

**Compliance**

**SAGA**

***SELF-ASSESSMENT SAGA COMPLIANCE REVIEW* *(SASAR)***

**BAHAGIAN KHIDMAT PERUNDING**

**JABATAN AKAUNTAN NEGARA MALAYSIA**

**NAMA AGENSI : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**KEMENTERIAN /**

**SUK NEGERI : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\*\*UNTUK KEGUNAAN SEKRETARIAT PEMATUHAN SAGA SAHAJA\*\***

**TARIKH LAWATAN : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**SIRI LAWATAN : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**SKOR FUNGSIAN : \_\_\_\_\_\_\_/ 12 KRITERIA**

**SKOR TEKNIKAL : \_\_\_\_\_\_\_/ 8 KRITERIA**

**TOTAL SKOR : \_\_\_\_\_\_\_/ 20 KRITERIA**

**RATING:**

**BAIK (15 – 20 KRITERIA)**

**MEMUASKAN (10 – 15 KRITERIA)**

**TIDAK MEMUASKAN (< 10 KRITERIA)**

**MAKLUMAT AGENSI:**

|  |  |  |
| --- | --- | --- |
| Latar Belakang Agensi | : |  |
| Alamat Agensi | : |  |
| Pegawai Bertanggungjawab | : |  |
| No. Telefon/ Faksimili | : |  |
| Bilangan Pengguna Sistem Aplikasi | : |  |
| Bilangan *Concurrent User* | : |  |
| Bilangan Cawangan | : |  |
| Lokasi Cawangan | : |  |

**MAKLUMAT SISTEM APLIKASI:**

|  |  |  |
| --- | --- | --- |
| Nama Sistem Aplikasi & Versi Terkini | : |  |
| Tarikh Kelulusan Reka Bentuk Sistem Aplikasi | : |  |
| Tarikh Pembangunan Aplikasi Sistem | : |  |
| Tarikh Pelaksanaan Sistem Aplikasi | : |  |
| Pembekal/ Pembangun Sistem Aplikasi | : |  |
| Senarai Modul Dalam Sistem Aplikasi Perakaunan & Kewangan | : |  |
| Senarai Sistem Sokongan Yang Berintegrasi Dengan Sistem Aplikasi Perakaunan & Kewangan | : |  |
| Capaian Sistem Aplikasi (Client/ Web based) | : |  |
| PlatformSistem Pengoperasian (Operating System-Platform)/ Versi Bagi Aplikasi | : |  |
| PlatformSistem Pengoperasian (Operating System-Platform)/ Versi Bagi Pangkalan Data |  |  |
| Perisian Pembangunan Aplikasi/ Versi | : |  |
| Perisian Pembangunan Pangkalan Data/ Versi | : |  |
| Spesifikasi Server Aplikasi | : |  |
| Spesifikasi ServerPangkalan Data | : |  |
| Kapasiti Storan Server Bagi Aplikasi & Pangkalan Data | : |  |
| Penggunaan (utilisation) Server Terkini Bagi Aplikasi & Pangkalan Data | : |  |

Tandakan (√) pada ruangan **‘YA’** atau **‘TIDAK’** dan catatan/ ulasan boleh diisi di ruangan **‘CATATAN AGENSI’**.

