# **DAFTAR TEMUAN-TEMUAN UTAMA DAN POIN-POIN PENGEMBANGAN**

**Temuan-temuan Utama**

Berikut adalah temuan bersifat kritikal terkait dengan integritas dan akurasi penyusunan laporan keuangan menggunakan aplikasi *Core Banking System* yang termasuk dalam cakupan audit:

* 1. Bank Belum Memiliki Standar untuk *Hardening* untuk OS, DB, Aplikasi, dan Perangkat *End User*
  2. Terdapat Aktivitas yang Dilakukan oleh Vendor yang Tidak Diketahui Oleh Bank
  3. Belum Terdapat Dokumentasi *User Access Matrix* untuk Penggunaan Aplikasi *Core Banking System*
  4. Perlu Peningkatan Pengelolaan Akun User yang Meninggalkan Bank

**Poin-poin Pengembangan**

Berikut adalah temuan yang kami masukin sebagai aspek pengembangan dari lingkungan Teknologi Informasi yang termasuk dalam cakupan audit:

1. Pembaruan Buku Pedoman Manajemen Risiko Teknologi
2. Penyesuaian Terhadap Parameter Konfigurasi Keamanan OS Aplikasi dan *Database*
3. **TEMUAN-TEMUAN UTAMA**
   1. **Bank Belum Memiliki Standar untuk *Hardening* untuk OS, DB, Aplikasi, dan Perangkat *End User***

**Kondisi:**

Berdasarkan observasi dan pemeriksaan yang dilakukan, bank telah mengatur kewajiban untuk pelaksanaan hardening. Hal ini tercakup dalam Buku Pedoman Manajemen Risiko Teknologi, Buku 2C : Pedoman Umum, Bab IV: Pengelolaan Konfigurasi Dan Sarana, No. 37/KEP.DIR/TSI/2019. Namun, Bank belum memiliki standar *hardening* yang dapat digunakan untuk OS, DB, dan Aplikasi untuk *Core Banking System* Konven (T24 Konven) dan *Core Banking System* Syariah (T24 Syariah).

Dalam melakukan pengaman Teknologi Informasi, Bank juga telah menerapkan standar yang direkomendasikan dari vendor untuk pelaksanaan *hardening* terhadap OS, DB, dan Aplikasi. Namun, saat ini bank belum menetapkan standar *hardening* yang baku untuk dikonfigurasikan di OS, DB, Aplikasi, dan Perangkat *End User*.

**Risiko:**

Tidak adanya standar untuk pelaksanaan atau implementasi *hardening* pada OS, DB, Aplikasi dan Perangkat *End User* dapat berimplikasi implementasi keamanan sistem yang tidak terstandar, sehingga menyebabkan terdapatnya celah keamanan yang berakibat pada serangan dan kejahatan siber.

**Rekomendasi:**

* Bank menetapkan standar *hardening* terhadap OS, DB, Aplikasi, dan Perangkan *End User*.
* Bank melakukan implementasi terhadap standar *hardening* yang telah ditetapkan.

**Tanggapan Manajemen:**

Sesuai dengan rekomendasi Bank akan melakukan review dan evaluasi dan pengkinian terhadap Buku Pedoman Manajemen Risiko TI utamanya terkait standar *hardening* terhadap OS, DB, Aplikasi, dan Perangkat *End User*.

Target Triwulan I tahun 2023.

* 1. **Terdapat Aktivitas yang Dilakukan oleh Vendor yang Tidak Diketahui Oleh Bank**

**Kondisi:**

Berdasarkan observasi dan pemeriksaan yang berkaitan dengan Log Aktivitas User pada Aplikasi Core Banking System, Bank sudah menerapkan adanya Log Event untuk setiap aktivitas yang dijalankan oleh User Aplikasi Core Banking System. User-user aplikasi Core Banking System terdiri atas User Internal (Pegawai Bank) dan User dari Vendor.

