Lampiran 1 Rekomendasi Kontrol

Kelompok Kontrol pada NIST SP 800-53 rev.5

Dimana pada lampiran diidentifikasikan bahwa pada kelompok kontrol hanya terdapat kelompok yang direkomendasikan untuk risiko pada penelitian ini.

AC- *Access Control* (Kontrol Akses)

Access Control (AC) bertujuan untuk membatasi informasi, sistem, dan akses komponen untuk individu atau mesin yang dapat didentifikasi, diketahui, kredibel, dan berwenang.

- **AC-4: (Penegakan Arus Informasi),**
  Kontrol: Menegakkan otorisasi yang disetujui untuk mengontrol arus informasi di dalam
  sistem dan antara sistem yang terhubung berdasarkan [Tugas: ditentukan organisasi
  kebijakan pengendalian arus informasi].
  Pembahasan: *Information fLow control* mengatur kemana informasi dapat berjalan dalam suatu sistem dan antara sistem (berbeda dengan siapa yang diizinkan untuk mengakses informasi) dan tanpa memperhatikan akses selanjutnya ke informasi tersebut. Pembatasan kontrol aliran termasuk pemblokiran eksternal lalu lintas yang mengklaim berasal dari dalam organisasi, menyimpan informasi yang dikontrol ekspor dari ditransmisikan secara jelas ke *Internet*, membatasi permintaan *website* yang bukan dari *server proxy web internal*, dan membatasi transfer informasi antar organisasi berbasis pada struktur data dan konten. Mentransfer informasi antar organisasi mungkin memerlukan perjanjian yang menetapkan bagaimana arus informasi ditegakkan (lihat CA-3). Mentransfer informasi antara sistem dalam domain keamanan atau privasi yang berbeda dengan keamanan atau privasi yang berbeda kebijakan

menimbulkan risiko bahwa transfer tersebut melanggar satu atau beberapa keamanan atau privasi domain kebijakan. Dalam situasi seperti itu, pemilik/pelayan informasi memberikan panduan pada kebijakan yang ditentukan titik penegakan antara sistem yang terhubung. Penegakan meliputi melarang transfer informasi antara sistem yang terhubung (yaitu, mengizinkan akses saja), memverifikasi izin menulis sebelum menerima informasi dari keamanan atau privasi lain domain atau sistem yang terhubung, menggunakan mekanisme perangkat keras untuk menegakkan informasi satu arah mengalir, dan menerapkan mekanisme *regrading* yang dapat dipercaya untuk menetapkan kembali keamanan atau privasi atribut dan label.

Organisasi umumnya menggunakan kebijakan kontrol arus informasi dan mekanisme penegakan untuk mengontrol aliran informasi antara sumber dan tujuan yang ditunjuk dalam sistem dan antara sistem yang terhubung. *FLow control* didasarkan pada karakteristik informasi dan/atau jalur informasi. Penegakan terjadi, misalnya, di perangkat perlindungan batas yang menggunakan kumpulan aturan atau menetapkan setelan konfigurasi yang membatasi layanan sistem, menyediakan kemampuan penyaringan paket berdasarkan informasi header, atau menyediakan kemampuan penyaringan pesan berdasarkan isi pesan. Organisasi juga mempertimbangkan kelayakan penyaringan dan/atau mekanisme inspeksi (yaitu komponen perangkat keras, *firmware*, dan perangkat lunak) yang sangat penting untuk penegakan arus informasi. Penyempurnaan kontrol 3 hingga 32 terutama menangani kebutuhan solusi lintas domain yang berfokus pada teknik pemfilteran yang lebih canggih, analisis mendalam, dan mekanisme penegakan aliran yang lebih kuat diterapkan dalam produk lintas domain, seperti penjaga jaminan tinggi. Kemampuan seperti itu umumnya tidak tersedia secara komersial produk. Penegakan aliran informasi juga berlaku untuk mengontrol lalu lintas pesawat (mis., Perutean dan DNS).

Kontrol Terkait: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24 , SA-17, SC-4, SC-7, SC-16, SC-31

- **AC-9 (Pemberitahuan Logon Sebelumnya),**

  Kontrol: Beri tahu pengguna, setelah berhasil masuk ke sistem, tanggal dan waktu terakhir *logon*.

  Pembahasan: Pemberitahuan *logon* sebelumnya berlaku untuk akses sistem melalui antarmuka pengguna manusia dan akses ke sistem yang terjadi pada jenis arsitektur lainnya. Informasi tentang yang terakhir berhasil logon memungkinkan pengguna untuk mengenali jika tanggal dan waktu yang diberikan tidak konsisten dengan akses terakhir pengguna.

  Kontrol Terkait: AC-7, PL-4.

AT- *Awareness and Training* (Kesadaran dan Pelatihan)

Awareness and Training (AT) bertujuan untuk memastikan bahwa personil organisasi dilatih secara memadai untuk melaksanakan tugas-tugas yang berhubungan dengan keamanan informasi ditugaskan mereka dan tanggung jawab.

- **AT- 2(2) (Ancaman Orang Dalam),**

  (2) PELATIHAN DAN KESADARAN LITERASI | ANCAMAN DALAM

  Kontrol:

  Berikan pelatihan literasi tentang mengenali dan melaporkan indikator potensi ancaman orang dalam.

  Pembahasan: Indikator potensial dan kemungkinan prekursor ancaman orang dalam dapat mencakup perilaku seperti ketidakpuasan kerja jangka panjang yang berlebihan; upaya untuk mendapatkan akses ke informasi yang tidak diperlukan untuk kinerja pekerjaan; akses yang tidak dapat dijelaskan ke sumber daya keuangan; intimidasi atau pelecehan terhadap sesama karyawan; kekerasan di tempat kerja; dan pelanggaran berat lainnya kebijakan, prosedur, arahan, peraturan, aturan, atau praktik.

Pelatihan literasi meliputi bagaimana mengomunikasikan kekhawatiran karyawan dan manajemen mengenai potensi indikator ancaman orang dalam melalui saluran yang ditetapkan oleh organisasi dan di sesuai dengan kebijakan dan prosedur yang telah ditetapkan. Organisasi dapat mempertimbangkan untuk menyesuaikan topik kesadaran ancaman orang dalam untuk peran tersebut. Misalnya, pelatihan untuk manajer mungkin berfokus pada perubahan perilaku anggota tim, sedangkan pelatihan untuk karyawan mungkin berfokus pada pengamatan yang lebih umum

Kontrol Terkait: PM-12

- **AT-3(1) (Kontrol Lingkungan)**

  Kontrol:

  A. Kembangkan, dokumentasikan, dan sebarkan ke [Tugas: personel atau peran yang ditetapkan organisasi]:

     1. [Pilihan (satu atau lebih): Tingkat organisasi; Tingkat misi/proses bisnis; Tingkat sistem] kesadaran dan kebijakan pelatihan yang:

        (a) Membahas tujuan, ruang lingkup, peran, tanggung jawab, komitmen manajemen, koordinasi antar entitas organisasi, dan kepatuhan; Dan

        (b) Konsisten dengan undang-undang yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, dan pedoman; Dan

     2. Prosedur untuk memfasilitasi implementasi kebijakan kesadaran dan pelatihan dan kontrol kesadaran dan pelatihan terkait;

  B. Tunjuk [Tugas: pejabat yang ditentukan organisasi] untuk mengelola pengembangan, dokumentasi, dan diseminasi kebijakan dan prosedur penyadaran dan pelatihan; Dan

  C. Tinjau dan perbarui kesadaran dan pelatihan saat ini:

1. Kebijakan [Penugasan: frekuensi yang ditentukan organisasi] dan mengikuti [Penugasan: acara yang ditentukan organisasi]; Dan
2. Prosedur [Tugas: frekuensi yang ditentukan organisasi] dan mengikuti [Tugas: acara yang ditentukan organisasi].

Pembahasan: Kebijakan dan prosedur kesadaran dan pelatihan mengatasi kontrol dalam keluarga AT yang diimplementasikan dalam sistem dan organisasi. Strategi manajemen risiko adalah faktor penting dalam menetapkan kebijakan dan prosedur tersebut. Kebijakan dan prosedur berkontribusi untuk jaminan keamanan dan privasi. Oleh karena itu, penting untuk program keamanan dan privasi berkolaborasi dalam pengembangan kebijakan dan prosedur kesadaran dan pelatihan. Keamanan dan kebijakan dan prosedur program privasi di tingkat organisasi lebih disukai, secara umum, dan dapat meniadakan kebutuhan akan kebijakan dan prosedur khusus misi atau sistem. Kebijakannya bisa dimasukkan sebagai bagian dari kebijakan keamanan dan privasi umum atau diwakili oleh beberapa kebijakan yang mencerminkan sifat kompleks organisasi. Prosedur dapat ditetapkan untuk keamanan dan program privasi, untuk misi atau proses bisnis, dan untuk sistem, jika diperlukan. Prosedur menggambarkan bagaimana kebijakan atau kontrol diimplementasikan dan dapat diarahkan pada individu atau peran yang menjadi objek dari prosedur. Prosedur dapat didokumentasikan dalam keamanan sistem dan rencana privasi atau dalam satu atau lebih dokumen terpisah. Peristiwa yang dapat memicu pembaruan ke kebijakan dan prosedur kesadaran dan pelatihan termasuk penilaian atau temuan audit, keamanan insiden atau pelanggaran, atau perubahan dalam undang-undang yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, dan pedoman. Hanya menyatakan kembali kontrol bukan merupakan suatu kebijakan atau prosedur organisasi.

Kontrol Terkait: PM-9, PS-8, SI-12.

CP- *Contingency Planning* (Perencanaan kontingensi)

Contingency Planning (CP) Perencanaan kontingenci bertujuan membangun, memelihara, dan secara efektif melaksanakan rencana untuk tanggap darurat, operasi *backup*, dan *recovery* pasca bencana untuk sistem informasi organisasi untuk memastikan ketersediaan informasi penting sumber daya dan kelangsungan operasi dalam situasi darurat.

- **CP-9(5) (Transfer ke Situs Penyimpanan Alternatif)**
  (5) PENCADANGAN SISTEM | TRANSFER KE SITUS PENYIMPANAN ALTERNATIF
  Kontrol: Mentransfer informasi cadangan sistem ke situs penyimpanan alternatif [Tugas: periode waktu yang ditentukan organisasi dan kecepatan transfer yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].
  Pembahasan: Informasi cadangan sistem juga dapat ditransfer ke situs penyimpanan alternatif secara elektronik atau dengan pengiriman fisik media penyimpanan.
  Kontrol Terkait: CP-7, MP-3, MP-4, MP-5

- **CP-9(8) (Perlindungan Kriptografi)**
  (8) PENCADANGAN SISTEM | PERLINDUNGAN KRIPTOGRAFI
  Kontrol: Terapkan mekanisme kriptografi untuk mencegah pengungkapan yang tidak sah dan modifikasi [Penugasan: informasi cadangan yang ditentukan organisasi].
  Pembahasan: Pemilihan mekanisme kriptografi didasarkan pada kebutuhan untuk melindungi kerahasiaan dan integritas informasi cadangan. Kekuatan mekanisme yang dipilih adalah sepadan dengan kategori keamanan atau klasifikasi informasi. Kriptografi perlindungan berlaku untuk informasi cadangan sistem dalam penyimpanan baik di primer maupun alternatif lokasi. Organisasi yang menerapkan mekanisme kriptografi untuk melindungi informasi saat istirahat juga pertimbangkan solusi manajemen kunci kriptografi.

Kontrol Terkait: SC-12, SC-13, SC-28.

- **CP-10 (Pemulihan dan Rekonstitusi Sistem),**
  Kontrol:
  Menyediakan pemulihan dan pemulihan sistem ke keadaan yang diketahui di dalamnya [Penugasan: periode waktu yang ditentukan organisasi konsisten dengan waktu pemulihan dan titik pemulihan tujuan] setelah gangguan, kompromi, atau kegagalan.
  Pembahasan: *Recovery* adalah pelaksanaan kegiatan *contingency plan* untuk mengembalikan misi organisasi dan fungsi bisnis. Rekonstitusi terjadi setelah pemulihan dan termasuk kegiatan untuk mengembalikan sistem ke keadaan operasional penuh. Operasi pemulihan dan rekonstitusi mencerminkan misi dan prioritas bisnis; titik pemulihan, waktu pemulihan, dan tujuan rekonstitusi; Dan metrik organisasi yang konsisten dengan persyaratan rencana darurat. Rekonstitusi meliputi penonaktifan kemampuan sistem sementara yang mungkin diperlukan selama pemulihan operasi. Rekonstitusi juga mencakup penilaian kemampuan sistem yang dipulihkan sepenuhnya, pembentukan kembali kegiatan pemantauan berkelanjutan, otorisasi ulang sistem (jika diperlukan), dan kegiatan untuk mempersiapkan sistem dan organisasi untuk gangguan, pelanggaran, kompromi, atau kegagalan. Kemampuan pemulihan dan pemulihan dapat mencakup mekanisme otomatis dan prosedur manual. Organisasi menetapkan tujuan waktu pemulihan dan titik pemulihan sebagai bagian dari perencanaan kontinjensi.
  Kontrol Terkait: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13

IA- ***Identification and Authentication*** **(Identifikasi dan Otentikasi)**

Identification and Authentication (IA) bertujuan memberikan Semua pengguna sistem diidentifikasi dan dikonfirmasi di sesuai dengan kebijakan keamanan informasi.