| **BIL.** | **KRITERIA PEMATUHAN SAGA** | **YA** | **TIDAK** | **CATATAN AGENSI** | **DOKUMEN SOKONGAN** |
| --- | --- | --- | --- | --- | --- |
| **A. KRITERIA FUNGSIAN** | | | | | |
| **1.** | **Piawaian Perakaunan Yang Diterima Pakai**  Sistem aplikasi perakaunan dan kewangan perlu mematuhi Prinsip Perakaunan Diterima Umum (*General Accepted Accounting Principles*) yang ditetapkan oleh mana-mana badan penetap piawaian. | | | | |
| **(a)** | Adakah agensi menerima pakai piawaian perakaunan yang ditetapkan oleh Jabatan Akauntan Negara Malaysia (JANM) iaitu MPSAS atau *Malaysian Accounting Standards Board* (MASB) iaitu MPERS/ MFRS? Nyatakan. |  |  |  | Penyata Kewangan Terkini Yang Telah Diaudit  Surat Kelulusan Pemakaian MPSAS |
| **(b)** | Adakah peraturan yang berkuat kuasa diterima pakai dalam penyediaan penyata kewangan seperti Akta/ Arahan/ Polisi dan lain-lain? Nyatakan. |  |  |  | Salinan Akta/ Arahan/ Polisi dan lain-lain (berkaitan Perakaunan dan Kewangan) |
| **(c)** | Adakah agensi mempunyai syarikat subsidiari?  Jika ya, senaraikan syarikat subsidiari dan piawaian perakaunan yang diterima pakai.  Jika tidak berkenaan, sila abaikan soalan ini. |  |  |  | Penyata Kewangan Terkini Yang Telah Diaudit (Nota Kepada Akaun) |
| **2.** | **Asas Perakaunan Akruan**  Sistem aplikasi perakaunan dan kewangan mesti berasaskan perakaunan akruan. | | | | |
| **(a)** | Adakah sistem aplikasi perakaunan dan kewangan agensi menggunakan asas perakaunan akruan? |  |  |  | Penyata Kewangan Terkini Yang Telah Diaudit (Dasar - dasar Perakaunan) |
| **(b)** | Adakah titik pengiktirafan dan catatan bergu adalah tepat dan betul bagi akaun berikut:     1. Hasil (Titik Pengiktirafan : Tarikh invois/ bil agensi dikeluarkan **atau** Tunai diterima). 2. Belanja (Titik Pengiktirafan : Tarikh barang/ perkhidmatan diterima *- Goods Received Notes (GRN)/ Delivery Order (DO)* **atau** Tarikh invois/ bil). 3. Aset (Contoh: Aset Tetap, Pelaburan Jangka Panjang, Pinjaman Pekerja, Akaun Belum Terima)? 4. Liabiliti (Contoh: Pinjaman, Geran, Manfaat Pekerja, Deposit Diterima)? |  |  |  | Paparan skrin catatan bergu pengiktirafan Hasil  Paparan skrin catatan bergu pengiktirafan Belanja  Paparan skrin catatan bergu pengiktirafan Aset  Paparan skrin catatan bergu pengiktirafan Liabiliti |
| **3.** | **Kod Carta Akaun Yang Fleksibel**  Sistem aplikasi perakaunan dan kewangan mempunyai Kod Carta Akaun yang fleksibel mengikut keperluan Agensi Kerajaan. Jenis Akaun bagi Kod Carta Akaun hendaklah terbahagi kepada Hasil, Belanja, Aset, Liabiliti dan Ekuiti. | | | | |
| **(a)** | Adakah Kod Carta Akaun adalah fleksibel iaitu boleh ditambah/ dikurang? Nyatakan bilangan dan saiz segmen bagi Kod Carta Akaun.  Contoh: 4 segmen Kod Carta Akaun   |  |  |  |  | | --- | --- | --- | --- | | **Jenis Akaun** | **Kelas Akaun** | **Sub Kelas** | **Siri** | | **L**  (1 aksara) | **9**  (1 aksara) | **9**  (1 aksara) | **999**  (3 aksara) | |  |  |  | Salinan Kod Carta Akaun  Penerangan mengenai Kod Carta Akaun. |
| **(b)** | Adakah Kod Carta Akaun diklasifikasi mengikut kategori aset, liabiliti, ekuiti, belanja dan hasil? |  |  |  | Salinan Kod Carta Akaun bagi setiap kategori L.E.B.A.H |
| **4.** | **Penutupan Akaun**  Transaksi kewangan boleh diperakaunkan pada setiap hari bagi menjana penyata kewangan. | | | | |
| **(a)** | 1. Adakah setiap transaksi kewangan diperakaunkan ke Lejar Am secara harian? 2. Adakah Imbangan Duga (Trial Balance) dapat dijana secara harian dan imbang? |  |  |  | Salinan Imbangan Duga bagi 2 hari berturutan |
| **(b)** | Bagi penutupan bulanan, adakah sistem secara automatik berupaya mengakaunkan transaksi hasil dan belanja bulanan seperti hasil faedah, belanja susut nilai dan lain-lain? |  |  |  | Paparan skrin Lejar Belanja Susut Nilai  Paparan skrin Lejar Hasil Faedah |
| **(c)** | Bagi penutupan tahunan, adakah sistem secara automatik berupaya:   1. menyifarkanakaun bagi item Penyata Prestasi Kewangan/ Penyata Pendapatan Komprehensif? 2. membawa baki akaun ke tahun hadapan bagi item Penyata Kedudukan Kewangan?   Nyatakan tarikh akaun tahun semasa ditutup dan baki awal dibawa ke hadapan. |  |  |  | Paparan skrin “baki akhir” tahun sebelum dan “baki awal” tahun semasa Penyata Prestasi/ Pendapatan  Paparan skrin “baki akhir” tahun sebelum dan “baki awal” tahun semasa bagi Penyata Kedudukan |