Berdasarkan pemeriksaan pada Log Aktivitas User aplikasi Core Banking System tanggal 30 November 2022, ditemukan bahwa terdapat sebanyak 17 aktivitas yang dilakukan oleh User dari Vendor pada tanggal tersebut. Namun, Tim TSI belum mengetahui tujuan dan aktivitas yang dijalankan oleh User dari Vendor tersebut. 17 aktivitas yang dilakukan oleh User dari Vendor tersebut diantaranya adalah seperti berikut:

| **Tanggal** | **Waktu** | **Akun** | **Aktivitas** | **Keterangan** |
| --- | --- | --- | --- | --- |
| 20221130 | 11:44:40:033 | FDSSUPPORT04 | DM.MAPPING.  DEFINITION | FDS.CHN.LIMIT.UPD |
| 20221130 | 12:23:14:093 | FDSSUPPORT02 | VERSION | FUNDS.TRANSFER |
| 20221130 | 16:47:00:097 | FDSSUPPORT03 | TSA.SERVICE | BNK/PACS.RAISE.  ENTRY.SINGLE |
| 20221130 | 19:56:54:060 | FDSSUPPORT01 | FUNDS.TRANSFER | FT22334VVBTV |
| 20221130 | 19:52:40:092 | FDSSUPPORT03 | DATA.CAPTURE | DC223340001004001 |
| 20221130 | 14:59:13:019 | FDSSUPPORT03 | DATA.CAPTURE | DC223340001001001 |
| 20221130 | 19:50:57:079 | FDSSUPPORT03 | DATA.CAPTURE | DC223340001003001 |
| 20221130 | 19:56:54:060 | FDSSUPPORT01 | FUNDS.TRANSFER | FT22334VVBTV |
| 20221130 | 12:23:14:093 | FDSSUPPORT02 | VERSION | FUNDS.TRANSFER |
| 20221130 | 16:47:00:097 | FDSSUPPORT03 | TSA.SERVICE | BNK/PACS.RAISE.  ENTRY.SINGLE |
| 20221130 | 19:14:27:069 | FDSSUPPORT03 | TSA.SERVICE | BNK/PACS.RAISE.  ENTRY.SINGLE |
| 20221130 | 19:52:40:092 | FDSSUPPORT03 | DATA.CAPTURE | DC223340001004001 |
| 20221130 | 19:50:57:079 | FDSSUPPORT03 | DATA.CAPTURE | DC223340001003001 |
| 20221130 | 15:00:09:003 | FDSSUPPORT03 | DATA.CAPTURE | DC223340001002001 |
| 20221130 | 14:59:13:019 | FDSSUPPORT03 | DATA.CAPTURE | DC223340001001001 |
| 20221130 | 11:44:40:033 | FDSSUPPORT04 | DM.MAPPING.  DEFINITION | FDS.CHN.LIMIT.UPD |
| 20221130 | 15:00:09:003 | FDSSUPPORT03 | DATA.CAPTURE | DC223340001002001 |

**Risiko:**

Apabila Bank tidak melakukan pemantauan terhadap aktivitas yang dijalankan oleh vendor, maka meningkatkan risiko penyalahgunaan akses yang tidak terdeteksi. Hal ini dapat berakibat disrupsi terhadap operasional aplikasi Bank dan pelanggaran kerahasiaan data.

**Rekomendasi:**

* Bank melakukan konfirmasi kepada pihak vendor untuk mengetahui aktivitas apa yang dijalankan oleh User dari Vendor tersebut.
* Bank melakukan pengkajian secara berkala terhadap Log Event/Audit Trail untuk memeriksa aktivitas user ID yang digunakan oleh vendor.

**Tanggapan Manajemen:**

* Bank menyampaikan konfirmasi transaksi tersebut di atas kepada pihak vendor melalui Bugzilla 21526 - Terdapat Aktivitas Yang Dilakukan Oleh User FDSSUPPORT untuk mengetahui aktivitas yang dijalankan (terlampir).
* Bank akan memonitoring Log Event/Audit Trail untuk memeriksa aktivitas user.



* 1. **Belum Terdapat Dokumentasi *User Access Matrix* untuk Penggunaan Aplikasi *Core Banking System***

**Kondisi:**

Berdasarkan hasil pemeriksaan yang dilakukan mengenai pengelolaan user, saat ini sudah terdapat pembagian fitur-fitur yang dapat diakses oleh user. Pembagian fitur tersebut sudah diimplementasikan kedalam Sistem Core Banking System, baik Syariah maupun Konven. Namun, berdasarkan hasil pemeriksaan, ditemukan bahwa bank belum menetapkan kebijakan mengenai pembuatan *User Access Matrix*, sehingga bank belum memiliki dokumen *User Access Matrix* yang telah diformalkan.