- **IA-2 (*Identification and Authentication (Organizational Users*));**

  Kontrol:

  Secara unik mengidentifikasi dan mengautentikasi pengguna organisasi dan mengaitkannya dengan unik identifikasi dengan proses yang bertindak atas nama pengguna tersebut.

  Pembahasan: Organisasi dapat memenuhi persyaratan identifikasi dan autentikasi dengan memenuhi persyaratan dalam [HSPD 12]. Pengguna organisasi termasuk karyawan atau individu yang organisasi anggap memiliki status setara dengan karyawan (misalnya, kontraktor dan peneliti tamu). Identifikasi unik dan autentikasi pengguna berlaku untuk semua akses selain yang secara eksplisit diidentifikasi dalam AC-14 dan yang terjadi melalui penggunaan resmi autentikator grup tanpa autentikasi individual. Sejak proses mengeksekusi atas nama kelompok dan peran, organisasi mungkin memerlukan identifikasi unik individu dalam rekening kelompok atau untuk akuntabilitas rinci aktivitas individu.

  Organisasi menggunakan kata sandi, autentikator fisik, atau biometrik untuk mengautentikasi pengguna identitas atau, dalam kasus otentikasi multi-faktor, beberapa kombinasinya. Akses ke sistem organisasi didefinisikan sebagai akses lokal atau akses jaringan. Akses lokal adalah apa saja akses ke sistem organisasi oleh pengguna atau proses yang bertindak atas nama pengguna, di mana akses berada diperoleh melalui koneksi langsung tanpa menggunakan jaringan. Akses jaringan adalah akses ke sistem organisasi oleh pengguna (atau proses yang bertindak atas nama pengguna) di mana akses diperoleh melalui koneksi jaringan (yaitu, akses nonlokal). Akses jarak jauh adalah jenis akses jaringan yang melibatkan komunikasi melalui jaringan eksternal. Jaringan internal mencakup area lokal jaringan dan jaringan area luas.

  Penggunaan jaringan pribadi virtual terenkripsi untuk koneksi jaringan antara titik akhir yang dikontrol organisasi dan titik akhir yang tidak dikontrol organisasi dapat diperlakukan sebagai internal jaringan sehubungan dengan melindungi kerahasiaan dan integritas informasi

melintasi jaringan. Persyaratan identifikasi dan autentikasi untuk pengguna non-organisasi adalah dijelaskan dalam IA-8.

Kontrol Terkait: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4 , MA 5, PE-2, PL-4, SA-4, SA-8.

- **IA-5(1)(a) (Otentikasi berbasis kata sandi);**

  (1) MANAJEMEN OTENTIK | AUTENTIKASI BERBASIS *PASSWORD*

  Untuk autentikasi berbasis kata sandi:

  (a) Memelihara daftar kata sandi yang umum digunakan, diharapkan, atau disusupi dan pembaruan daftar [Tugas: frekuensi yang ditentukan organisasi] dan saat organisasi kata sandi diduga telah disusupi secara langsung atau tidak langsung;

  (b) Memverifikasi, saat pengguna membuat atau memperbarui kata sandi, bahwa kata sandi tidak ditemukan daftar kata sandi yang umum digunakan, diharapkan, atau disusupi dalam IA-5(1)(a);

  (c) Mengirimkan kata sandi hanya melalui saluran yang dilindungi secara kriptografis;

  (d) Simpan kata sandi menggunakan fungsi derivasi kunci asin yang disetujui, sebaiknya menggunakan kunci hash;

  (e) Membutuhkan pemilihan kata sandi baru setelah pemulihan akun;

  (f) Izinkan pengguna memilih kata sandi dan frasa sandi yang panjang, termasuk spasi dan semuanya karakter yang dapat dicetak;

  (g) Menggunakan alat otomatis untuk membantu pengguna dalam memilih kata sandi yang kuat autentikator; Dan

  (h) Menerapkan aturan komposisi dan kompleksitas berikut: [Penugasan: aturan komposisi dan kompleksitas yang ditentukan organisasi].

  Pembahasan: Otentikasi berbasis kata sandi berlaku untuk kata sandi terlepas dari apakah itu digunakan dalam autentikasi satu faktor atau multi faktor. Kata sandi atau frasa sandi yang panjang adalah lebih disukai daripada kata sandi yang lebih pendek. Aturan komposisi yang dipaksakan memberikan keamanan marjinal manfaat sementara mengurangi kegunaan. Namun, organisasi dapat memilih untuk menetapkan tertentu aturan untuk

pembuatan kata sandi (mis., panjang karakter minimum untuk kata sandi yang panjang) di bawah keadaan tertentu dan dapat menegakkan persyaratan ini dalam IA-5(1)(h). Pemulihan akun bisa terjadi, misalnya, dalam situasi ketika kata sandi dilupakan. Dilindungi secara kriptografis kata sandi termasuk hash kriptografis asin satu arah dari kata sandi. Daftar umumnya kata sandi yang digunakan, disusupi, atau diharapkan termasuk kata sandi yang diperoleh dari sebelumnya korpus pelanggaran, kata-kata kamus, dan karakter berulang atau berurutan. Daftarnya termasuk kata-kata khusus konteks, seperti nama layanan, nama pengguna, dan turunannya.

Kontrol Terkait: IA-6

IR- ***Incident Response*** **(Tanggapan Insiden)**

Incident Respons (IR) Tanggapan inside bertujuan memberikan *track*, dokumen, dan laporan insiden untuk tepat pejabat organisasi dan / atau kewenangan.

- **IR-4 (Penanganan Insiden);**

  Kontrol:

  A. Menerapkan kemampuan penanganan insiden untuk insiden yang konsisten dengan insiden tersebut rencana respon dan termasuk persiapan, deteksi dan analisis, penahanan, pemberantasan, dan pemulihan;

  B. Mengkoordinasikan kegiatan penanganan insiden dengan kegiatan perencanaan kontinjensi;

  C. Menggabungkan pembelajaran dari aktivitas penanganan insiden yang sedang berlangsung ke dalam respons insiden prosedur, pelatihan, dan pengujian, dan mengimplementasikan perubahan yang dihasilkan sesuai; Dan

  D. Pastikan ketelitian, intensitas, ruang lingkup, dan hasil kegiatan penanganan insiden sebanding dan dapat diprediksi di seluruh organisasi.

Pembahasan: Organisasi menyadari bahwa kemampuan respons insiden bergantung pada
kemampuan sistem organisasi dan misi serta proses bisnis yang didukung oleh sistem tersebut. Organisasi menganggap respons insiden sebagai bagian dari definisi, desain, dan pengembangan misi dan proses bisnis dan sistem. Informasi terkait insiden dapat diperoleh dari berbagai sumber, termasuk pemantauan audit, pemantauan akses fisik, dan pemantauan jaringan; laporan pengguna atau administrator; dan melaporkan peristiwa rantai pasokan. Sebuah kemampuan penanganan insiden yang efektif mencakup koordinasi di antara banyak entitas organisasi (misalnya, pemilik misi atau bisnis, pemilik sistem, pejabat yang berwenang, kantor sumber daya manusia, kantor keamanan fisik, kantor keamanan personel, departemen hukum, [fungsi] eksekutif risiko, personel operasi, kantor pengadaan). Insiden keamanan yang dicurigai termasuk penerimaan komunikasi email mencurigakan yang dapat berisi kode berbahaya. Rantai pasokan yang dicurigai insiden termasuk penyisipan perangkat keras palsu atau kode berbahaya ke dalam organisasi sistem atau komponen sistem. Untuk agen federal, insiden yang melibatkan pribadi informasi yang dapat diidentifikasi dianggap sebagai pelanggaran. Pelanggaran menghasilkan pengungkapan yang tidak sah, yaitu kehilangan kendali, akuisisi yang tidak sah, kompromi, atau kejadian serupa di mana seseorang selain pengguna yang berwenang mengakses atau berpotensi mengakses identitas pribadi informasi atau pengguna yang berwenang mengakses atau berpotensi mengakses informasi tersebut untuk orang lain dari tujuan yang diizinkan.

Kontrol Terkait: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8 , PE-6, PL 2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

MA- *Maintenance* (Pemeliharaan)

Maintenance (MA) Pemeliharaan bertujuan melakukan perawatan berkala dan tepat waktu pada sistem informasi organisasi dan memberikan kontrol yang efektif pada alat, teknik, mekanisme, dan personil digunakan untuk melakukan sistem informasi pemeliharaan.

- **MA-1 (Kebijakan dan Prosedur),**

  Kontrol:

  A. Mengembangkan, mendokumentasikan, dan menyebarluaskan ke [Tugas: personel yang ditentukan organisasi atau peran]:
     1. [Pilihan (satu atau lebih): Tingkat organisasi; Tingkat misi/proses bisnis; Tingkat sistem] kebijakan pemeliharaan yang:
        (a) Membahas tujuan, ruang lingkup, peran, tanggung jawab, komitmen manajemen, koordinasi antar entitas organisasi, dan kepatuhan; Dan
        (b) Konsisten dengan undang-undang yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, dan pedoman; Dan
     2. Prosedur untuk memfasilitasi pelaksanaan kebijakan pemeliharaan dan kontrol pemeliharaan terkait;

  B. Tunjuk [Tugas: pejabat yang ditentukan organisasi] untuk mengelola pengembangan, dokumentasi, dan sosialisasi kebijakan dan prosedur pemeliharaan; Dan

  C. Tinjau dan perbarui pemeliharaan saat ini:
     1. Kebijakan [Penugasan: frekuensi yang ditentukan organisasi] dan mengikuti [Penugasan: acara yang ditentukan organisasi]; Dan
     2. Prosedur [Tugas: frekuensi yang ditentukan organisasi] dan mengikuti [Tugas: acara yang ditentukan organisasi].

  Pembahasan: Kebijakan dan prosedur perawatan membahas kontrol dalam keluarga MA yang ada diimplementasikan dalam sistem dan organisasi. Strategi manajemen risiko adalah penting faktor dalam menetapkan kebijakan dan prosedur tersebut. Kebijakan dan prosedur

berkontribusi pada keamanan dan jaminan privasi. Oleh karena itu, program keamanan dan privasi harus berkolaborasi pada pengembangan kebijakan dan prosedur pemeliharaan. Program keamanan dan privasi kebijakan dan prosedur di tingkat organisasi lebih disukai, secara umum, dan dapat meniadakan kebutuhan akan kebijakan dan prosedur khusus misi atau sistem. Kebijakan tersebut dapat dimasukkan sebagai bagian dari kebijakan keamanan dan privasi umum atau diwakili oleh beberapa kebijakan yang mencerminkan sifat organisasi yang kompleks. Prosedur dapat ditetapkan untuk keamanan dan privasi program, untuk misi atau proses bisnis, dan untuk sistem, jika diperlukan. Prosedur menjelaskan bagaimana kebijakan atau kontrol tersebut diimplementasikan dan dapat diarahkan pada individu atau peran yang ada obyek prosedur. Prosedur dapat didokumentasikan dalam keamanan sistem dan rencana privasi atau dalam satu atau lebih dokumen terpisah. Peristiwa yang dapat memicu pembaruan untuk pemeliharaan penilaian kebijakan dan prosedur atau temuan audit, insiden atau pelanggaran keamanan, atau perubahan dalam hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, dan pedoman. Hanya menyatakan kembali kontrol bukan merupakan kebijakan atau prosedur organisasi.

Kontrol Terkait: PM-9, PS-8, SI-12

PE- ***Physical and Environmental Protection*** **(Perlindungan Fisik dan Lingkungan)**

Physical and Environmental (PE) Lingkungan fisik bertujuan mengintegrasikan perlindungan fisik dan keamanan informasi mekanisme untuk memastikan perlindungan yang teat dari informasi organisasi sumber.

- **PE-9 (Peralatan Listrik dan Kabel),**

  Kontrol: Lindungi peralatan listrik dan kabel listrik untuk sistem dari kerusakan dan penghancuran.

Pembahasan: Organisasi menentukan jenis perlindungan yang diperlukan untuk peralatan listrik dan pemasangan kabel yang digunakan di lokasi berbeda yang bersifat internal dan eksternal organisasi fasilitas dan lingkungan operasi. Jenis peralatan listrik dan kabel termasuk internal kabel dan sumber daya tak terputus di kantor atau pusat data, generator dan listrik pemasangan kabel di luar gedung, dan sumber daya untuk komponen mandiri seperti satelit, kendaraan, dan sistem lain yang dapat digunakan.

Kontrol Terkait: PE-4

- **PE-11 (Daya Darurat),**

  Kontrol:

  Gunakan dan pertahankan pencahayaan darurat otomatis untuk sistem yang aktif terjadi pemadaman listrik atau gangguan dan yang mencakup pintu keluar darurat dan jalur evakuasi dalam fasilitas.

  Pembahasan: Ketentuan penerangan darurat berlaku terutama untuk fasilitas organisasi yang berisi konsentrasi sumber daya sistem, termasuk pusat data, ruang *server*, dan ruang komputer *mainframe*. Ketentuan pencahayaan darurat untuk sistem dijelaskan dalam rencana darurat untuk organisasi. Jika penerangan darurat untuk sistem gagal atau tidak bisa asalkan, organisasi mempertimbangkan situs pemrosesan alternatif untuk kontinjensi terkait daya.