| **5.** | ***Single-Point Data Entry* DanIntegrasi**  Sistem aplikasi perakaunan dan kewangan bercirikan *single-point data entry* iaitu modul-modul dalam sistem aplikasi perakaunan dan kewangan mestilah berhubung kait (*interoperability*). Sistem sokongan berkaitan datakewangan mestilah berintegrasi dengan sistem aplikasi perakaunan dan kewangan secara harian. | | | | |
| **(a)** | Adakah sistem menggunakan konsep *Single Point Data Entry* iaitu hanya perlu mengunci masuk data kewangan sekali sahaja dan sistem akan mengemas kini maklumat secara automatik dalam semua modul yang berkaitan? |  |  |  | Gambar Rajah Keseluruhan Sistem (termasuk sistem sokongan yang memberikan input kewangan)  Gambar Rajah Aliran Kerjautama |
| **(b)** | Adakah semua transaksi diperakaun ke Lejar Am melalui modul dalam sistem aplikasi atau sistem sokongan? Contoh: Belanja Susut Nilai diperakaunkan melalui Modul Aset.  Nota: Transaksi yang diperakaunkan melalui jurnal pelarasan manual adalah tidak mematuhi konsep *single-point data entry*. |  |  |  | Paparan skrin menu/ senarai modul dalam sistem perakaunan dan kewangan  Paparan skrin menu sistem sokongan |
|  |  |  |
| **(c)** | Adakah modul-modul yang berhubung kait (interoperability) dalam sistem aplikasi perakaunan dan kewangan berintegrasi secara *real-time*?  Nota: *Walkthrough test* bagi satu transaksi sehingga selesai diperakaunkan ke Lejar Am. Contoh: Proses bayaran dan proses terimaan. |  |  |  | Paparan skrin proses bayaran daripada input pertama sehingga diperakaunkan ke Lejar Am |
| **(d)** | Adakah sistem sokongan berkaitan data kewangan berintegrasi dengan sistem aplikasi perakaunan dan kewangan secara harian? |  |  |  | Senarai sistem sokongan, kaedah integrasi dan masa penghantaran data ke sistem perakaunan |
| **6.** | **Penambahan/ Pengurangan Modul**  Penambahan dan pengurangan modul boleh dilakukan mengikut keperluan Agensi Kerajaan. | | | | |
| **(a)** | Adakah sistem aplikasi adalah fleksibel untuk menambah dan mengurangkan modul mengikut keperluan agensi? |  |  |  | Senarai penambahan/ pengurangan modul  Paparan skrin modul yang ditambah/ dikurang |
| **7.** | **Proses Kelulusan Dalam Talian (Online Workflow)**  Sistem aplikasi perakaunan dan kewangan berupaya untuk membuat proses aliran kerja dalam talian (*online workflow*)bermula dari peringkat penyediaan sehingga kelulusan*.* | | | | |
| **(a)** | Adakah proses aliran kerja dalam talian (online workflow) boleh dilakukan di dokumen kewangan berikut:   1. Pesanan Tempatan? 2. Baucar Bayaran? 3. Baucar Jurnal?   Nyatakan bilangan proses aliran kerja dalam talian (online workflow) bagi setiap dokumen kewangan tersebut.  Nota: Sistem tidak membenarkan pegawai yang sama menyemak dan melulus dokumen yang sama. |  |  |  | Paparan skrin proses kelulusan Pesanan Tempatan  Paparan skrin proses kelulusan Baucar Bayaran  Paparan skrin proses kelulusan Baucar Jurnal |
| **(b)** | Adakah maklumat berikut dipaparkan pada dokumen kewangan yang dijana:   1. Tarikh sedia, semak dan lulus 2. Masa sedia, semak dan lulus 3. Nama pegawai penyedia, penyemak dan pelulus 4. Jawatan pegawai penyedia, penyemak dan pelulus |  |  |  | Salinan Pesanan Tempatan yang dijana  Salinan Baucar Bayaran yang dijana  Salinan Baucar Jurnal yang dijana |
| **(c)** | Adakah sistem berupaya memaparkan senarai transaksi yang belum selesai? |  |  |  | Paparan skrin transaksi yang belum selesai |
| **(d)** | Adakah senarai transaksi belum selesai yang dipaparkan adalah tepat? |  |  |  |
| **(e)** | Adakah agensi menggunakan *Public Key Infrastructure* (PKI) sebagai kawalan keselamatan tambahan bagi sistem ini?  Jika tidak berkenaan, sila abaikan soalan ini. |  |  |  | Paparan skrin tandatangan digital  Senarai pengguna dan tempoh sah guna PKI |
| **8.** | **Pembayaran dan Terimaan Secara Elektronik**  Sistem aplikasi perakaunan dan kewangan mempunyai kemudahan pembayaran dan terimaan secara elektronik. | | | | |
| **(a)** | Adakah sistem berupaya membuat pembayaransecara Pindahan Dana Elektronik(EFT)?  Jika ya, nyatakan:   1. Nisbah EFT kepada cek (Contoh: 90:10) 2. Justifikasi sekiranya nisbah EFT kepada cek kurang daripada 90%. |  |  |  | Paparan skrin urutan proses pembayaran EFT |