Selain itu, berdasarkan hasil pemeriksaan yang dilakukan terhadap daftar user yang memiliki akses ke aplikasi T24 Konven dan T24 Syariah, terdapat sebanyak 10 akun user dari vendor pada aplikasi T24 Konven dan 10 akun user dari vendor pada aplikasi T24 Syariah. Bank sudah menutup akses untuk akun dari vendor yang sudah tidak digunakan, sehingga tersisa sebanyak 4 akun user dari vendor yang aktif pada aplikasi T24 Konven dan 3 akun user dari vendor pada aplikasi T24 Syariah. Akun dari Vendor tersebut adalah seperti berikut.

|  |  |
| --- | --- |
| Aplikasi T24 Konven: | * FDSSUPPORT01 |
|  | * FDSSUPPORT02 |
|  | * FDSSUPPORT03 |
|  | * FDSSUPPORT04 |
|  |  |
| Aplikasi T24 Syariah: | * FDSSUPPORT01 |
|  | * FDSSUPPORT02 |
|  | * FDSSUPPORT03 |

Sejumlah akun user vendor tersebut digunakan untuk membantu Bank dalam menyelesaikan permasalahan operasional yang dihadapi oleh Bank ketika menggunakan aplikasi T24 Konven maupun T24 Syariah. Namun, sejumlah akun user dari vendor tersebut tidak teridentifikasi memiliki *role*/*group* pada aplikasi T24 Konven maupun T24 Syariah. Bank juga belum mendokumentasikan batasan apa saja yang dapat dilakukan oleh akun user dari vendor tersebut.

**Risiko:**

* Tanpa standar manajemen akses yang baku dapat menimbulkan risiko pemberian hak akses yang tidak sesuai dengan kebutuhan pengguna atau user.
* Tanpa adanya informasi terkait wewenang dan tanggung jawab user vendor, maka Bank akan dapat mengalami hambatan akurasi dalam melakukan audit/pemeriksaan berkala terhadap aktivitas transaksi yang tidak diotorisasi.

**Rekomendasi:**

* Bank menyusun *user access matrix* yang secara formal dicakupkan ke dalam kebijakan yang baku dan mencakup untuk user internal maupun user eksternal. Dalam praktiknya, *user access matrix* dapat disusun berdasarkan pemetaan fungsi/kelompok fungsi pada sistem terhadap kelompok/unit kerja pengguna. Matriks tersebut dijadikan acuan dalam memberikan hak akses kepada suatu kelompok/unit kerja sesuai dengan kebutuhan tugas dan tanggung jawab kelompok/unit kerja tersebut.
* Bank menetapkan dan mendokumentasikan batasan yang dapat dilakukan oleh user dari Vendor tersebut.

**Tanggapan Manajemen:**

* Bank akan menyusun *user access matrix* sebagaimana rekomendasi auditor.
* Bank akan menetapkan dan mendokumentasikan batasan yang dapat dilakukan oleh user.

Target Triwulan II tahun 2023.

* 1. **Perlu Peningkatan Pengelolaan Akun User yang Meninggalkan Bank**

**Kondisi:**

Berdasarkan hasil observasi yang dilakukan terhadap prosedur pengelolaan User ketika pengguna meninggalkan entitas, Tim TSI Bank akan mendapatkan informasi karyawan yang meninggalkan Bank dari Tim Human Capital, kemudian Tim TSI akan melakukan penonaktifan akun karyawan tersebut dengan melakukan perubahan pada *Profile Expiry Date*. Dengan melakukan penyesuaian terhadap *Profile Expiry Date*, maka akun karyawan tersebut tidak akan dapat digunakan apabila sudah melewati tanggal yang ditetapkan.

Namun, berdasarkan pemeriksaan yang telah dilakukan terhadap daftar Akun User yang terdapat pada aplikasi T24 Konven dan T24 Syariah, ditemukan bahwa terdapat sebanyak 17 karyawan yang sudah meninggalkan Bank, tetapi akun user tersebut terlambat dinonaktifkan pada aplikasi T24 Konven maupun T24 Syariah. Dari sebanyak 17 akun user tersebut, ditemukan sebanyak 6 karyawan yang sudah meninggalkan Bank, tetapi memiliki *Profile Expiry Date* pada tahun 2099. Sebanyak 17 akun tersebut diantaranya adalah seperti berikut.