  Kontrol Terkait: CP-2, CP-7.

- **PE-14 (Kontrol Lingkungan),**

  Kontrol:

  A. Pertahankan [Pilihan (satu atau lebih): suhu; kelembaban; tekanan; radiasi; [Penugasan: pengendalian lingkungan yang ditentukan organisasi]] tingkat dalam fasilitas di mana sistem berada di [Tugas: tingkat yang dapat diterima yang ditentukan organisasi]; Dan

  B. Pantau tingkat kontrol lingkungan [Tugas: frekuensi yang ditentukan organisasi].

Pembahasan: Ketentuan pengendalian lingkungan berlaku terutama untuk fasilitas organisasi yang mengandung konsentrasi sumber daya sistem (misalnya, pusat data, ruang komputer mainframe, dan ruang *server*). Kontrol lingkungan yang tidak memadai, terutama di lingkungan yang sangat keras, dapat memiliki dampak merugikan yang signifikan terhadap ketersediaan sistem dan komponen sistem yang diperlukan untuk mendukung misi organisasi dan fungsi bisnis.

Kontrol Terkait: AT-3, CP-2.

- **PE-17 (Tempat Kerja Alternatif),**

  Kontrol:

  A. Tentukan dan dokumentasikan [Tugas: situs kerja alternatif yang ditentukan organisasi] diizinkan untuk digunakan oleh karyawan;
  B. Terapkan kontrol berikut di lokasi kerja alternatif: [Tugas: ditentukan organisasi kontrol];
  C. Menilai efektivitas kontrol di lokasi kerja alternatif; Dan
  D. Menyediakan sarana bagi karyawan untuk berkomunikasi dengan keamanan informasi dan privasi personil jika terjadi insiden.

  Pembahasan: Lokasi kerja alternatif termasuk fasilitas pemerintah atau tempat tinggal pribadi karyawan. Meskipun berbeda dari lokasi pemrosesan alternatif, lokasi kerja alternatif dapat disediakan lokasi alternatif yang tersedia selama operasi kontinjensi. Organisasi dapat menentukan set kontrol yang berbeda untuk situs kerja alternatif tertentu atau jenis situs tergantung pada kegiatan terkait pekerjaan yang dilakukan di lokasi. Menerapkan dan menilai efektivitas dari kontrol yang ditentukan organisasi dan menyediakan sarana untuk mengomunikasikan insiden pada pekerjaan alternatif situs mendukung kegiatan perencanaan kontinjensi organisasi.

  Kontrol Terkait: AC-17, AC-18, CP-7

- **PE-20 (Pemantauan dan Pelacakan Aset),**

  Kontrol: Mempekerjakan [Penugasan: teknologi lokasi aset yang ditentukan organisasi] untuk melacak dan memantau lokasi dan pergerakan [Tugas: aset yang ditentukan organisasi] di dalam [Penugasan: area terkontrol yang ditentukan organisasi].

  Pembahasan: Teknologi lokasi aset dapat membantu memastikan bahwa aset penting—termasuk kendaraan, peralatan, dan komponen sistem—tetap berada di lokasi resmi. Organisasi berkonsultasi dengan Kantor Penasihat Umum dan pejabat agensi senior untuk privasi terkait penempatan dan penggunaan teknologi lokasi aset untuk mengatasi potensi masalah privasi.

  Kontrol Terkait: CM-8, PE-16, PM-8

PS- *Personnel Security* (Keamanan Personil)

Personnel Security (PS) Keamanan personal bertujuan memastikan bahwa individu menempati posisi tanggung jawab dalam organisasi dapat dipercaya dan gemenuhi keamanan didirikan kriteria untuk posisi tersebut.

- **PS-3 (Penyaringan Personil),**

  Kontrol:

  A. Saring individu sebelum mengizinkan akses ke sistem; Dan
  B. Saring ulang individu sesuai dengan [Tugas: kondisi yang ditentukan organisasi membutuhkan penyaringan ulang dan, jika penyaringan ulang diindikasikan, frekuensi penyaringan ulang].

  Pembahasan: Kegiatan penyaringan dan penyaringan ulang personel mencerminkan undang-undang yang berlaku, eksekutif perintah, arahan, peraturan, kebijakan, standar, pedoman, dan kriteria khusus yang ditetapkan untuk penunjukan risiko dari posisi yang ditugaskan. Contoh penyaringan personel termasuk latar belakang investigasi dan pemeriksaan agen. Organisasi dapat menentukan ketentuan penyaringan ulang yang

berbeda dan frekuensi untuk personel yang mengakses sistem berdasarkan jenis informasi yang diproses, disimpan, atau ditransmisikan oleh sistem.
Kontrol Terkait: AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

RA- *Risk Assessment* (Penilaian Risiko)

Risk Assessnent (RA) Penilaian resiko bertujuan menilai berkala risiko untuk operasi organisasi (Termasuk misi, fungsi, gambar, atau reputasi), set organisasi, dan individu yang dihasilkan dari pengoperasian sistem informasi organisasi.

- **RA-3 (*Risk Assessment*),**
  Kontrol:
  A. Melakukan penilaian risiko, antara lain:
     1. Mengidentifikasi ancaman dan kerentanan dalam sistem;
     2. Menentukan kemungkinan dan besarnya bahaya dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran sistem, informasi itu memproses, menyimpan, atau mentransmisikan, dan informasi terkait lainnya; Dan
     3. Menentukan kemungkinan dan dampak dari efek merugikan pada individu yang timbul dari pemrosesan informasi identitas pribadi;
  B. Mengintegrasikan hasil penilaian risiko dan keputusan manajemen risiko dari organisasi dan perspektif misi atau proses bisnis dengan penilaian risiko tingkat sistem;
  C. Hasil penilaian risiko dokumen di [Pilihan: rencana keamanan dan privasi; tugas beresiko laporan; [Tugas: dokumen yang ditentukan organisasi]];
  D. Meninjau hasil penilaian risiko [Penugasan: frekuensi yang ditentukan organisasi];
  E. Menyebarluaskan hasil penilaian risiko ke [Penugasan: personel yang ditentukan organisasi atauperan]; Dan

F. Perbarui penilaian risiko [Penugasan: frekuensi yang ditentukan organisasi] atau bila ada perubahan signifikan pada sistem, lingkungan operasinya, atau kondisi lain yang mungkin memengaruhi status keamanan atau privasi sistem.

Pembahasan: Penilaian risiko mempertimbangkan ancaman, kerentanan, kemungkinan, dan dampak terhadap operasi organisasi dan aset, individu, organisasi lain, dan Bangsa. Mempertaruhkan penilaian juga mempertimbangkan risiko dari pihak eksternal, termasuk kontraktor yang mengoperasikan system atas nama organisasi, individu yang mengakses sistem organisasi, penyedia layanan, dan entitas outsourcing. Organisasi dapat melakukan penilaian risiko pada ketiga tingkat dalam hierarki manajemen risiko (yaitu, tingkat organisasi, tingkat misi/proses bisnis, atau tingkat sistem informasi) dan di mana saja tahap dalam siklus hidup pengembangan sistem. Penilaian risiko juga dapat dilakukan di berbagai langkah-langkah dalam Kerangka Manajemen Risiko, termasuk persiapan, kategorisasi, seleksi kontrol, implementasi kontrol, penilaian kontrol, otorisasi, dan pemantauan kontrol. Penilaian risiko adalah aktivitas berkelanjutan yang dilakukan sepanjang siklus hidup pengembangan sistem. Penilaian risiko juga dapat menangani informasi yang terkait dengan sistem, termasuk desain sistem, tujuan penggunaan sistem, hasil pengujian, dan informasi atau artefak terkait rantai suplai.

Kontrol Terkait: CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL10, PL-11, PM-8, PM-9, PM-28, PT-2, PT-7, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12.

SC- *System and Communications Protection* (Perlindungan Sistem dan Komunikasi)

System and Communications Protection (SC) Perlindungan sistem dan komunikasi bertujuan mengalokasikan sumber daya yang cukup untuk melindungi memadaiinfrastruktur informasi elektronik.

- **SC-10 (Putus Jaringan),**

  Kontrol:

  Mengakhiri koneksi jaringan yang terkait dengan sesi komunikasi di akhir sesi atau setelah [Tugas: periode waktu yang ditentukan organisasi] tidak aktif.

  Pembahasan: Pemutusan jaringan berlaku untuk jaringan internal dan eksternal. Mengakhiri jaringan koneksi yang terkait dengan sesi komunikasi tertentu termasuk pengalokasian *TCP/IP* pasangan alamat atau port pada tingkat sistem operasi dan de-alokasi penugasan jaringan di tingkat aplikasi jika beberapa sesi aplikasi menggunakan satu tingkat sistem operasi koneksi jaringan. Periode tidak aktif dapat ditetapkan oleh organisasi dan termasuk waktu periode berdasarkan jenis akses jaringan atau untuk akses jaringan tertentu.

  Kontrol Terkait: AC-17, SC-23

SI- *System and Information Integrity* (Integritas Sistem dan Informasi)

System and Information Integrity (SI) Integritas sistem dan informasi bertujuan memberikan perlindungan dari kode berbahaya di tepat lokasi dalam sistem informasi organisasi, memonitor sistem informasi peringatan keamanan dan nasihat, dan mengambil tindakan yang tepat dalam menanggapi.

- **SI-2(5) (Pembaruan Perangkat Lunak dan Firmware Otomatis),**

  (5) PERBAIKAN CACAT | PEMBARUAN PERANGKAT LUNAK DAN FIRMWARE OTOMATIS.

  Kontrol: Instal [Tugas: perangkat lunak dan firmware terkait keamanan yang ditentukan organisasi pembaruan] secara otomatis ke [Penugasan: komponen sistem yang ditentukan organisasi].

  Pembahasan: Karena masalah integritas dan ketersediaan sistem, organisasi mempertimbangkan metodologi yang digunakan untuk melakukan pembaruan otomatis. Organisasi menyeimbangkan kebutuhan untuk memastikan bahwa pembaruan diinstal sesegera mungkin dengan

kebutuhan pemeliharaan manajemen konfigurasi dan kontrol dengan misi atau dampak operasional apa pun yang pembaruan otomatis mungkin memaksakan.

Kontrol Terkait: Tidak ada

- **SI-3 (Perlindungan Kode Berbahaya),**

  Kontrol:

  A. Terapkan [Pilihan (satu atau lebih): berdasarkan tanda tangan; kode berbahaya] berbasis non-tanda tangan mekanisme perlindungan pada titik masuk dan keluar sistem untuk mendeteksi dan memberantas berbahaya kode;

  B. Secara otomatis memperbarui mekanisme perlindungan kode berbahaya saat rilis baru tersedia sesuai dengan kebijakan dan prosedur manajemen konfigurasi organisasi;

  C. Konfigurasikan mekanisme perlindungan kode berbahaya untuk:

     1. Lakukan pemindaian sistem secara berkala [Penugasan: frekuensi yang ditentukan organisasi] dan pemindaian file secara real-time dari sumber eksternal di [Pilihan (satu atau lebih): titik akhir; titik masuk dan keluar jaringan] saat file diunduh, dibuka, atau dieksekusi disesuai dengan kebijakan organisasi; Dan
     2. [Pilihan (satu atau lebih): blokir kode berbahaya; kode berbahaya karantina; mengambil [Tugas: tindakan yang ditentukan organisasi]]; dan kirim peringatan ke [Penugasan: personel atau peran yang ditentukan organisasi] sebagai respons terhadap deteksi kode berbahaya; Dan

  D. Mengatasi penerimaan positif palsu selama deteksi dan pemberantasan kode berbahaya dan dampak potensial yang dihasilkan pada ketersediaan sistem.

  Pembahasan: Titik masuk dan keluar sistem mencakup *firewall*, *server* akses jarak jauh, *workstation*, *server* surat elektronik, *server web*, *server proxy*, komputer notebook, dan perangkat seluler. Kode berbahaya

termasuk *virus*, *worm*, *trojan horse*, dan *spyware*. Kode berbahaya juga bisa dikodekan dalam berbagai format yang terkandung dalam file terkompresi atau tersembunyi atau disembunyikan dalam file menggunakan teknik seperti steganografi.

Kontrol Terkait: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26 , SC 28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.

- **SI-4(4) (Lalu Lintas Komunikasi Masuk dan Keluar)**
  (4) PEMANTAUAN SISTEM | TRAFFIC KOMUNIKASI MASUK DAN KELUAR

  Kontrol:

  (a) Menentukan kriteria untuk aktivitas atau kondisi yang tidak biasa atau tidak sah untuk masuk dan lalu lintas komunikasi keluar;

  (b) Memantau lalu lintas komunikasi masuk dan keluar [Penugasan: frekuensi yang ditentukan organisasi] untuk [Penugasan: tidak biasa atau tidak sah yang ditentukan organisasi kegiatan atau kondisi].