| **(b)** | Adakah notifikasi pembayaran dihantar secara automatik kepada penerima melalui sistem aplikasi agensi? Jika ya, nyatakan kaedah yang digunakan.  Nota: Semakan di portal agensi juga dibenarkan. |  |  |  | Paparan skrin notifikasi pembayaran EFT |
| **(c)** | Adakah sistem menyokong terimaan secara elektronik/ perbankan internet?  Jika ya, nyatakan:   1. Kaedah terimaan secara elektronik/ perbankan internet. 2. Kaedah untuk memperakaunkan transaksi terimaan secara elektronik/ perbankan internet. |  |  |  | Senarai terimaan elektronik/ perbankan internet |
| **9.** | **Penyesuaian Bank**  Sistem aplikasi perakaunan dan kewangan berupaya membuat penyesuaian bank melalui penyata bank yang dimuat naik. | | | | |
| **(a)** | Adakah Penyata Penyesuaian Bank disediakan melalui sistem? Nyatakan sistem aplikasi/ modul yang digunakan untuk membuat penyesuaian bank. |  |  |  | Senarai semua akaun bank (termasuk Cawangan) dan kaedah penyesuaian bank (manual/ auto)  Paparan skrin Penyata Penyesuaian Bank  Salinan Penyata Penyesuaian Bank terkini yang dijana daripada sistem |
| **(b)** | Adakah fail penyata bank boleh dimuat naik ke dalam sistem? |  |  |  | Surat kuasa untuk muat naik penyata bank ke sistem  Paparan skrin urutan proses muat naik penyata bank ke sistem |
| **(c)** | Adakah sistem berupaya membuat padanan automatik (auto-match) dan padanan manual (force-match) untuk tujuan penyediaan penyata penyesuaian bank? |  |  |  | Paparan skrin urutan proses padanan automatik (auto-match)  Paparan skrin urutan proses padanan manual (force-match*)* |
| **(d)** | Adakah sistem mempunyai petunjuk/ indikator bagi membezakan item padanan automatik (auto-match) dan padanan manual (force-match) dalam penyediaan penyesuaian bank? |  |  |  | Paparan skrin petunjuk/ indikator bagi padanan automatik (auto-match) dan padanan manual (force-match) |
| **10.** | **Penjanaan Penyata Kewangan dan Laporan**  Sistem aplikasi perakaunan dan kewangan berupaya untuk menjana dan mencetak Penyata Kewangan yang lengkap dan laporan yang diperlukan pada bila-bila masa. | | | | |
| **(a)** | Adakah sistem berupaya untuk menyedia dan menjana Penyata Kewangan berikut pada setiap bulan:   1. Penyata Prestasi Kewangan/ Penyata Pendapatan Komprehensif? 2. Penyata Kedudukan Kewangan? 3. Penyata Aliran Tunai? 4. Penyata Perubahan Aset Bersih/ Ekuiti? |  |  |  | Salinan Penyata Kewangan yang dijana melalui sistem pada 31 Disember (jumlah amaun dikira semula dan disemak silang) |
| **(b)** | Adakah Penyata Kewangan yang dijana betul dan tepat? |  |  |  |
| **(c)** | Adakah sistem berupaya menjana dan mencetak laporan lain yang diperlukan? Nyatakan laporan tersebut. |  |  |  | Salinan laporan yang dijana oleh sistem (Contoh: Laporan Pengumuran (*Ageing Report)*, Daftar Bil dan lain-lain) |
| **(d)** | Adakah laporan boleh diekstrak menggunakan pelbagai format fail (contoh: excel, html, pdfdan lain-lain)? |  |  |  | Paparan skrin pilihan format fail yang boleh dijana |
| **11.** | **Pengauditan**  Data boleh diekstrak daripada pangkalan data bagi tujuan pengauditan. | | | | |
| **(a)** | Adakah data kewangan boleh diekstrak daripada pangkalan data apabila diperlukan oleh juruaudit atau pihak tertentu untuk digunakan dalam aplikasi pengauditan seperti *Audit Command Language* (ACL)? |  |  |  | Paparan skrin fail yang telah diekstrak |
| **(b)** | Adakah jenis pangkalan data agensi merupakan *Relational Database Management System (RDBMS)*?  Nota: RDBMS adalah sistem pengurusan pangkalan data yang menyimpan data dalam bentuk jadual (table) yang berhubung kait. |  |  |  | *Entity Relationship Diagram (ERD)* |
| **12.** | **Penyimpanan Data (Storan)**  Sistem aplikasi perakaunan dan kewangan berupaya untuk menyimpan data dan jejak audit bagi tempoh sekurang-kurangnya 2 tahun. | | | | |
| **(a)** | Adakah sistem mempunyai kapasiti storan yang mencukupi? Nyatakan jumlah kapasiti storan dan peratus penggunaan terkini. |  |  |  | Paparan skrin kapasiti storan dan peratus penggunaan storan terkini |
| **(b)** | Adakah sistem berupaya untuk menyimpan data dan jejak audit dalam pangkalan data bagi tempoh sekurang-kurangnya 2 tahun? Nyatakan tempoh storan dalam pangkalan data. |  |  |  | Sampel dokumen kewangan di sistem bagi 2 tahun dan ke atas (contoh: Baucar, Resit) |