| **Nama** | **Tanggal Keluar** | **Jabatan** | **Expired Date Konven** | **Expired date Syariah** | **Status Akun** |
| --- | --- | --- | --- | --- | --- |
| Achmad Rifa'i | 10-Aug-22 | Staf Seksi Operasional | 31-Dec-99 | 31-Dec-99 | Aktif |
| Dita Permatasari | 12-Aug-22 | Staf Transaksi Kredit | 31-Dec-99 | 31-Dec-99 | Aktif |
| Firda Nur Annisa | 24-Oct-22 | Staf Seksi Pelayanan Nasabah (Teller) | 31-Dec-99 | 31-Dec-99 | Aktif |
| Dita Permata Puteri | 03-Oct-22 | Staf Seksi Pelayanan Nasabah (Teller) | 31-Dec-99 | 31-Dec-99 | Aktif |
| Hendry Septian Saputra | 24-Oct-22 | Staf Transaksi Kredit | 31-Dec-99 | 31-Dec-99 | Aktif |
| Muhammad Hanafiah | 31-Oct-22 | Kepala Cabang | 01-Nov-22 | 31-Dec-99 | Aktif |
| Edward Maliq AS. | 07-Feb-22 | Staf Seksi Pemasaran | 18-May-22 | #N/A | Nonaktif |
| Yuniar Fauzia | 01-Mar-22 | Staf Seksi Pemasaran (Funding) | 18-May-22 | 10-Jun-22 | Nonaktif |
| Annisa Erliani | 21-Feb-22 | Staf Seksi Operasional | 18-May-22 | 10-Jun-22 | Nonaktif |
| Anton Tjahjadi | 31-Jan-22 | KIC Cabang A. Yani Banjarmasin | 18-May-22 | 18-May-22 | Nonaktif |
| Eka Puspa Sari | 14-Feb-22 | Staf Seksi Pemasaran | 18-May-22 | 10-Jun-22 | Nonaktif |
| Gelly Susanti | 04-Apr-22 | Staf Seksi Operasional | 18-May-22 | 10-Jun-22 | Nonaktif |
| Indra Azhari | 01-Mar-22 | Kredit/Pembiayaan Bermasalah Cabang Martapura | 01-Mar-22 | 10-Jun-22 | Nonaktif |
| Linda Lusiana | 03-Jan-22 | Teller Cabang Pembantu Pagatan | 18-May-22 | 18-May-22 | Nonaktif |
| Mega Pardosi | 07-Feb-22 | Staf Seksi Pelayanan Nasabah (Customer Service) | 18-May-22 | 18-May-22 | Nonaktif |
| Nanda Wulan Pratiwi | 03-Jan-22 | Staf Seksi Customer Service | 18-May-22 | 18-May-22 | Nonaktif |
| Sri Heldawati | 21-Mar-22 | Staf Pemasar Konsumer KC Pembantu Gunung Tinggi | 18-May-22 | 10-Jun-22 | Nonaktif |
| Wahyu Adhitya | 21-Mar-22 | Staf Pemasaran Cabang Pembantu Handil Bakti | 18-May-22 | 10-Jun-22 | Nonaktif |

Selain itu ditemukan 17 akun yang terlambat dinonaktifkan lebih dari 3 bulan, ditemukan pula sebanyak 6 karyawan yang sudah meninggalkan Bank, tetapi akun user karyawan tersebut masih melakukan aktivitas Login ke sistem T24 Konven dan T24 Syariah setelah karyawan meninggalkan Bank. Sebanyak 6 akun tersebut diantaranya adalah seperti berikut:

| **Nama** | **Tanggal Keluar** | **Jabatan** | **Last Login T24 Konven** | **Last Login T24 Syariah** |
| --- | --- | --- | --- | --- |
| Ahmad Akbar | 30-Jun-22 | Staf Bagian Support UMK | 25-Jul-22 | 30-Dec-21 |
| Achmad Rifa'i | 10-Aug-22 | Staf Seksi Operasional | 00-Jan-00 | 08-Nov-22 |
| Dita Permatasari | 12-Aug-22 | Staf Transaksi Kredit | 11-Aug-22 | 26-Sep-22 |
| Edward Maliq AS. | 07-Feb-22 | Staf Seksi Pemasaran | 31-Mar-22 | #N/A |
| Firda Nur Annisa | 24-Oct-22 | Staf Seksi Pelayanan Nasabah (Teller) | 31-Oct-22 | 27-May-22 |
| Yuniar Fauzia | 01-Mar-22 | Staf Seksi Pemasaran (Funding) | 28-Apr-22 | 14-Nov-21 |

**Risiko:**

Apabila masih terdapat hak akses bagi karyawan yang sudah meninggalkan Bank, maka dapat menimbulkan risiko adanya penyalahgunaan dalam menggunakan sistem termasuk melakukan transaksi yang tidak sah dan dapat berdampak langsung pada laporan keuangan

**Rekomendasi:**

* Bank melakukan penonaktifan hak akses untuk akun user pengguna/karyawan yang sudah meninggalkan Bank.
* Bank meningkatkan koordinasi dengan tim Human Capital untuk memperoleh informasi karyawan yang meninggalkan Bank secara berkala.
* Bank melakukan pengkajian secara berkala untuk memastikan bahwa tidak ada akun User yang masih aktif setelah pengguna/karyawan meninggalkan Bank.