  Pembahasan: Aktivitas atau kondisi yang tidak biasa atau tidak sah terkait dengan sistem masuk dan lalu lintas komunikasi keluar termasuk lalu lintas internal yang menunjukkan adanya kode berbahaya atau penggunaan kode atau kredensial yang sah secara tidak sah dalam organisasi sistem atau menyebar di antara komponen sistem, pensinyalan ke sistem eksternal, dan pengeksporan informasi yang tidak sah. Bukti kode berbahaya atau penggunaan yang tidak sah dari kode atau kredensial yang sah digunakan untuk mengidentifikasi sistem atau sistem yang berpotensi disusupi komponen.

  Kontrol Terkait: Tidak ada.

- **SI-10 (*Valid*asi Input Informasi),**

  Kontrol: Periksa *valid*itas input informasi berikut: [Penugasan: input informasi yang ditentukan organisasi ke sistem].

  Pembahasan: Memeriksa sintaks dan semantik yang *valid* dari input sistem—termasuk rangkaian karakter, panjang, rentang numerik, dan nilai

yang dapat diterima—memverifikasi bahwa input cocok dengan definisi yang ditentukan untuk format dan konten. Misalnya, jika organisasi menentukan nilai numerik antara

1-100 adalah satu-satunya input yang dapat diterima untuk bidang dalam aplikasi tertentu, input "387", "abc", atau “%K%” adalah input yang tidak *valid* dan tidak diterima sebagai input ke sistem. Input yang *valid* cenderung bervariasi dari bidang ke bidang dalam aplikasi perangkat lunak. Aplikasi biasanya mengikuti didefinisikan dengan baik protokol yang menggunakan pesan terstruktur (yaitu, perintah atau kueri) untuk berkomunikasi modul perangkat lunak atau komponen sistem. Pesan terstruktur dapat berisi mentah atau tidak terstruktur diselingi dengan metadata atau informasi kontrol. Jika aplikasi perangkat lunak menggunakan input yang disediakan penyerang untuk membuat pesan terstruktur tanpa menyandikan pesan tersebut dengan benar, maka penyerang bisa menyisipkan perintah jahat atau karakter khusus yang dapat menyebabkan data untuk ditafsirkan sebagai informasi kontrol atau metadata. Akibatnya, modul atau komponen yang menerima output yang rusak akan melakukan operasi yang salah atau menafsirkannya data secara tidak benar. Prapenyaringan input sebelum meneruskannya ke juru bahasa akan mencegah konten dari yang tidak sengaja ditafsirkan sebagai perintah. Validasi masukan memastikan akurat dan masukan yang benar dan mencegah serangan seperti cross-site scripting dan berbagai serangan injeksi.

Kontrol Terkait: Tidak ada.

- **SI-11 (Penanganan Kesalahan),**

  Kontrol:

  A. Hasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungkapkan informasi yang dapat dimanfaatkan; Dan

  B. Ungkapkan pesan kesalahan hanya ke [Tugas: personel atau peran yang ditentukan organisasi].

Pembahasan: Organisasi mempertimbangkan struktur dan isi pesan kesalahan. Sejauh
sistem mana yang dapat menangani kondisi kesalahan dipandu dan diinformasikan oleh kebijakan organisasi dan kebutuhan operasional. Informasi yang dapat dieksploitasi mencakup pelacakan tumpukan dan implementasi rincian; upaya masuk yang salah dengan kata sandi yang dimasukkan secara keliru sebagai nama pengguna; misi atau informasi bisnis yang dapat diturunkan dari, jika tidak dinyatakan secara eksplisit oleh, informasi tersebut tercatat; dan informasi pribadi, seperti nomor rekening, jaminan sosial nomor, dan nomor kartu kredit. Pesan kesalahan juga dapat menyediakan saluran rahasia untuk mengirimkan informasi.

Kontrol Terkait: AU-2, AU-3, SC-31, SI-2, SI-15.

- **SI-16 (Perlindungan Memori),**

  Kontrol: Terapkan kontrol berikut untuk melindungi memori sistem dari eksekusi kode yang tidak sah: [Penugasan: kontrol yang ditentukan organisasi].

  Pembahasan: Beberapa musuh meluncurkan serangan dengan tujuan mengeksekusi kode di wilayah memori yang tidak dapat dieksekusi atau di lokasi memori yang dilarang. Kontrol yang digunakan untuk melindungi memori termasuk pencegahan eksekusi data dan pengacakan tata letak ruang alamat. Kontrol pencegahan eksekusi data dapat didukung oleh perangkat keras atau perangkat lunak dengan penegakan perangkat keras memberikan kekuatan mekanisme yang lebih besar.

  Kontrol Terkait: AC-25, SC-3, SI-7.

Lampiran 2 Rencana Tindak Pengendalian

Di mana penelitian yang dilakukan pada website bsip.pertanian.co.id di Badan Standarisasi Instrumen Pertanian (BSIP) dengan NIST SP 800-30 untuk penilaian risiko dan NIST SP 800-53 rev.5 untuk rekomendasi kontrol.

1. **Identifikasi Aset**

   Aset yang didapatkan yaitu pada *hardware, software,* data dan informasi, sumber daya manusia (SDM) dan infrastrukturnya.

2. **Identifikasi Ancaman**

   Terdapat berbagai sumber ancaman berupa kejadian ancaman yang didapatkan yaitu berupa 10 ancaman adversarial dan 8 ancaman non-adversarial terdapat 2 *High*, 5 *Medium*, 6 *Low* dan 5 *Very Low* pada rentan efek ancaman di *website* bsip.pertanian.co.id.

3. **Identifikasi Kerentanan**

   Pada tahapan ini yaitu penulis akan mengembangkan daftar kekurangan maupun kelemahan yang ada pada sistem dan teknologi informasi di website bsip.pertanian.go.id yang dapat dipicu atau disebabkan oleh ancaman dengan skala penilaian kerentanan dengan hasil yaitu daftar kerentanan berdasarkan temuan ancaman terdapat 4 *High*, 1 *Medium*, 8 *Low* dan 5 *Very Low* pada kerentanan di *website* bsip.pertanian.co.id.

4. **Analisis Kontrol**

   Pengendalian kerentanan sistem dengan adanya kontrol untuk sumber informasi dari kontrol yang dilakukan saat ini dan terdapat ancaman yang masih kurang untuk dilindungi dengan kontrol yang telah dilakukan oleh BSIP (Badan Standarisasi Instrumen Pertanian) saat ini.

5. Penentuan Kemungkinan (*Likelihood*)

Dengan menentukan kerentanan yang relevan dengan kejadian ancaman yang terjadi untuk risiko potensial yang akan dinilai terdapat 1 *High*, 3 *Medium*, 8 *Low* dan 6 *Very Low* pada keseluruhan kemungkinan di *website* bsip.pertanian.co.id.

6. Analisis Dampak

Mengidentifikasi dampak untuk menentukan potensi dampak buruk dalam pada sistem terdapat 3 *Very High*, 2 *High*, 4 *Medium*, 6 *Low* dan 3 *Very Low* pada dampak yang dialami di *website* bsip.pertanian.co.id.

7. Penilaian Risiko

Penilaian risiko peristiwa ancaman dari identifikasi kemungkinan dan dampak yang yang telah dilakukan. Tingkat risiko tersebut yang teridentifikasi menjadi salah satu penentu sejauh mana sistem terancam oleh berbagai peristiwa tersebut terdapat 2 *High*, 3 *Medium*, 7 *Low* dan 6 *Very Low* pada penilaian risiko di *website* bsip.pertanian.co.id.

8. Rekomendasi Kontrol

Membuat rekomendasi untuk risiko yang telah terdeteksi untuk mengidentifikasikan kontrol yang dapat mengurangi ataupun menghilangkan risiko yang berdasarkan pada pedoman pendukung NIST SP 800-53 rev.5 yang disesuaikan dengan 20 kelompok kontrol yang ada.

Yang mana pada penelitian yang telah dilakukan pada website bsip.pertanian.co.id ini di Badan Standarisasi Instrumen Pertanian (BSIP) ini nantinya akan didokumentasikan berupa dengan rencana tindak pengendalian (RTP) yang nantinya kan ditunjukan kepada entitas tujuan atau dari tempat penelitian, sebagai berikut:

Nama Entitas/OPD : Badan Standarisasi Instrumen Pertanian

Daftar Risiko

Kegiatan : Pemeliharaan pelayanan publik pada *website* BSIP

Tujuan Kegiatan : Terpenuhinya sarana untuk peningkatan pelayanan publik

KIR	Pernyataan Risiko	Penyebab	
		Sumber Aset	Uraian
1	2	3	4
1.	Adanya serangan *malware* atau *virus* yang disebabkan oleh pihak luar/dalam.	*Software*	Terjadi kerentanan pada aset *software*, dimana terdapat serangan *ransomware* pada bulan Juli lalu yang menyebabkan sistem berhenti. Sehingga rekomendasinya yaitu dengan perlindungan dengan anti*virus*.
2.	Kegagalan *Backup*	Data dan Informasi	Terjadi kerentanan pada aset data dan informasi, dimana pada serangan *ransomware* tersebut menyebabkan kegagalan *backup* menjadikan data hilang selama 2 bulan ke belakang. Sehingga rekomendasi kontrolnya yaitu dengan membuat cadangan data.
3.	Pemanfaatan celah keamanan oleh pihak dalam/luar.	*Software*	Terjadi kerentanan pada aset *software*, dimana pemanfaatan celah keamanan yang menjadikan serangan dari pihak lain untuk masuk, seperti pada serangan *ransomware* tersebut. Sehingga rekomendasinya yaitu dengan pembatasan penggunaan akses sistem.
4.	Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.	Data dan Informasi	Terjadi kerentanan pada aset data dan informasi, dimana pada serangan *ransomware* tersebut menyebabkan data hilang. Sehingga rekomendasinya yaitu dengan perlindungan pada *storage* data.

KIR	Pernyataan Risiko	Penyebab	
		Sumber Aset	Uraian
1	2	3	4
5.	Kehilangan data yang sifatnya sensitif.	Data dan Informasi	Terjadi kerentanan pada aset data dan informasi, dimana kurangnya salinan *backup*. Sehingga rekomendasinya yaitu dengan menambahkan *storage* khusus untuk sistem *backup*.

Rencana Tindak Pengendalian

Nama Entitas/OPD : Badan Standarisasi Instrumen Pertanian

Kegiatan : Pemeliharaan pelayanan publik pada *website* BSIP

Tujuan Kegiatan : Terpenuhinya sarana untuk peningkatan pelayanan publik

No.	Pernyataan Risiko	Uraian Rencana Pengendalian	Target Waktu	Penanggung Jawab
1	**2**	**3**	**4**	**5**
1.	Adanya serangan *malware* atau *virus* yang disebabkan oleh pihak luar/dalam.	SI-3 Perlindungan Kode Berbahaya (Mekanisme perlindungan kode berbahaya di titik masuk dan keluar sistem untuk mendeteksi dan membasmi kode berbahaya.)	Agustus – Desember 2023	Staff IT bagian Teknisi
2.	Kegagalan *Backup*	SI-16 Perlindungan Memori (Mengeksekusi kode di wilayah memori yang tidak dapat dieksekusi atau di lokasi memori yang dilarang untuk melindungi memori termasuk pencegahan	Agustus – Desember 2023	Staff IT bagian Teknisi dan Konten

No.	Pernyataan Risiko	Uraian Rencana Pengendalian	Target Waktu	Penanggung Jawab
1	2	3	4	5
		eksekusi data dan pengacakan tata letak ruang alamat)		
3.		CP-9(5): Transfer ke Situs Penyimpanan Alternatif (Mentransfer informasi cadangan sistem ke situs penyimpanan alternatif.)	Agustus – Desember 2023	Staff IT bagian Teknisi dan Konten
4.	Pemanfaatan celah keamanan oleh pihak dalam/luar.	RA-3: *Risk Assessment* (Mengidentifikasi dan mendokumentasikan ancaman dan kerentanan dalam sistem baik internal maupun eksternal)	Agustus – Desember 2023	Staff IT bagian Teknisi
5.	Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.	SI-4(4): Lalu Lintas Komunikasi Masuk dan Keluar (Menunjukkan adanya kode berbahaya atau penggunaan tidak sah melalui lalu lintas komunikasi sistem masuk dan keluar termasuk lalu lintas internal)	Agustus – Desember 2023	Staff IT bagian Teknisi dan Konten
6.		CP-9(8): Perlindungan	Agustus – Desember	Staff IT bagian

No.	Pernyataan Risiko	Uraian Rencana Pengendalian	Target Waktu	Penanggung Jawab
1	2	3	4	5
		Kriptografi (Perlindungan kriptografi berlaku untuk informasi cadangan sistem dalam penyimpanan di lokasi utama dan alternatif)	2023	Teknisi dan Konten
7.		AC-4: Penegakan Arus Informasi (Pembatasan aliran informasi termasuk memblokir lalu lintas eksternal)	Agustus – Desember 2023	Staff IT bagian Teknisi dan Konten
8.	Kehilangan data yang sifatnya sensitif.	CP-9(8): Perlindungan Kriptografi (Perlindungan kriptografi berlaku untuk informasi cadangan sistem dalam penyimpanan di lokasi utama dan alternatif)	Agustus – Desember 2023	Staff IT bagian Teknisi dan Konten

Lampiran 3 Surat Penelitian

KEMENTERIAN PERTANIAN
BADAN PENELITIAN DAN PENGEMBANGAN PERTANIAN
JALAN RAGUNAN NO. 29 PASARM NGGU JAKARTA 12540 KOTAK POS 76 PSM
TELEPON (021) 7806202, 7806203, 7806204, FAKSIMILI (021) 7800644
WEBSITE: www.litbang.pertanian.go.id e-mail: sekretariat@litbang.pertanian.go.id

Nomor : B- 01 /TI.120/H.1.1.1/12/2022 01 Desember 2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Keterangan telah menyelesaikan Kegiatan Penelitian di Badan Litbang Pertanian Mahasiswi Esa Unggul

Yth. Pimpinan Program Sarjana
Universitas Esa Unggul

di
Tempat

Bersama surat ini kami memberitahukan kepada Pimpinan Program Sarjana Universitas Esa Unggul bahwa mahasiswi Prodi Komputer di bawah ini :

No	Nama	NIM
1	Liuzly Hindun N.U	20190803082
2	Cindy Asari	20190803008

Telah melakukan penelitian untuk bahan sekripsi dan wawancara di instansi kami Badan Litbang Pertanian Komorterian Pertaniar, Jl. Ragunan no 29 Pasar Minggu, Jakarta Selatan.