**Disediakan Oleh**:

Bahagian Kewangan

……………………………………..

Nama :

Jawatan :

Tarikh :

**Disahkan Oleh**:

Bahagian Kewangan

………………………………………..

Nama :

Jawatan :

Tarikh :

| **BIL** | **KRITERIA PEMATUHAN SAGA** | **YA** | **TIDAK** | **CATATAN AGENSI** | **DOKUMEN SOKONGAN** |
| --- | --- | --- | --- | --- | --- |
| **B. KRITERIA TEKNIKAL** | | | | | | |
| **1.** | **Pentadbiran Profil Keselamatan Pengguna**  Sistem aplikasi perakaunan dan kewangan mempunyai Pentadbiran Profil Keselamatan Pengguna merangkumi hak dan had penggunaan sistem, surat lantikan pentadbir sistem dan *Standard Operating Procedure* (SOP). | | | | | |
| **(a)** | 1. Adakah agensi melantik pentadbir sistem untuk sistem aplikasi perakaunan dan kewangan di agensi? 2. Adakah agensi melantik sekurang-kurangnya dua orang pentadbir sistem? |  |  |  | Surat Lantikan Pentadbir Sistem |
| **(b)** | Adakah pentadbir sistem tidak terlibat dalam operasi sistem aplikasi perakaunan dan kewangan agensi? |  |  |  | Paparan skrin profil capaian Pentadbir Sistem |
| **(c)** | Adakah agensi mempunyai *Standard Operating Procedure* (SOP) bagi pentadbiran pengguna? |  |  |  | SOP Pentadbiran Profil Keselamatan Pengguna |
| **(d)** | Adakah SOP pentadbiran pengguna mempunyai maklumat berikut:   1. Penerangan mengenai tatacara pendaftaran pengguna, pengemaskinian tahap capaian/ hak modul dan peranan, had kuasa kelulusan pengguna serta penamatan ID? 2. Borang permohonan pendaftaran pengguna, pengemaskinian tahap capaian/ hak, had kuasa, penamatan ID? 3. Carta alir tatacara pendaftaran pengguna, pengemaskinian tahap capaian/ hak, had kuasa serta penamatan ID? 4. Tarikh kemas kini? |  |  |  |
| **(e)** | Adakah agensi mempunyai borang pentadbiran profil keselamatan pengguna yang merekodkan maklumat berikut:   1. Pendaftaran ID? 2. Tahap capaian/ hak modul dan peranan? 3. Had kuasa kelulusan? 4. Penamatan ID? 5. Tarikh kuat kuasa? |  |  |  | Salinan Borang Capaian Pengguna Sistem yang telah diluluskan |
| **(f)** | Adakah sistem aplikasi mempunyai kemudahan pentadbiran profil keselamatan untuk mengkonfigurasi dan menyenggara setiap capaian pengguna di sistem? |  |  |  | Paparan skrin senarai pengguna dan capaian/ had kuasa |
| **(g)** | Adakah setiap pengguna dibekalkan dengan satu ID dan ID tersebut adalah unik seperti nama singkatan, nombor kad pengenalan atau nombor pekerja? Nyatakan. |  |  |  | Paparan skrin bukti ID adalah unik |
| **(h)** | Adakah ID pengguna yang berstatus *inactive* tidak akan dihapuskan (dalam sesuatu tempoh mengikut dasar keselamatan agensi) bagi membolehkan rekod jejak audit diekstrak apabila diperlukan?  Nota: ID pengguna boleh dihapuskan dari pangkalan data dalam proses pengemasan (housekeeping) mengikut tempoh yang bersesuaian. |  |  |  | Paparan skrin bukti ID ditukar kepada status *inactive* |
| **2.** | **Jejak Audit(Audit Trail)Daripada Sistem**  Sistem aplikasi perakaunan dan kewangan mempunyai jejak audit bagi merekod semua aktiviti pengguna yang merangkumi ID pengguna, modul yang diakses serta tarikh dan masa bagi setiap aktiviti termasuk log masuk dan log keluar. | | | | | |
| **(a)** | Adakah sistem aplikasi perakaunan dan kewangan mempunyai fungsi jejak audit?  Nota: Setiap aktiviti yang dilakukan perlu direkod mengikut kronologi bagi tujuan mengesan jejak audit. |  |  |  | Paparan skrin Laporan Jejak Audit terkini berdasarkan modul  Paparan skrin Laporan Jejak Audit terkini berdasarkan ID  Paparan skrin Laporan Jejak Audit (*login* pengguna) |
| **(b)** | Adakah sistem aplikasi perakaunan dan kewangan merekod setiap aktiviti pengguna di dalam sistem seperti berikut:   1. ID Pengguna? 2. Tarikh dan Masa Transaksi? 3. Jenis Transaksi? 4. Modul yang Diakses? 5. Maklumat log masuk dan log keluar |  |  |  |
| **(c)** | Adakah sistem aplikasi perakaunan dan kewangan berupaya menjana/ mengekstrak laporan jejak audit? |  |  |  |
| **3.** | **Sistem *Log Server***  Sistem aplikasi perakaunan dan kewangan mempunyai sistem log bagi merekodkan semua aktiviti capaian di server aplikasi dan pangkalan data. | | | | | |