**Tanggapan Manajemen:**

* Bank telah melakukan penonaktifan user pengguna/karyawan (terlampir).
* Bank telah menyampaikan NDE (nota dinas elektronik) ke Divisi Human Capital untuk memperoleh informasi karyawan yang meninggalkan Bank secara berkala (terlampir).
* Bank akan menonaktifkan user yang masih aktif setelah pengguna/karyawan meninggalkan Bank.



1. **POIN-POIN PENGEMBANGAN**
   1. **Pembaruan Buku Pedoman Manajemen Risiko Teknologi**

**Kondisi:**

Berdasarkan pemeriksaan yang dilakukan terhadap dokumen kebijakan dan prosedur manajemen risiko terknologi informasi (TI), bank sudah mendokumentasikan prosedur yang berkaitan dengan manajemen risiko TI.

Namun, dari beberapa dokumen kebijakan dan prosedur manajemen risiko TI tersebut, ditemukan bahwa terdapat beberapa Buku Pedoman yang terakhir diperbarui pada tahun 2019. Buku Pedoman tersebut diantaranya adalah.

1. Buku Pedoman Teknologi Sistem Informasi Buku 2A Kebijakan Umum Pengamanan Teknologi Informasi No. 35/KEP.DIR/TSI/2019, tanggal 14 Juni 2019.
2. Buku Pedoman Teknologi Sistem Informasi Buku 2B Pedoman Pengembangan Dan Pengadaan Teknologi Informasi (BAB I, BAB II, BAB III, BAB IV, BAB VI, BAB VII) No. 36/KEP.DIR/TSI/2019, tanggal 14 Juni 2019.
3. Buku Pedoman Manajemen Risiko Teknologi Informasi 2C Pedoman Operasional Teknologi Informasi, 37/KEP.DIR/TSI/2019, 14 Juni 2019.

**Risiko:**

Terlambatnya pengkajian dan pengkinian terhadap kebijakan dapat menyebabkan adanya ketidaktepatan antara penerapan pengelolaan teknologi informasi dengan tren keamanan teknologi dan ancaman siber lainnya.

**Rekomendasi:**

Bank melakukan review dan evaluasi dan pengkinian terhadap Buku Pedoman Manajemen Risiko TI

**Tanggapan Manajemen:**

Target Triwulan II tahun 2023.

* 1. **Penyesuaian Terhadap Parameter Konfigurasi Keamanan OS Aplikasi dan *Database***

**Kondisi:**

Berdasarkan pemeriksaan yang dilakukan terhadap parameter konfigurasi keamanan, Bank mengimplementasikan konfigurasi keamanan yang mengacu pada rekomendasi standar konfigurasi keamanan dari pihak Vendor.

Namun, terdapat perbedaan antara rekomendasi konfigurasi dengan implementasi konfigurasi pada OS *database* dan aplikasi T24 Konven dan T24 Syariah. Perbedaan antara rekomendasi dengan implementasi konfigurasi adalah seperti berikut:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Parameter** | **Rekomendasi** | **OS T24 Konven** | **OS T24 Konven** | **OS T24 Konven** | **OS T24 Konven** |
| *Pass Max Days* | 30 – 60 hari | 90 hari | 90 hari | 99999 hari | 99999 hari |
| *Min Pas Len* | 6 karakter | 6 karakter | 6 karakter | 5 Karakter | 5 Karakter |

**Risiko:**

Ketidaktepatan konfigurasi keamanan perangkat berisiko menimbulkan gangguan operasional dan risiko kelemahan keamanan informasi. Bank juga berisiko mengalami hambatan dalam menyeragamkan konfigurasi masing-masing perangkat jaringan di lingkungan perusahaan.

**Rekomendasi:**

Bank melakukan penyesuaian implementasi konfigurasi dengan rekomendasi konfigurasi.

**Tanggapan Manajemen:**

* Bank sesuai rekomendasi auditor akan melakukan penyesuaian implementasi konfigurasi Keamanan OS Aplikasi dan *Database* dan meminta petunjuk vendor yang telah disampaikan melalui Bugzilla [21525](https://bugz.fds.co.id/show_bug.cgi?id=21525) - Penyesuaian Terhadap Password Parameter Konfigurasi Keamanan OS Aplikasi dan Database (terlampir).