Demikian surat keterangan ini kami dibuat agar dipergunakan sebagaimana mestinya,
Atas perhatiannya kami sampaikan terima kasih.

Subkoordinator Data dan Informasi,

Henera Yuniar, S.Kom., M.Kom
NIP. 197306281998031001

Lampiran 4 Surat Perpindahan Domain

KEMENTERIAN PERTANIAN
BADAN PENELITIAN DAN PENGEMBANGAN PERTANIAN
JALAN RAGUNAN NO. 29 PASARMINGGU JAKARTA 12540 KOTAK POS 76 PSM
TELEPON (021) 7806202, 7803203, 7806204, FAKSIMILI (021) 7800644
WEBSITE: www.litbang.pertanian.go.id e-mail: sekretariat@litbang.pertanian.go.id

Nomor : B-313/TI.110/H.1/02/2023 14 Februari 2023
Sifat : Segera
Lampiran : satu berkas
Hal : Permintaan Virtual Server dan Domain Website Satker lingkup BSIP

Yth. Kepala Pusat Data dan Sistem Informasi Pertanian

di
Tempat

Sehubungan dengan transformasi kelembagaan Balitbangtan menjadi Badan Standardisasi Instrumen Pertanian (BSIP) telah dilakukan pengembangan situs web BSIP. Dalam kerangka operasionalnya, diperlukan virtual server dan domain baru untuk seluruh satker lingkup BSIP, sebagaimana terlampir. Mohon kiranya Saudara dapat membantu keperluan dimaksud.

Atas perhatian dan kerjasama Saudara, saya sampaikan terima kasih.

Sekretaris Badan,

Dr. Ir. Haris Syahbuddin, DEA
NIP. 196804121992031001

Tembusan :
Plt. Kepala Badan

NO	SATKER	PERMENTAN NO 19/2022 dan PERMENTAN NO 15/2023	PENYEBUTAN	DOMAIN WEBSITE
1	Badan Standardisasi Instrumen Pertanian	BSIP	BSIP	bsip.pertanian.go.id
2	Sekretariat Badan Standardisasi Instrumen Pertanian		SEKRETARIAT BSIP	
3	Pusat Standardisasi Instrumen Tanaman Pangan	PSI TANAMAN PANGAN	BSIP TANAMAN PANGAN	tanamanpangan.bsip.pertanian.go.id
4	Pusat Standardisasi Instrumen Hortikultura	PSI HORTIKULTURA	BSIP HORTIKULTURA	hortikultura.bsip.pertanian.go.id
5	Pusat Standardisasi Instrumen Tanaman Perkebunan	PSI TANAMAN PERKEBUNAN	BSIP PERKEBUNAN	perkebunan.bsip.pertanian.go.id
6	Pusat Standardisasi Instrumen Peternakan dan Kesehatan Hewan	PSI PETERNAKAN DAN KESWAN	BSIP PETERNAKAN DAN KESWAN	peternakan.bsip.pertanian.go.id
7	Balai Besar Pengujian Standar Instrumen Padi	BBPSI PADI	BSIP PADI	padi.bsip.pertanian.go.id
8	Balai Besar Pengujian Standar Instrumen Veteriner	BBPSI VETERINER	BSIP VETERINER	veteriner.bsip.pertanian.go.id
9	Balai Besar Pengujian Standar Instrumen Sumber Daya Lahan Pertanian	BBPSI SDLP	BSIP SDLP	sdlp.bsip.pertanian.go.id
10	Balai Besar Pengujian Standar Instrumen Mekanisasi Pertanian	BBPSI MEKTAN	BSIP MEKTAN	mektan.bsip.pertanian.go.id
11	Balai Besar Pengujian Standar Instrumen Bioteknologi dan Sumber Daya Genetik Pertanian	BBPSI BIOGEN	BSIP BIOGEN	biogen.bsip.pertanian.go.id
12	Balai Besar Pengujian Standar Instrumen Pasca Panen	BBPSI PASCAPANEN	BSIP PASCAPANEN	pascapanen.bsip.pertanian.go.id
13	Balai Besar Penerapan Standar Instrumen Pertanian	BBPSIP	BSIP PENERAPAN	bbpsip.bsip.pertanian.go.id
14	Balai Pengujian Standar Instrumen Tanaman Aneka Kacang	BPSI TANAMAN ANEKA KACANG	BSIP ANEKA KACANG	aneka.kacang.bsip.pertanian.go.id
15	Balai Pengujian Standar Instrumen Tanaman Serealia	BPSI TANAMAN SEREALIA	BSIP SEREALIA	serealia.bsip.pertanian.go.id
16	Balai Pengujian Standar Instrumen Tanaman Sayuran	BPSI TANAMAN SAYURAN	BSIP SAYURAN	sayuran.bsip.pertanian.go.id
17	Balai Pengujian Standar Instrumen Tanaman Buah Tropik	BPSI TANAMAN BUAH TROPIKA	BSIP BUAH TROPIKA	buahtropika.bsip.pertanian.go.id
18	Balai Pengujian Standar Instrumen Tanaman Hias	BPSI TANAMAN HIAS	BSIP TANAMAN HIAS	hias.bsip.pertanian.go.id
19	Balai Pengujian Standar Instrumen Tanaman Jeruk dan Buah Subtropika	BPSI TANAMAN JERUK DAN BUAH SUBTROPIKA	BSIP TANAMAN JERUK DAN BUAH SUBTROPIKA	jeruk.bsip.pertanian.go.id
20	Balai Pengujian Standar Instrumen Tanaman Rempah, Obat dan Aromatik	BPSI TANAMAN REMPAH, OBAT DAN AROMATIK	BSIP TANAMAN REMPAH OBAT AROMAT	rempahobat.bsip.pertanian.go.id
21	Balai Pengujian Standar Instrumen Tanaman Industri dan Penyegar	BPSI TANAMAN INDUSTRI DAN PENYEGAR	BSIP TANAMAN INDUSTRI	industri.bsip.pertanian.go.id
22	Balai Pengujian Standar Instrumen Tanaman Pemanis dan Serat	BPSI TANAMAN PEMANIS DAN SERAT	BSIP PEMANIS DAN SERAT	gulma.bsip.pertanian.go.id
23	Balai Pengujian Standar Instrumen Tanaman Palma	BPSI TANAMAN PALMA	BSIP PALMA	palma.bsip.pertanian.go.id
24	Balai Pengujian Standar Instrumen Unggas dan Aneka Ternak	BPSI UNGGAS DAN ANEKA TERNAK	BSIP UNGGAS DAN ANEKA TERNAK	unggas.bsip.pertanian.go.id
25	Balai Pengujian Standar Instrumen Tanah dan Pupuk	BPSI TANAH DAN PUPUK	BSIP TANAH	tanah.bsip.pertanian.go.id
26	Balai Pengujian Standar Instrumen Lingkungan Pertanian	BPSI LINGKUNGAN PERTANIAN	BSIP LINGKUNGAN	lingkungan.bsip.pertanian.go.id
27	Balai Pengujian Standar Instrumen Pertanian Lahan Rawa	BPSI PERTANIAN LAHAN RAWA	BSIP LAHAN RAWA	lahanrawa.bsip.pertanian.go.id
28	Balai Pengujian Standar Instrumen Agroklimat dan Hidrologi Pertanian	BPSI AGROKLIMAT DAN HIDROLOGI PERTANIAN	BSIP AGROKLIMAT	agroklimat.bsip.pertanian.go.id
29	Balai Informasi Standar Instrumen Pertanian	BSIP	BSIP INFORMASI	informasi.bsip.pertanian.go.id
30	Loka Pengujian Standar Instrumen Tanaman Aneka Umbi	LPSI TANAMAN ANEKA UMBI	BSIP ANEKA UMBI	aneka.umbi.bsip.pertanian.go.id
31	Loka Pengujian Standar Instrumen Ruminansia Besar	LPSI RUMINANSIA BESAR	BSIP RUMINANSIA BESAR	ruminansiabesar.bsip.pertanian.go.id
32	Loka Pengujian Standar Instrumen Ruminansia Kecil	LPSI RUMINANSIA KECIL	BSIP RUMINANSIA KECIL	ruminansiakecil.bsip.pertanian.go.id
33	Balai Penerapan Standardisasi Instrumen Pertanian Aceh	BPSIP ACEH	BSIP ACEH	aceh.bsip.pertanian.go.id
34	Balai Penerapan Standardisasi Instrumen Pertanian Sumatera Utara	BPSIP SUMATERA UTARA	BSIP SUMUT	sumut.bsip.pertanian.go.id
35	Balai Penerapan Standardisasi Instrumen Pertanian Sumatera Barat	BPSIP SUMATERA BARAT	BSIP SUMBAR	sumbar.bsip.pertanian.go.id
36	Balai Penerapan Standardisasi Instrumen Pertanian Riau	BPSIP RIAU	BSIP RIAU	riau.bsip.pertanian.go.id
37	Balai Penerapan Standardisasi Instrumen Pertanian Jambi	BPSIP JAMBI	BSIP JAMBI	jambi.bsip.pertanian.go.id
38	Balai Penerapan Standardisasi Instrumen Pertanian Sumatera Selatan	BPSIP SUMATERA SELATAN	BSIP SUMSEL	sumsel.bsip.pertanian.go.id

Lampiran 5 Wawancara

Wawancara pengambilan data awal:

1. Perangkat fisik apa saja yang menjadi pendukung dalam menjalankan *website* bsip.pertanian.go.id?

   Jawab: Perangkat fisik yang menjadi pendukung dalam menjalankan *website* yaitu *server*, komputer dan *router*.
2. Software dan hardware pendukung dalam menjalankan *website* bsip.pertanian.go.id?

   Jawab: *Software* yaitu *Ubuntu* 16.04.5 ITS (*GNU/Linux* 4.4.0-210-*generic* x86 64) dan *hardware* yaitu memiliki memori 4 GB, *processors* 4, *hard disk* 100 GB, *network adapter bridged (autometic)*, *Laravel* 8.0, dan *Postgresql* 13.
3. Siapa saja yang bertanggung jawab atau berhak dalam menjalankan *website* bsip.pertanian.go.id?

   Jawab: Yang bertanggung jawab dan berhak dalam menjalankan *website* yaitu semua yang ada, dimana semua memiliki hak akses berupa *password* yang diketahui oleh semua.
4. Dimana letak *server* yang digunakan sebagai pendukung dalam menjalankan *website* bsip.pertanian.go.id?

   Jawab: Berada di ruang *server*.
5. Apa saja data dan informasi yang ada pada *website* bsip.pertanian.go.id?

   Jawab: Data dan informasi yang ada yaitu antara lain hasil riset, publikasi, kerja sama, layanan, profil dan KIP (keterbukaan informasi publik).
6. Apa saja kemungkinan risiko yang pernah terjadi pada *website* bsip.pertanian.go.id?

   Jawab: Kemungkinannya yaitu pada *windows server* yang terkena *ransomware* pada bulan Juli yang termasuk paling fatal selama ini.
7. Seberapa sering kemungkinan risiko yang terjadi pada *website* bsip.pertanian.go.id?

Jawab: Pada kemungkinan risiko yang terjadi yaitu baru terjadi sekali dalam berjalannya *website* tersebut.

8. Bagaimana penanganan yang dilakukan pada saat kasus risiko terjadi?
   Jawab: Penanganan yang dilakukan pada saat menghadapi yaitu belum ada tindakan lanjut mengenai masalah yang ada.
9. Pada *website*bsip.pertanian.go.id terhubung dalam interkoneksi sistem atau aplikasi apa saja?
   Jawab: *Website*terhubung dengan *website* yang ada berupa link seperti aplikasi badan Litbang Pertanian, Jaringan Dokumentasi dan Informasi Hukum Kementrian Pertanian Republik Indonesia, Pusat Genom Pertanian Indonesia (PGPI), *WhistlebLower's* Sistem Kementrian Pertanian, Sistem Informasi Grafikasi Pertanian (SIGAP).

Wawancara pengambilan data:

Narasumber: Staff IT 1

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
3. Apakah pernah terjadi *update* sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Pernah

9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah

Narasumber: Staff IT 2

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?