| **(a)** | Adakah sistem log server dipasang/ dikonfigurasi di server aplikasi dan pangkalan data untuk merekod semua aktiviti capaian ke atas server?  Nota: Setiap aktiviti capaian perlu direkod bagi tujuan mengesan ralat atau wujudnya aktiviti lain yang tidak sah. Jejak audit dan log sistem hendaklah dilog secara berpusat dan integriti dilindungi dari perubahan yang disengaja atau tidak disengajakan, dipantau setiap hari untuk mengesan aktiviti luar biasa dan disimpan dalam tempoh yang disarankan oleh Arkib Negara. |  |  |  | Paparan skrin log bagi server aplikasi  Paparan skrin log bagi server pangkalan data |
| **(b)** | Adakah log server aplikasi dan serverpangkalan data (database) mempunyai maklumat berikut:   1. Alamat IP Pengguna? 2. Tarikh dan Masa Transaksi? |  |  |  |
| **(c)** | Adakah laporan log server aplikasi dan serverpangkalan data (database) boleh dijana dan diekstrak sendiri oleh agensi? |  |  |  | Paparan skrin urutan proses mengekstrak log server |
| **(d)** | Adakah laporan log server aplikasi dan serverpangkalan data (*database*) disemak bagi mengenalpasti capaian IP yang meragukan? |  |  |  |
| **4.** | **Kaedah Penyulitan Data (*Encryption*)**  Sistem aplikasi perakaunan dan kewangan menggunakan kaedah penyulitan (*encryption*) dan penyahsulitan (*decryption*) data bagi pemindahan data secara elektronik kepada/ daripada sistem pihak ketiga. | | | | | |
| **(a)** | Adakah fail disulitkan (encrypted) di dalam sistem aplikasi perakaunan dan kewangan sebelum dihantar ke bank bagi transaksi:   1. Data *Electronic Fund Transfer* (EFT)? 2. Data gaji?   Jika ya, nyatakan:   1. Kaedah penyulitan (encryption) 2. *Encryption tools* yang digunakan   Nota: Data EFT ialah data bagi semua pembayaran termasuk gaji yang dihantar dari sistem agensi ke bank utama.  Data gaji ialah perincian gaji bagi setiap pegawai yang dihantar dari sistem agensi ke bank/akaun gaji. |  |  |  | Paparan skrin urutan proses penyulitan data di sistem  Paparan skrin fail pembayaran EFT gaji dan lain-lain yang telah disulitkan (encrypted) |
| **(b)** | Adakah kaedah penyulitan (encryption) dan penyahsulitan (decryption) dilaksanakan untuk semua bank agensi yang melibatkan penghantaran fail EFT dan senarai penerima gaji? Nyatakan bilangan dan bank yang berkenaan. |  |  |  | Senarai bank yang melibatkan penghantaran fail EFT |
| **5.** | **Keselamatan Maklumat Dalam Rangkaian dan Infrastruktur ICT**  Sistem aplikasi perakaunan dan kewangan mestilah mempunyai ciri-ciri keselamatan berpandukan kepada Arahan Keselamatan, Arahan Teknologi Maklumat dan Dasar Keselamatan ICT yang berkuatkuasa dalam penyediaan rangkaian (LAN/WAN) serta infrastruktur ICT di Pusat Data dan Pusat Pemulihan Bencana. | | | | | |
| **(a)** | Adakah Pusat Data (DC) dan Pusat Pemulihan Bencana (DRC) ditempatkan di premis kerajaan dalam negara atau premis swasta yang mendapat pengesahan daripada Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO)?  Nyatakan lokasi:   1. Pusat Data (DC) 2. Pusat Pemulihan Bencana (DRC) |  |  |  | Surat Pengesahan daripada CGSO |
| **(b)** | Adakah *Network Diagram* mempunyai maklumat berikut:   1. Fizikal perkakasan yang terlibat dengan akses ke sistem aplikasi perakaunan dan kewangan (termasuk sistem yang berintegrasi) dan kemudahan sandaran data (backup facilities)? 2. Logikal diagram sekiranya perkakasan menggunakan pendekatan *virtual machines* (termasuk sistem yang berintegrasi) dan kemudahan sandaran data(backup facilities)? 3. *Network segmentation* (User Zone, DMZ Zone, Secure Zone)? 4. Capaian rangkaian dari cawangan/ subsidiari (yang mengakses ke sistem aplikasi perakaunan dan kewangan atau sistem yang berintegrasi - jika berkaitan)? 5. Pusat Data (DC) dan Pusat Pemulihan Bencana (DRC)? |  |  |  | *Network Diagram* |
