.06.2020   * Poin 5.5.3: "Untuk aplikasi yang dikembangkan oleh penyedia jasa, senior manajemen dan Project Manager harus memastikan bahwa pelatihan dan/atau pendampingan yang cukup dan dokumentasi manual telah tersedia sebagai bagian dari paket pengembangan sistem serta dapat dipahami dengan jelas oleh semua pihak terkait;" * Poin 5.5.10: "Unit kerja yang terkena dampak deployment suatu perubahan harus diidentifikasi sebelum implementasi. Selanjutnya, unit kerja tersebut diberikan informasi dan/atau pelatihan terkait solusi baru yang diakibatkan oleh perubahan sistem;"   **Penyebab**  Kurangnya *review* secara menyeluruh terhadap perkembangan dan dokumentasi layanan pihak ketiga. | **Rekomendasi**   * Melakukan pengkinian dan *update* pada dokumen FAQ untuk memastikan semua informasi terkait dengan layanan yang diberikan kepada nasabah dapat informasikan dengan tepat. * Melakukan sirkulasi dokumen FAQ ke unit terkait untuk memastikan kecukupan atas informasi yang terdapat pada FAQ telah tersedia.     **Tanggapan *Auditee***  (mohon untuk diisi)  **PIC**  Process Improvement & System Control  ***Target Date (Status)***  dd-mm-yy (mohon untuk diisi) (*Open*) |

**Lampiran 1 – Detail *Requirement* BRD yang Tidak Sesuai Dengan Kondisi Terkini**

|  |  |  |
| --- | --- | --- |
| **No** | ***Requirement* Pada BRD** | **Kondisi Pengembangan Terkini** |
| a. | Dari menu *confirmation page* OCTO Mobile, nasabah melakukan *approve* atau *reject* transaksi OOB dan menampilkan halaman resi transaksi sukses atau *pop up* transaksi tidak dilanjutkan. | Terdapat aktivitas *input* mPIN OCTO Mobile untuk konfirmasi transaksi OOB sebagai validasi transaksi. Informasi ini belum tersedia pada *flow* transaksi dan detail *requirement* BRD. |
| b. | 2.3. *Scope of Work*  VCAS mengimplementasikan sistem otentikasi untuk transaksi 3DS dengan menerapkan *Risk Based Analysis* (RBA) yang memberikan skor risiko transaksi yang dapat digunakan untuk menetapkan aturan *parameter* untuk memutuskan apakah transaksi akan berhasil, gagal, atau di-*challenge* (menggunakan OTP/MFA OCTO Mobile). | Bank menggunakan portal VCAS milik pihak ketiga sebagai media untuk *setting* parameter yang memutuskan apakah transaksi akan berhasil, gagal, atau di-*challenge*. Informasi penggunaan portal milik pihak ketiga belum tersedia pada BRD. |
| c. | 2.4. *User*  *Internal xxx Users*  Fraud Management Group, Credit Card Business, Debit Card Business, Corporate Card Business, Customer Experience, Customer Care, Digital Banking Business.  *XXXX CC Cardholders* | Pengembangan *Frictionless* *Transaction with* VCAS via OCTO Mobile juga akan digunakan oleh nasabah xxxx pengguna kartu debit, namun pada subbab ‘2.4. *User’* hanya menyebutkan pengguna kartu kredit saja. |
| d. | 3.3. *Functional Requirements*  3.3.1. *Positive Flow*  Inisiasi Transaksi  Dari sisi ESB akan mengirimkan data CC ke Asccend / *debit card* ke ITM atau SIBS untuk mendapatkan data *specific* nasabah (CIF, no HP, *Cardholder Name* & *Card Type*). | Pada aktivitas pengiriman data spesifik nasabah untuk debit card akan diambil dari aplikasi ITM dan tidak melibatkan aplikasi SIBS, sehingga informasi keterlibatan SIBS perlu disesuaikan. |