Jawab: Pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah

Narasumber: Staff IT 3

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website*bsip.pertanian.go.id?
   Jawab: Tidak pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah

Narasumber: Pengguna 1

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website*bsip.pertanian.go.id?
    Jawab: Pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website*bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah

Narasumber: Pengguna 2

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah

Narasumber: Pengguna 3

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak Pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Pernah

Narasumber: Pengguna 4

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website*bsip.pertanian.go.id?
    Jawab: Pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah

Narasumber: Pengguna 5

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website*bsip.pertanian.go.id?
   Jawab: Tidak pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website*bsip.pertanian.go.id?
   Jawab: Tidak pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website*bsip.pertanian.go.id?
    Jawab: Pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website*bsip.pertanian.go.id?
    Jawab: Tidak pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah

Narasumber: Pengguna 6

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website*bsip.pertanian.go.id?
   Jawab: Tidak pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website*bsip.pertanian.go.id?
   Jawab: Tidak pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website*bsip.pertanian.go.id?
    Jawab: Tidak pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website*bsip.pertanian.go.id?
    Jawab: Pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak Pernah

Narasumber: Pengguna 7

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah

Narasumber: Pengguna 8

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah

Narasumber: Pengguna 9

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah

Narasumber: Pengguna 10

Daftar Pertanyaan:

1. Apakah pernah terjadi kerusakan pada aset yang sudah menua ataupun rusak pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
2. Apakah pernah terjadi adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
3. Apakah pernah terjadi update sistem yang belum dilakukan menyebabkan sistem berhenti/*error* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
4. Apakah pernah terjadi *windows* tidak berjalan semestinya pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
5. Apakah pernah terjadi pemanfaatan celah keamanan oleh pihak dalam/luar pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
6. Apakah pernah terjadi *server* down yang menyebabkan halaman tidak bisa diakses pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
7. Apakah pernah terjadi pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
8. Apakah pernah terjadi kehilangan data yang sifatnya sensitif pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah
9. Apakah pernah terjadi kegagalan *Backup* pada *website* bsip.pertanian.go.id?
   Jawab: Tidak pernah

10. Apakah pernah terjadi menggunakan *password* yang lemah/default *password* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
11. Apakah pernah terjadi kesalahan dalam pengelolahan data oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
12. Apakah pernah terjadi akses *password* oleh karyawan yang tidak berwenang pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
13. Apakah pernah terjadi kesalahan operasional yang disebabkan oleh staff IT pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
14. Apakah pernah terjadi gangguan tegangan listrik/tegangan listrik tidak stabil pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
15. Apakah pernah terjadi ruangan *server* yang temperatur suhunya tidak sesuai standart pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
16. Apakah pernah terjadi gangguan Jaringan pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
17. Apakah pernah terjadi kerusakan kabel LAN akibat hewan pengerat pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah
18. Apakah pernah terjadi bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server* pada *website* bsip.pertanian.go.id?
    Jawab: Tidak pernah

Transkrip Wawancara

Hari/tanggal wawancara : Rabu, 31 Mei 2023

Nama : Sony Hanjaya selaku bagian Teknisi

Daftar Pertanyaan:

1. **Apa saja ancaman yang pernah terjadi pada *website* tersebut?**
   Mengenai Ancaman (Adversarial dan Non-adversarial)

   - Adversarial

   Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Hampir Pasti Terjadi	Musuh adalah yakin untuk memulai peristiwa ancaman.
Tinggi (*High*)	Sangat Mungkin Terjadi	Musuh adalah sangat mungkin untuk memulai peristiwa ancaman
Sedang (*Medium*)	Agak Mungkin	Musuh adalah agak mungkin untuk memulai acara perawatan.
Rendah (*Low*)	Tidak Mungkin	Musuh adalah tidak mungkin untuk memulai peristiwa ancaman.
Sangat Rendah (*Very Low*)	Sangat Tidak Mungkin Terjadi	Musuh adalah sangat tidak mungkin untuk memulai peristiwa ancaman

   Daftar Pertanyaan:

   1) Berapa tingkat kerentangan dari Adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam?
      Jawab: *High*

2) Berapa tingkat kemungkinan ancaman dari *Windows* tidak berjalan semestinya?
   Jawab:*Very Low*
3) Berapa tingkat kemungkinan ancaman dari Pemanfaatan celah keamanan oleh pihak dalam/luar?
   Jawab: *High*
4) Berapa tingkat kemungkinan ancaman dari *Server* Down yang menyebabkan halaman tidak bisa diakses?
   Jawab: *Medium*
5) Berapa tingkat kemungkinan ancaman dari Akses *password* oleh karyawan yang tidak berwenang?
   Jawab: *Very Low*
6) Berapa tingkat kemungkinan ancaman dari Gangguan Jaringan?
   Jawab: *Very Low*

- Non-adversarial

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Hampir Pasti Terjadi	Kesalahan, kecelakaan, atau tindakan alam adalah hampir pasti terjadi; atau terjadi lebih dari 100 kali setahun.
Tinggi (*High*)	Sangat Mungkin Terjadi	Kesalahan, kecelakaan, atau tindakan alam adalah sangat mungkin terjadi; atau terjadi antara 10-100 kali setahun.
Sedang (*Medium*)	Agak Mungkin	Kesalahan, kecelakaan, atau tindakan alam adalah agak mungkin teriadi; atau terjadi antara 1-10 kali setahun.
Rendah (*Low*)	Tidak Mungkin	Kesalahan, kecelakaan, atau tindakan alam adalah tidak mungkin terjadi; atau terjadi kurang dari setahun sekali, tetapi lebih dari sekali setiap 10 tahun.
Sangat Rendah (*Very Low*)	Sangat Tidak Mungkin Terjadi	Kesalahan, kecelakaan, atau tindakan alam adalah sangat tidak mungkin terjadi; atau terjadi kurang dari sekali setiap 10 tahun.

Daftar Pertanyaan:

1) Berapa tingkat kemungkinan ancaman dari Kerusakan pada aset yang sudah menua ataupun rusak?
   Jawab:*Medium*
2) Berapa tingkat kemungkinan ancaman dari Update sistem yang belum dilakukan menyebabkan system berhenti/*error*?
   Jawab: *Medium*
3) Berapa tingkat kemungkinan ancaman dari Kesalahan operasional yang disebabkan oleh staff IT?
   Jawab: *Very Low*
4) Berapa tingkat kemungkinan ancaman dari Gangguan tegangan listrik/tegangan listrik tidak stabil?
   Jawab: *Low*
5) Berapa tingkat kemungkinan ancaman dari Ruangan *server* yang temperatur suhunya tidak sesuai standart?
   Jawab: *Low*
6) Berapa tingkat kemungkinan ancaman dari Kerusakan kabel LAN akibat hewan pengerat?
   Jawab: *Low*
7) Berapa tingkat kemungkinan ancaman dari Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server*?
   Jawab: *Very Low*

2. Berapa tingkat kerentanan pada *website* tersebut?

Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Keterangan
Sangat Tinggi (*Very High*)	Terbuka dan dapat dieksploitasi	Kerentanan terbuka dan dapat dieksploitasi, dan eksploitasinya dapat mengakibatkan dampak yang parah. Kontrol keamanan yang relevan atau perbaikan lainnya tidak dilaksanakan dan tidak direncanakan; atau tidak ada tindakan keamanan yang dapat

Skala	NIST SP 800-30	Keterangan
		diidentifikasi untuk memulihkan kerentanan.
Tinggi (*High*)	Memprihatinkan	Kerentanan tersebut sangat memprihatinkan, berdasarkan paparan kerentanan dan kemudahan eksploitasi dan/atau keparahan dampak yang dapat ditimbulkan dari eksploitasinya. Kontrol keamanan yang relevan atau perbaikan lainnya direncanakan tetapi tidak dilaksanakan; kontrol kompensasi sudah ada dan setidaknya efektif secara minimal.
Sedang (*Medium*)	Sedang	Kerentanan tergolong sedang, berdasarkan paparan kerentanan dan kemudahan eksploitasi dan/atau tingkat keparahan dampak yang dapat ditimbulkan dari eksploitasinya. Kontrol keamanan yang relevan atau perbaikan lainnya diterapkan sebagian dan agak efektif.
Rendah (*Low*)	Perhatian Kecil	Kerentanan menjadi perhatian kecil, tetapi efektivitas remediasi dapat ditingkatkan. Kontrol keamanan yang relevan atau perbaikan lainnya diterapkan sepenuhnya dan agak efektif.
Sangat Rendah (*Very Low*)	Tidak menjadi Perhatian	Kerentanan tidak menjadi perhatian. Kontrol keamanan yang relevan atau perbaikan lainnya sepenuhnya dilaksanakan, dinilai, dan efektif.

Daftar Pertanyaan:

1) Berapa tingkat kerentangan dari Kerusakan pada aset yang sudah menua ataupun rusak?
   Jawab: *Low*
2) Berapa tingkat kerentangan dari Adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam?
   Jawab: *High*
3) Berapa tingkat kerentangan dari Update sistem yang belum dilakukan menyebabkan system berhenti/*error*?
   Jawab: *Low*
4) Berapa tingkat kerentangan dari *Windows* tidak berjalan semestinya?
   Jawab: *Very Low*
5) Berapa tingkat kerentangan dari Pemanfaatan celah keamanan oleh pihak dalam/luar?
   Jawab: *Medium*

6) Berapa tingkat kerentangan dari *Server* Down yang menyebabkan halaman tidak bisa diakses?
   Jawab: *Low*
7) Berapa tingkat kerentanan dari Akses *password* oleh karyawan yang tidak berwenang.
   Jawab: *Low*
8) Berapa tingkat kerentangan dari Kesalahan operasional yang disebabkan oleh staff IT?
   Jawab: *Very Low*
9) Berapa tingkat kerentangan dari Gangguan tegangan listrik/tegangan listrik tidak stabil?
   Jawab: *Low*
10) Berapa tingkat kerentangan dari Ruangan *server* yang temperatur suhunya tidak sesuai standart?
   Jawab: *Very Low*
11) Berapa tingkat kerentangan dari Gangguan Jaringan?
   Jawab: *Very Low*
12) Berapa tingkat kerentangan dari Kerusakan kabel LAN akibat hewan pengerat?
   Jawab: *Low*
13) Berapa tingkat kerentangan dari Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server*?
   Jawab: *Very Low*

3. Berapa kemungkinan terjadinya ancaman pada *website* tersebut?

Kemungkinan Inisiasi Kejadian Ancaman Menyebabkan Dampak Yang Merugikan

Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Hampir Pasti Terjadi	Jika peristiwa ancaman dimulai atau terjadi, itu adalah yakin untuk memiliki dampak yang

Skala	NIST SP 800-30	Kriteria
		merugikan.
Tinggi (*High*)	Sangat Mungkin Terjadi	Jika peristiwa ancaman dimulai atau terjadi, itu adalah sangat mungkin untuk memiliki dampak yang merugikan
Sedang (*Medium*)	Agak Mungkin	Jika peristiwa ancaman dimulai atau terjadi, itu adalah agak mungkin untuk memiliki dampak yang merugikan.
Rendah (*Low*)	Tidak Mungkin	Jika peristiwa ancaman dimulai atau terjadi, itu adalah tidak mungkin untuk memiliki dampak yang merugikan.
Sangat Rendah (*Very Low*)	Sangat Tidak Mungkin Terjadi	Jika peristiwa ancaman dimulai atau terjadi, itu adalah sangat tidak mungkin untuk memiliki dampak yang merugikan.

Daftar Pertanyaan:

1) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kerusakan pada aset yang sudah menua ataupun rusak?
   Jawab: *Low*
2) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam?
   Jawab: *High*
3) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Update sistem yang belum dilakukan menyebabkan system berhenti/*error*
   Jawab: *Medium*
4) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari *Windows* tidak berjalan semestinya?
   Jawab: *Low*
5) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Pemanfaatan celah keamanan oleh pihak dalam/luar?
   Jawab: *Medium*

6) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari *Server* Down yang menyebabkan halaman tidak bisa diakses?
   Jawab: *Low*
7) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Akses *password* oleh karyawan yang tidak berwenang?
   Jawab: *Medium*
8) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kesalahan operasional yang disebabkan oleh staff IT?
   Jawab: *Low*
9) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Gangguan tegangan listrik/tegangan listrik tidak stabil?
   Jawab: *Very Low*
10) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Ruangan *server* yang temperatur suhunya tidak sesuai standart?
   Jawab: *Very Low*
11) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Gangguan Jaringan?
   Jawab: *Low*
12) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kerusakan kabel LAN akibat hewan pengerat?
   Jawab: *Low*
13) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server*?
   Jawab: *Very Low*

4. Berapa tingkatan dampak yang terjadi yang disebabkan ancaman pada *website* tersebut?

Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Beberapa Parah	Peristiwa ancaman bisa diperkirakan terjadi beberapa parah atau bencana efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Tinggi (*High*)	Besar	Peristiwa ancaman dapat diharapkan memiliki parah atau bencana efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Sedang (*Medium*)	Serius	Peristiwa ancaman dapat diharapkan memiliki serius efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Rendah (*Low*)	Terbatas	Peristiwa ancaman dapat diharapkan memiliki terbatas efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Sangat Rendah (*Very Low*)	Diabaikan	Peristiwa ancaman dapat diharapkan memiliki diabaikan efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.