| **(c)** | **Sila jawab soalan ini jika sistem aplikasi perakaunan dan kewangan berasaskan web (web-based):**   1. Adakah sistem aplikasi perakaunan dan kewangan dilengkapkan dengan *Secure Socket Layer* (SSL) dan algorithma yang digunakan adalah sekurang-kurangnya sha-2 (secure hash algorithm)? 2. Adakah sistem sokongan berasaskan web (web-based) yang berintegrasi dengan sistem aplikasi perakaunan dan kewangan (web-based) dilengkapkan dengan SSL?   **Sila jawab soalan ini jika sistem aplikasi perakaunan dan kewangan adalah berasaskan klien (client-based):**   1. Adakah capaian pengguna ke atas sistem aplikasi perakaunan dan kewangan dari luar kampus rangkaian agensi menggunakan *Virtual Private Network* (VPN) atau pendekatan lain yang setara? 2. Adakah sistem sokongan (web-based) yang berintegrasi dengan sistem aplikasi perakaunan dan kewangan (client-based) dilengkapkan dengan SSL? |  |  |  | Paparan skrin URL sistem di *browser*  Paparan skrin *SSL Certificate*  Paparan skrin *VPN Login*  Paparan skrin *SSL Certificate* |
| **6.** | **Penamatan Sesi Secara Automatik (Auto Logoff)**  Sistem aplikasi perakaunan dan kewangan mempunyai keupayaan untuk menamatkan aplikasi secara automatik (auto logoff) bagi pengguna tidak aktif (idle) selepas suatu tempoh masa yang ditetapkan. | | | | | |
| **(a)** | Adakah sistem aplikasi perakaunan dan kewangan mempunyai fungsi untuk menamatkan sesi secara automatik (auto logoff) sekiranya pengguna tidak aktif bagi sesuatu tempoh yang ditetapkan?  Jika ya, nyatakan tempoh penamatan sesi secara automatik (auto logoff) yang ditetapkan. |  |  |  | Paparan skrin penetapan *auto logoff*  Paparan skrin yang membuktikan *auto logoff* berfungsi mengikut tempoh yang ditetapkan |
| **(b)** | Adakah agensi berkeupayaan untuk menukar tetapan penamatan sesi secara automatik (auto logoff)? |  |  |  | Paparan skrin penetapan *auto logoff* |
| **(c)** | Adakah tempoh penamatan sesi secara automatik (auto logoff) dinyatakan dalam polisi agensi seperti Dokumen Keselamatan ICT (DKICT)? |  |  |  | Cabutan DKICT mengenai tempoh penamatan sesi secara automatik  Salinan polisi yang lain yang berkaitan |
| **7.** | **Sandaran Data (Backup) Dan Pengujian *Restore* Secara Berkala**  Aplikasi dan data bagi sistem perakaunan dan kewangan dibuat sandaran data (backup) secara berkala dan pengujian *restore* dilaksanakan sekurang-kurangnya satu (1) kali setahun serta didokumenkan. *Standard Operating Procedure* (SOP) hendaklah mengambil kira pengendalian keselamatan ke atas media sandaran data meliputi penyediaan, penghantaran, penyimpanan, penggunaan dan pelupusan termasuk data yang direplikasikan ke Pusat Pemulihan Bencana. | | | | | |
| **(a)** | Adakah agensi mempunyai *Standard Operating Procedure* (SOP) bagi pengendalian sandaran data (backup)dan *restore* untuk sistem aplikasi perakaunan dan kewangan? |  |  |  | SOP Sandaran Data (Backup) & *Restore*  Salinan Borang-Borang Permohonan  Carta Alir Sandaran Data (Backup) & *Restore* |
| **(b)** | Adakah *Standard Operating Procedure* (SOP) sandaran data (backup) mengandungi maklumat berikut:   * 1. Media sandaran data (backup) yang digunakan?   2. Kekerapan sandaran data (Contoh: harian, bulanan, tahunan)?   3. Kaedah sandaran data (Contoh: *incremental backup*, *full backup*, automatik, manual)?   4. Penempatan/ penyimpanan media sandaran data (backup) di lokasi luar premis?   5. Prosedur pengendalian media sandaran (backup) meliputi penyediaan, penghantaran, penyimpanan, penggunaan dan pelupusan dilaksanakan mengikut DKICT, Arahan Keselamatan, Arahan Teknologi Maklumat dan/ atau Akta Arkib Negara? |  |  |  |
| **(c)** | Adakah terdapat kemudahan sistem sandarandata (backup)yang menyokong dan melindungi sistem aplikasi perakaunan dan kewangan agensi? Nyatakan media sandaran (backup) yang digunakan.  Contoh media sandaran (backup):   1. *Network-Attached Storage* (NAS)/ *Storage Area Network* (SAN) 2. *Server Replication* 3. *Tape* 4. Lain-lain : *External Hard Disk*/ *Pendrive*/ CD/ Micro SD dan lain-lain (nyatakan) |  |  |  | Paparan skrin log backup |
| **(d)** | Adakah prosedur sandaran (backup) dibuat secara berkala? Nyatakan kekerapan pelaksanaan *backup.* (contoh: harian, mingguan atau bulanan). |  |  |  | Buku log sandaran data (backup) |
| **(e)** | Adakah salinan sandaran data (backup) disimpan di luar premis agensi dan lokasi merupakan premis Kerajaan? Nyatakan lokasi dan kekerapan penghantaran. |  |  |  | Gambar lokasi penyimpanan sandaran data (backup)  Buku log sandaran data (backup) |