Daftar Pertanyaan:

1) Berapa tingkat dampak dari Kerusakan pada aset yang sudah menua ataupun rusak?
   Jawab: *Low*
2) Berapa tingkat dampak dari Adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam?
   Jawab: *High*
3) Berapa tingkat dampak dari Update sistem yang belum dilakukan menyebabkan system berhenti/*error*?
   Jawab: *Low*
4) Berapa tingkat dampak dari *Windows* tidak berjalan semestinya?
   Jawab: *Very Low*
5) Berapa tingkat dampak dari Pemanfaatan celah keamanan oleh pihak dalam/luar?
   Jawab: *Medium*
6) Berapa tingkat dampak dari *Server Down* yang menyebabkan halaman tidak bisa diakses?

Jawab: *Low*

7) Berapa tingkat dampak dari Akses *password* oleh karyawan yang tidak berwenang?
   Jawab: *Medium*
8) Berapa tingkat dampak dari Kesalahan operasional yang disebabkan oleh staff IT?
   Jawab: *Low*
9) Berapa tingkat dampak dari Gangguan tegangan listrik/tegangan listrik tidak stabil?
   Jawab: *Very Low*
10) Berapa tingkat dampak dari Ruangan *server* yang temperatur suhunya tidak sesuai standart?
   Jawab: *Very Low*
11) Berapa tingkat dampak dari Gangguan Jaringan?
   Jawab: *Low*
12) Berapa tingkat dampak dari Kerusakan kabel LAN akibat hewan pengerat?
   Jawab: *Low*
13) Berapa tingkat dampak dari Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server*?
   Jawab: *Very Low*

Transkrip Wawancara

Hari/tanggal wawancara : Rabu, 31 Mei 2023

Nama : Tundunsekar selaku bagian Konten

Daftar Pertanyaan:

1. **Apa saja ancaman yang pernah terjadi pada *website* tersebut?**
   Mengenai Ancaman (Adversarial dan Non-adversarial)

   - Adversarial

   Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Hampir Pasti Terjadi	Musuh adalah yakin untuk memulai peristiwa ancaman.
Tinggi (*High*)	Sangat Mungkin Terjadi	Musuh adalah sangat mungkin untuk memulai peristiwa ancaman
Sedang (*Medium*)	Agak Mungkin	Musuh adalah agak mungkin untuk memulai acara perawatan.
Rendah (*Low*)	Tidak Mungkin	Musuh adalah tidak mungkin untuk memulai peristiwa ancaman.
Sangat Rendah (*Very Low*)	Sangat Tidak Mungkin Terjadi	Musuh adalah sangat tidak mungkin untuk memulai peristiwa ancaman

   Daftar Pertanyaan:

   1) Berapa tingkat kemungkinan ancaman dari Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system?
      Jawab: *Low*

2) Berapa tingkat kemungkinan ancaman dari Kehilangan data yang sifatnya sensitif?
   Jawab: *Low*
3) Berapa tingkat kemungkinan ancaman dari Kegagalan *Backup*?
   Jawab: *Medium*

2. Berapa tingkat kerentanan pada *website* tersebut?

Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Keterangan
Sangat Tinggi (*Very High*)	Terbuka dan dapat dieksploitasi	Kerentanan terbuka dan dapat dieksploitasi, dan eksploitasinya dapat mengakibatkan dampak yang parah. Kontrol keamanan yang relevan atau perbaikan lainnya tidak dilaksanakan dan tidak direncanakan; atau tidak ada tindakan keamanan yang dapat diidentifikasi untuk memulihkan kerentanan.
Tinggi (*High*)	Memprihatinkan	Kerentanan tersebut sangat memprihatinkan, berdasarkan paparan kerentanan dan kemudahan eksploitasi dan/atau keparahan dampak yang dapat ditimbulkan dari eksploitasinya. Kontrol keamanan yang relevan atau perbaikan lainnya direncanakan tetapi tidak dilaksanakan; kontrol kompensasi sudah ada dan setidaknya efektif secara minimal.
Sedang (*Medium*)	Sedang	Kerentanan tergolong sedang, berdasarkan paparan kerentanan dan kemudahan eksploitasi dan/atau tingkat keparahan dampak yang dapat ditimbulkan dari eksploitasinya. Kontrol keamanan yang relevan atau perbaikan lainnya diterapkan sebagian dan agak efektif.
Rendah (*Low*)	Perhatian Kecil	Kerentanan menjadi perhatian kecil, tetapi efektivitas remediasi dapat ditingkatkan. Kontrol keamanan yang relevan atau perbaikan lainnya diterapkan sepenuhnya dan agak efektif.
Sangat Rendah (*Very Low*)	Tidak menjadi Perhatian	Kerentanan tidak menjadi perhatian. Kontrol keamanan yang relevan atau perbaikan lainnya sepenuhnya dilaksanakan, dinilai, dan efektif.

Daftar Pertanyaan:

1) Berapa tingkat kerentangan dari Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system?
   Jawab: *High*

2) Berapa tingkat kerentangan dari Kehilangan data yang sifatnya sensitif?
   Jawab: *High*

3) Berapa tingkat kerentangan dari Kegagalan *Backup*?
   Jawab: *High*

3. Berapa kemungkinan terjadinya ancaman pada *website* tersebut?

Kemungkinan Inisiasi Kejadian Ancaman Menyebabkan Dampak Yang Merugikan

Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Hampir Pasti Terjadi	Jika peristiwa ancaman dimulai atau terjadi, itu adalah yakin untuk memiliki dampak yang merugikan.
Tinggi (*High*)	Sangat Mungkin Terjadi	Jika peristiwa ancaman dimulai atau terjadi, itu adalah sangat mungkin untuk memiliki dampak yang merugikan
Sedang (*Medium*)	Agak Mungkin	Jika peristiwa ancaman dimulai atau terjadi, itu adalah agak mungkin untuk memiliki dampak yang merugikan.
Rendah (*Low*)	Tidak Mungkin	Jika peristiwa ancaman dimulai atau terjadi, itu adalah tidak mungkin untuk memiliki dampak yang merugikan.
Sangat Rendah (*Very Low*)	Sangat Tidak Mungkin Terjadi	Jika peristiwa ancaman dimulai atau terjadi, itu adalah sangat tidak mungkin untuk memiliki dampak yang merugikan.

Daftar Pertanyaan:

1) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system
   Jawab: *Medium*
2) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kehilangan data yang sifatnya sensitif?
   Jawab: *Medium*
3) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kegagalan *Backup*?
   Jawab: *Medium*

4. Berapa tingkatan dampak yang terjadi yang disebabkan ancaman pada *website* tersebut?

Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Beberapa Parah	Peristiwa ancaman bisa diperkirakan terjadi beberapa parah atau bencana efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Tinggi (*High*)	Besar	Peristiwa ancaman dapat diharapkan memiliki parah atau bencana efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Sedang (*Medium*)	Serius	Peristiwa ancaman dapat diharapkan memiliki serius efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Rendah (*Low*)	Terbatas	Peristiwa ancaman dapat diharapkan memiliki terbatas efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Sangat Rendah (*Very Low*)	Diabaikan	Peristiwa ancaman dapat diharapkan memiliki diabaikan efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.

Daftar Pertanyaan:

1) Berapa tingkat dampak dari Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua system?

   Jawab: *Very High*

2) Berapa tingkat dampak dari Kehilangan data yang sifatnya sensitif?

   Jawab: *Very High*

3) Berapa tingkat dampak dari Kegagalan *Backup*

   Jawab: *Very High*

Transkrip Wawancara

Hari/tanggal wawancara : Rabu, 31 Mei 2023

Nama : Rahmi Juwita Sukma selaku bagian Konten

Daftar Pertanyaan:

1. **Apa saja ancaman yang pernah terjadi pada *website* tersebut?**
   Mengenai Ancaman (Adversarial dan Non-adversarial)

   - Adversarial

   Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Hampir Pasti Terjadi	Musuh adalah yakin untuk memulai peristiwa ancaman.
Tinggi (*High*)	Sangat Mungkin Terjadi	Musuh adalah sangat mungkin untuk memulai peristiwa ancaman
Sedang (*Medium*)	Agak Mungkin	Musuh adalah agak mungkin untuk memulai acara perawatan.
Rendah (*Low*)	Tidak Mungkin	Musuh adalah tidak mungkin untuk memulai peristiwa ancaman.
Sangat Rendah (*Very Low*)	Sangat Tidak Mungkin Terjadi	Musuh adalah sangat tidak mungkin untuk memulai peristiwa ancaman

Daftar Pertanyaan:

1) Berapa tingkat kemungkinan ancaman dari Menggunakan *password* yang lemah/default *password*?
   Jawab: *Medium*

- Non-adversarial

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Hampir Pasti Terjadi	Kesalahan, kecelakaan, atau tindakan alam adalah hampir pasti terjadi; atau terjadi lebih dari 100 kali setahun.
Tinggi (*High*)	Sangat Mungkin Terjadi	Kesalahan, kecelakaan, atau tindakan alam adalah sangat mungkin terjadi; atau terjadi antara 10-100 kali setahun.
Sedang (*Medium*)	Agak Mungkin	Kesalahan, kecelakaan, atau tindakan alam adalah agak mungkin teriadi; atau terjadi antara 1-10 kali setahun.
Rendah (*Low*)	Tidak Mungkin	Kesalahan, kecelakaan, atau tindakan alam adalah tidak mungkin terjadi; atau terjadi kurang dari setahun sekali, tetapi lebih dari sekali setiap 10 tahun.
Sangat Rendah (*Very Low*)	Sangat Tidak Mungkin Terjadi	Kesalahan, kecelakaan, atau tindakan alam adalah sangat tidak mungkin terjadi; atau terjadi kurang dari sekali setiap 10 tahun.

Daftar Pertanyaan:

1) Berapa tingkat kemungkinan ancaman dari Terjadi kesalahan dalam pengelolahan data oleh staff IT?
   Jawab: *Low*

2. Berapa tingkat kerentanan pada *website* tersebut?

Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Keterangan
Sangat Tinggi (*Very High*)	Terbuka dan dapat dieksploitasi	Kerentanan terbuka dan dapat dieksploitasi, dan eksploitasinya dapat mengakibatkan dampak yang parah. Kontrol keamanan yang relevan atau perbaikan lainnya tidak dilaksanakan dan tidak

Skala	NIST SP 800-30	Keterangan
		direncanakan; atau tidak ada tindakan keamanan yang dapat diidentifikasi untuk memulihkan kerentanan.
Tinggi (*High*)	Memprihatinkan	Kerentanan tersebut sangat memprihatinkan, berdasarkan paparan kerentanan dan kemudahan eksploitasi dan/atau keparahan dampak yang dapat ditimbulkan dari eksploitasinya. Kontrol keamanan yang relevan atau perbaikan lainnya direncanakan tetapi tidak dilaksanakan; kontrol kompensasi sudah ada dan setidaknya efektif secara minimal.
Sedang (*Medium*)	Sedang	Kerentanan tergolong sedang, berdasarkan paparan kerentanan dan kemudahan eksploitasi dan/atau tingkat keparahan dampak yang dapat ditimbulkan dari eksploitasinya. Kontrol keamanan yang relevan atau perbaikan lainnya diterapkan sebagian dan agak efektif.
Rendah (*Low*)	Perhatian Kecil	Kerentanan menjadi perhatian kecil, tetapi efektivitas remediasi dapat ditingkatkan. Kontrol keamanan yang relevan atau perbaikan lainnya diterapkan sepenuhnya dan agak efektif.
Sangat Rendah (*Very Low*)	Tidak menjadi Perhatian	Kerentanan tidak menjadi perhatian. Kontrol keamanan yang relevan atau perbaikan lainnya sepenuhnya dilaksanakan, dinilai, dan efektif.

Daftar Pertanyaan:

1) Berapa tingkat kerentangan dari Menggunakan *password* yang lemah/default *password*?
   Jawab: *Medium*
2) Berapa tingkat kerentangan dari Terjadi kesalahan dalam pengelolahan data oleh staff IT?
   Jawab: *Low*

3. Berapa kemungkinan terjadinya ancaman pada *website* tersebut?

Kemungkinan Inisiasi Kejadian Ancaman Menyebabkan Dampak Yang Merugikan

Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Hampir Pasti Terjadi	Jika peristiwa ancaman dimulai atau terjadi, itu adalah yakin untuk memiliki dampak yang merugikan.
Tinggi (*High*)	Sangat Mungkin Terjadi	Jika peristiwa ancaman dimulai atau terjadi, itu adalah sangat mungkin untuk memiliki dampak yang merugikan
Sedang (*Medium*)	Agak Mungkin	Jika peristiwa ancaman dimulai atau terjadi, itu adalah agak mungkin untuk memiliki dampak yang merugikan.
Rendah (*Low*)	Tidak Mungkin	Jika peristiwa ancaman dimulai atau terjadi, itu adalah tidak mungkin untuk memiliki dampak yang merugikan.
Sangat Rendah (*Very Low*)	Sangat Tidak Mungkin Terjadi	Jika peristiwa ancaman dimulai atau terjadi, itu adalah sangat tidak mungkin untuk memiliki dampak yang merugikan.