| **(f)** | Adakah terdapat kawalan keselamatan ke atas pengendalian media sandaran (backup) di luar premis? Nyatakan.  Contoh:   1. Peti besi berkunci 2. Kawalan keselamatan lokasi penyimpanan 3. Pegawai bertanggungjawab 4. Rekod log aktiviti |  |  |  | Gambar peti besi berkunci  Gambar kawalan keselamatan lokasi penyimpanan media sandaran (backup)  Buku atau laporan log aktiviti |
| **(g)** | Adakah prosedur pengujian *restore* bagi semua media sandaran (backup) diuji sekurang-kurangnya satu (1) kali setahun? |  |  |  | Borang Permohonan Pengujian *Restore*  Laporan aktiviti *restore* |
| **(h)** | Adakah data kewangan sebelum dan selepas *restore* disemak dan disahkan oleh pegawai kewangan? |  |  |  | Imbangan Duga sebelum dan selepas *restore*  (di server produksi) yang mempunyai tarikh, masa dan telah disahkanoleh pegawai kewangan. |
| **8.** | **Pelan Pemulihan Bencana (*Disaster Recovery Plan*-DRP)**  Agensi Kerajaan mempunyai Pelan Pemulihan Bencana (DRP) bagi sistem aplikasi perakaunan dan kewangan, melaksanakan simulasi dan mengemas kini pelan sekurang-kurangnya satu (1) kali setahun serta didokumenkan. DRP hendaklah selari dengan Pelan Kesinambungan Perkhidmatan (PKP) Agensi Kerajaan (sekiranya ada). | | | | | |
| **(a)** | Adakah agensi mempunyai Pelan Pemulihan Bencana (DRP) untuk sistem aplikasi perakaunan dan kewangan? |  |  |  | *Disaster Recovery Plan (DRP)*. |
| **(b)** | Adakah Pelan Pemulihan Bencana (DRP) mempunyai maklumat berikut:   * 1. Struktur Organisasi Pasukan DRP (*DR Team*)?   2. Prosedur/ tatacara bagi tiga fasa minimum iaitu fasa normal (perlu mempunyai penerangan berkaitan strategi simulasi), fasa pemulihan bencana dan fasa selepas bencana?   3. *Recovery Point Objective* (RPO) yang sepadan dengan strategi *backup?*   4. *Recovery Time Objective* (RTO) yang sepadan dengan jumlah masa diambil dalam fasa pemulihan dan jenis DRC?   5. Maklumat lokasi dan jenis DRC sama ada *cold, warm atau hot?*   6. Strategi menangani kehilangan data?   Nota: Pelan ini bertujuan memastikan pemulihan bencana dapat dilakukan segera dengan kehilangan data yang minimum. |  |  |  |
| **(c)** | Adakah pengisytiharan bencana dilakukan oleh Ketua/ Timbalan Agensi? |  |  |  | DR Team |
| **(d)** | Adakah DRP diuji sekurang-kurangnya satu (1) kali setahun?  Nota : Sekiranya jenis DRC adalah ”Cold” dan tidak mempunyai perkakasan utama, simulasi DRP menggunakan *testing environment* di Pusat Data adalah dibenarkan.  Nota: Ada 3 jenis kategori DRC:   |  |  |  |  | | --- | --- | --- | --- | | **JENIS** | **PENERANGAN** | **KOS** | **RISIKO KEHILANGAN DATA** | | Hot | Real time (RTO/RPO)-lost data dalam 15minit – kedua-dua server bagi production dan DRC online pada masa yang sama | Tinggi | Rendah | | Warm | Server di DRC akan *up* apabila server di production *down.* | Sederhana | Sederhana | | Cold | pegawai perlu pergi ke lokasi untuk up server  secara manual apabila berlaku bencana. | Rendah | Tinggi | |  |  |  | Laporan Pengujian DRP  Notis Pengisytiharan Bencana  Notis Penamatan Bencana  Laporan Penilaian Bencana |
| **(e )** | Adakah laporan DRP mempunyai maklumat berikut:   1. Notis Pengisytiharan Bencana? 2. Notis Penamatan Bencana? 3. Laporan Penilaian Bencana? |  |  |  |
| **(f)** | Adakah tempoh sebenar RPO dan RTO semasa simulasi bersesuaian dengan tempoh yang dinyatakan dalam dokumen DRP? |  |  |  | Laporan perbandingan masa antara tempoh sebenar dengan tempoh yang dinyatakan dalam dokumen DRP |
| **(g)** | Adakah data kewangan sebelum dan selepas simulasi DRP disemak dan disahkan oleh pegawai kewangan? |  |  |  | Imbangan Duga sebelum dan selepas *restore* (di server produksi) yang mempunyai tarikh, masa dan telah disahkanoleh pegawai kewangan  Imbangan Dugaselepas *restore* yang **telah mempunyai transaksi** dan disahkan oleh pegawai kewangan. |

**Disediakan Oleh**:

Bahagian Teknologi Maklumat

………………………………………..

Nama :

Jawatan :

Tarikh :

**Disahkan Oleh**:

Bahagian Teknologi Maklumat

………………………………………..

Nama :

Jawatan :

Tarikh :