Daftar Pertanyaan:

1) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Menggunakan *password* yang lemah/default *password*?
   Jawab: *Medium*
2) Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Terjadi kesalahan dalam pengelolahan data oleh staff IT?
   Jawab: *Low*

4. Berapa tingkatan dampak yang terjadi yang disebabkan ancaman pada *website* tersebut?

Terdapat 5 Skala Penilaian:

Skala	NIST SP 800-30	Kriteria
Sangat Tinggi (*Very High*)	Beberapa Parah	Peristiwa ancaman bisa diperkirakan terjadi beberapa parah atau bencana efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.

Skala	NIST SP 800-30	Kriteria
Tinggi (*High*)	Besar	Peristiwa ancaman dapat diharapkan memiliki parah atau bencana efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Sedang (*Medium*)	Serius	Peristiwa ancaman dapat diharapkan memiliki serius efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Rendah (*Low*)	Terbatas	Peristiwa ancaman dapat diharapkan memiliki terbatas efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.
Sangat Rendah (*Very Low*)	Diabaikan	Peristiwa ancaman dapat diharapkan memiliki diabaikan efek buruk pada operasi organisasi, aset organisasi, individu organisasi lain atau Bangsa.

Daftar Pertanyaan:

1) Berapa tingkat dampak dari Menggunakan *password* yang lemah/default *password*?

   Jawab: *Medium*

2) Berapa tingkat dampak dari Terjadi kesalahan dalam pengelolahan data oleh staff IT?

   Jawab: *Medium*

Lampiran 6 Hasil Wawancara

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Ancaman (Adverserial dan Non-adverserial)				
1.	Berapa tingkat kemungkinan ancaman dari Kerusakan pada aset yang sudah menua ataupun rusak.	*Medium*		
2.	Berapa tingkat kerentangan dari Adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam.	*High*		
3.	Berapa tingkat kemungkinan ancaman dari Update sistem yang belum dilakukan menyebabkan system berhenti/*error*.	*Medium*		
4.	Berapa tingkat kemungkinan ancaman dari *Windows* tidak berjalan semestinya.	*Very Low*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Ancaman (Adverserial dan Non-adverserial)				
5.	Berapa tingkat kemungkinan ancaman dari Pemanfaatan celah keamanan oleh pihak dalam/luar.	*High*		
6.	Berapa tingkat kemungkinan ancaman dari *Server* Down yang menyebabkan halaman tidak bisa diakses.	*Medium*		
7.	Berapa tingkat kemungkinan ancaman dari Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.		*Low*	
8.	Berapa tingkat kemungkinan ancaman dari Kehilangan data yang sifatnya sensitif.		*Low*	
9.	Berapa tingkat kemungkinan ancaman		*Medium*	

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Ancaman (Adverserial dan Non-adverserial)				
	dari Kegagalan *Backup*			
10.	Berapa tingkat kemungkinan ancaman dari Menggunakan *password* yang lemah/default *password*.			*Medium*
11.	Berapa tingkat kemungkinan ancaman dari Terjadi kesalahan dalam pengelolahan data oleh staff IT.			*Low*
12.	Berapa tingkat kemungkinan ancaman dari Akses *password* oleh karyawan yang tidak berwenang.	*Very Low*		
13.	Berapa tingkat kemungkinan ancaman dari Kesalahan operasional yang disebabkan oleh staff IT.	*Very Low*		
14.	Berapa tingkat	*Low*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Ancaman (Adverserial dan Non-adverserial)				
	kemungkinan ancaman dari Gangguan tegangan listrik/tegangan listrik tidak stabil.			
15.	Berapa tingkat kemungkinan ancaman dari Ruangan *server* yang temperatur suhunya tidak sesuai standart.	*Low*		
16.	Berapa tingkat kemungkinan ancaman dari Gangguan Jaringan.	*Very Low*		
17.	Berapa tingkat kemungkinan ancaman dari Kerusakan kabel LAN akibat hewan pengerat.	*Low*		
18.	Berapa tingkat kemungkinan ancaman dari Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server*.	*Very Low*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Kerentanan				
1.	Berapa tingkat kerentangan dari Kerusakan pada aset yang sudah menua ataupun rusak	*Low*		
2.	Berapa tingkat kerentangan dari Adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam.	*High*		
3.	Berapa tingkat kerentangan dari Update sistem yang belum dilakukan menyebabkan system berhenti/*error*.	*Low*		
4.	Berapa tingkat kerentangan dari *Windows* tidak berjalan semestinya.	*Very Low*		
5.	Berapa tingkat kerentangan dari Pemanfaatan celah keamanan oleh pihak	*Medium*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Kerentanan				
	dalam/luar.			
6.	Berapa tingkat kerentangan dari *Server* Down yang menyebabkan halaman tidak bisa diakses.	*Low*		
7.	Berapa tingkat kerentangan dari Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.		*High*	
8.	Berapa tingkat kerentangan dari Kehilangan data yang sifatnya sensitif.		*High*	
9.	Berapa tingkat kerentangan dari Kegagalan *Backup*		*High*	
10.	Berapa tingkat kerentangan dari Menggunakan *password*			*Low*

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Kerentanan				
	yang lemah/default *password*.			
11.	Berapa tingkat kerentangan dari Terjadi kesalahan dalam pengelolahan data oleh staff IT.			*Low*
12.	Berapa tingkat kerentanan dari Akses *password* oleh karyawan yang tidak berwenang.	*Low*		
13.	Berapa tingkat kerentangan dari Kesalahan operasional yang disebabkan oleh staff IT.	*Very Low*		
14.	Berapa tingkat kerentangan dari Gangguan tegangan listrik/tegangan listrik tidak stabil.	*Low*		
15.	Berapa tingkat	*Very Low*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Kerentanan				
	kerentangan dari Ruangan *server* yang temperatur suhunya tidak sesuai standart.			
16.	Berapa tingkat kerentangan dari Gangguan Jaringan.	*Very Low*		
17.	Berapa tingkat kerentangan dari Kerusakan kabel LAN akibat hewan pengerat.	*Low*		
18.	Berapa tingkat kerentangan dari Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server*.	*Very Low*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Inisiasi Yang Mengasilkan Dampak				
1.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kerusakan pada aset yang sudah menua ataupun rusak.	*Low*		
2.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam.	*High*		
3.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Update sistem yang belum dilakukan menyebabkan system berhenti/*error*.	*Medium*		
4.	Berapa tingkat kemungkinan yang memiliki dampak	*Low*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Inisiasi Yang Mengasilkan Dampak				
	merugikan dari *Windows* tidak berjalan semestinya.			
5.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Pemanfaatan celah keamanan oleh pihak dalam/luar.	*Medium*		
6.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari *Server* Down yang menyebabkan halaman tidak bisa diakses.	*Low*		
7.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.		*Medium*	

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Inisiasi Yang Mengasilkan Dampak				
8.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kehilangan data yang sifatnya sensitif.		*Medium*	
9.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kegagalan *Backup*		*Medium*	
10.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Menggunakan *password* yang lemah/default *password*.			*Low*
11.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Terjadi kesalahan dalam pengelolahan data oleh			*Low*

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Inisiasi Yang Mengasilkan Dampak				
	staff IT.			
12.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Akses *password* oleh karyawan yang tidak berwenang.	*Medium*		
13.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kesalahan operasional yang disebabkan oleh staff IT.	*Low*		
14.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Gangguan tegangan listrik/tegangan listrik tidak stabil.	*Very Low*		
15.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Ruangan	*Very Low*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Inisiasi Yang Mengasilkan Dampak				
	server yang temperatur suhunya tidak sesuai standart.			
16.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Gangguan Jaringan.	*Low*		
17.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Kerusakan kabel LAN akibat hewan pengerat.	*Low*		
18.	Berapa tingkat kemungkinan yang memiliki dampak merugikan dari Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server*.	*Very Low*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Dampak				
1.	Berapa tingkat dampak dari Kerusakan pada aset yang sudah menua ataupun rusak.	*Low*		
2.	Berapa tingkat dampak dari Adanya serangan malware atau *virus* yang disebabkan oleh pihak luar/dalam.	*High*		
3.	Berapa tingkat dampak dari Update sistem yang belum dilakukan menyebabkan system berhenti/*error*.	*Low*		
4.	Berapa tingkat dampak dari *Windows* tidak berjalan semestinya.	*Very Low*		
5.	Berapa tingkat dampak dari Pemanfaatan celah keamanan oleh pihak dalam/luar.	*Medium*		
6.	Berapa tingkat dampak	*Low*		

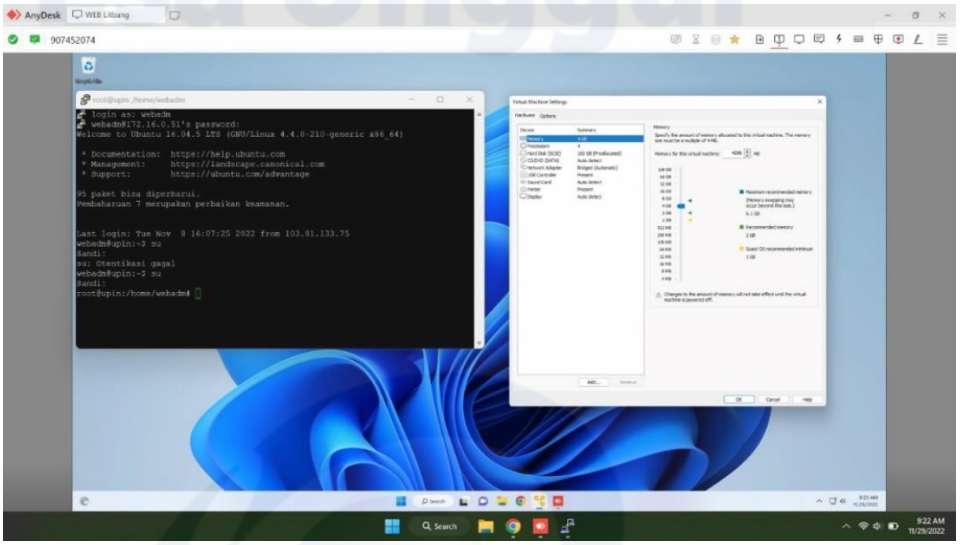
No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Dampak				
	dari *Server* Down yang menyebabkan halaman tidak bisa diakses.			
7.	Berapa tingkat dampak dari Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.		*Very High*	
8.	Berapa tingkat dampak dari Kehilangan data yang sifatnya sensitif.		*Very High*	
9.	Berapa tingkat dampak dari Kegagalan *Backup*		*Very High*	
10.	Berapa tingkat dampak dari Menggunakan *password* yang lemah/default *password*.			*Medium*
11.	Berapa tingkat dampak dari Terjadi kesalahan dalam pengelolahan data oleh staff IT.			*Medium*

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Dampak				
12.	Berapa tingkat dampak dari Akses *password* oleh karyawan yang tidak berwenang.	*Medium*		
13.	Berapa tingkat dampak dari Kesalahan operasional yang disebabkan oleh staff IT.	*Low*		
14.	Berapa tingkat dampak dari Gangguan tegangan listrik/tegangan listrik tidak stabil.	*Very Low*		
15.	Berapa tingkat dampak dari Ruangan *server* yang temperatur suhunya tidak sesuai standart.	*Very Low*		
16.	Berapa tingkat dampak dari Gangguan Jaringan.	*Low*		
17.	Berapa tingkat dampak dari Kerusakan kabel LAN akibat hewan pengerat.	*Low*		

No.	Daftar Pertanyaan	Hasil Wawancara		
		Informan 1	Informan 2	Informan 3
		Staff IT (Teknisi)	Staff IT (Konten)	Staff IT (Konten 2)
Pertanyaan Mengenai Dampak				
18.	Berapa tingkat dampak dari Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada *server*.	*Very Low*		

Lampiran 7 Foto

- *Software* dan *Hardware* pada *website*.



Terdapat *server* dengan memori 4 GB, *processors* 4, *hard disk* 100 GB, *network adapter bridged (autometic)* dan *software* yaitu *Ubuntu* 16.04.5 *ITS* (*GNU/Linux* 4.4.0-210-*generic* x86 64), *Laravel* 8.0, dan *Postgresql* 13.

- AC (*air conditioner*) pada ruangan *server*.

Terdapat AC (*air conditioner*) pada ruangan *server* dengan merk panasonic.

- Terdapat *Sun Oracle*

Terdapat *Sun Oracle* pada ruangan *server* sebagai solusi *database* "*plugin and go*" dalam satu paket, infrastruktur *server* dan jaringan dari *Sun*.

- Terdapat UPS (*Uninterruptible Power Supply*) dan ETS (*Electricity Treatment System)*

Terdapat penunjang daya, jikalau terjadi pemadaman listrik ataupun gangguan yang terjadi.

- *Finger print*

Ruangan *Server* dilengkapi dengan doorlock yang menggunakan *finger print* dan kunci.

- Foto Wawancara yang dilakukan di BSIP (Badan Standarisasi Instrumen Pertanian)

Wawancara dilakukan pada Rabu, 31 Mei 2023 di BSIP (Badan Standarisasi Instrumen Pertanian).