IT Risk Management

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

2. Monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah (WFH). Pihak perusahaan dituntut tetap dapat memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "*Employee Monitoring Software*" yang dapat dideploy sehubungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

--- Selamat bekerja ----

1. Sebuah perusahaan yang bergerak dalam bidang penjualan mendapati kebocoran data dalam sistem penyimpanan data konsumennya, yang mana data yang dikelola merupakan jenis data yang cukup confidential. Kebocoran data tersebut dapat mengakibatkan konsumen dirugikan, baik secara langsung maupun tidak langsung. Data-data tersebut meliputi data identitas diri, nomor rekening, nomor kartu kredit dan beberapa data yang lain.

dalam proses Risk Treatment yang dilakukan oleh manager IT perusahaan tersebut, resiko yang dihadapi oleh perusahaan ini berada pada level High Probability Low Impact, yang mengharuskan proses dari perbaikan dan manajemen resiko dari kebocoran data pada perusahaan ini harus di monitoring secara berkelanjutan.

langkah pertama yang dilakukan adalah membuat checlist dari proses kerja yang dilakukan oelh setiap pekerja dan juga melakukan interview kepada seluruh pegawai atau pun user terkait. Hal ini dilakukan untuk merumuskan kapn dan bagaimana ancaman ini awalnya bermula. checklist yang dilakukan, digunakan untuk membantu menyederhanakan proses yang telah dilksanakan oleh manager IT dalam penanganan kasus yang sedang terjadi.

Dari proses risk treatment tersebut, didapatkan hasil bahwa kebocoran data yang terjadi, dilakukan oleh salah satu pegawai yang bekerja di perusahaan tersebut.

hal ini dapat terjadi, karena akses ke ruang server tidak dijaga dengan cukup ketat, dimana hampir semua orang dapat masuk ke ruang server yang tidak diberikan pengamanan khusus.

Dalam rencana perbaikan yang akan dilakukan untuk meminimalkan hal serupa terjadi lagi di masa yang akan datang, maka perlu dilakukan perbaikan sistem keamanan yang berkaitan dengan hak akses ke ruang server, dan juga perbaikan dari ruangan server itu sendiri.

2.

A. Risk Identification

resiko yang dihadapi dalam pemantuan kinerja karayawan dalam masa pandemik ini, salah satunya adalah masalah produktivitas yang sulit dipantau. Dengan kebebasan waktu untuk bekerja dan tanpa adanya pengawasan secara langsung dari atasan seringkali membuat seorang karyawan untuk bekerja semaunya sendiri, dan cenderung mengabaikan peforma yang bekaitan langsung dengan produktivitas. Maka dari itu, perusahaan perlu mempunyai suatu software pemantau yang mampu menyediakan feature seperti timesheet, time tracking, penjadwalan, dan sampai pada laporan-laporan yang dibutuhkan perusahaan.

B. Risk Estimation

Resiko yang dihadapi tersebut diperkirakan dapat diatasi dengan terpantaunya aktivitas karyawan yang dimonitor secara daring oleh suatu perangkat lunak yang dikelola oleh perusahaan. Maka dari itu perusahaan dapat menggunakan aplikasi Hubstaff yang mempunyai features seperti yang disebutkan diatas sesuai dengan kebutuhan dan identifikasi masalah yang telah dilakukan sebelumnya. Hubstaff memungkinkan manajemen untuk memantau karyawan menggunakan sistem GPS, dan juga menyediakan Project Manajemen yang dapat dugunakan untuk memantau kinerja team demi produktifitas perusahaan.

Nama:Hendra Yada Putra
Kelas:MTI Reg B angkatan 21

UAS IT Risk Management

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

2. Monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah (WFH). Pihak perusahaan dituntut tetap dapat memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "*Employee Monitoring Software*" yang dapat dideploy sehubungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

Jawaban:

1. Risk treatment merupakan tindak lanjut dari hasil risk evaluation. Dimana risk evaluation ini sendiri merupakan sub kegiatan dan merupakan rangkaian akhir dari risk assessment. Output dari risk evaluation sendiri sudah berupa daftar hasil penilaian risko serta proritasnya terhadap contex/ruang lingkup yang sudah ditentukan diawal kegiatan proses risk management ini untuk diidentifikasi (penentuan kreteria risk evaluasi pada tahap Context Establishment), output dari risk evaluation ini nantinya akan diproses pada tahapan risk treatment.

   Pada tahap risk treatment, setiap risk dari output risk evaluation akan dikendalikan baik dengan opsi :
   a. menurunkan nilai risiko (risk reduction), atau
   b. menerima risiko (risk retaintion), atau
   c. menghidari risiko(risk avoidance) atau
   d. mentransfer risiko (risk transfer) .

   Pemilihan opsi dilakukan dengan mempertimbangkan nilai dari risiko itu sendiri, biaya yang timbul dari opsi treatmen yang dipilih dan manfaat dari opsi treatmen risiko yang dipilih.

Sebagai Contoh implementasinya, suatu organisasi melakukan bekerja sama dengan banyak mitra terkait dengan pembayaran, secara bisnis kerja sama ini sangat menguntungkan organisasi dan hal ini menjadi salah satu proritas utama dalam target bisnis organisasi.

Pola kerjasama tersebut mengharuskan organisasi melakukan koneksi data elektronik dengan mitra menggunakan metode host to host, namun koneksi yang tersedia untuk terhubung dengan mitra hanyalah koneksi internet publik. Setelah di asessement risikonya ternyata hasil evaluasi menunjukkan kerjasama ini memiliki risiko yang tinggi.

Mulai dari identifikasi ancaman dari area internet dimana data yang lewat merupakan data sensitif (data pembayaran) yang dapat dimanipulasi karena protokol koneksi masih berupa protokol http yang tidak aman, ditambah lagi dari sisi mitrapun belum memiliki kemampuan untuk mengembangkan aplikasi menggunakan protokol yang aman. Secara proses alur data, belum ada juga prosedur yang menunjukkan pengamanan terhadap kegiatan ini dan setelah dihitung dampaknya terhadap risiko yang dii, risiko kerjasama ini dapat merugikan kedua pihak, mulai dari kerugian finansial hingga reputasi.

Mengingat kerjasama ini adalah proritas dari organisasi maka hasil evaluasi risiko ini dilakukan treatmen, dan dengan mempertimbangkan dampak, biaya dan manfaat yang diperoleh treatmen yang dipilih organisasi adalah dengan menghidari risiko tersetbu terjadi (avoidance risiko) dengan langkah:

1. melakukan pengamanan jalur internet dengan peneyediaan firewall dan pengaktifan fungsi tunneling untuk mengamankan protokol http yang masih digunakan
2. Membuat control berupa prosedur pengamanan terhadap kerjasama tersebut, dan diawasi secara berkala.

2. Software yang digunakan oleh karyawan saat melakukan kerja secara WFH adalah aplikasi Remote Team Viewer

   Tahap pertama yang dilakukan adalah Context Establishment

   1. Menentukan ruang lingkup dan batasan terhadap penggunaan team viewer, baik dengan menentukan siapa saja atau dari bagian kerja mana saja yang boleh melakukan akses remote.
   2. Menentukan kerteria risk evaluasi, berupa asset mana saja yang boleh diremote untuk diniliai risknya, aturan mana saja terkait penggunaan remote, dan operasi bisnis mana yang boleh dilakukan secara remote terkait nilai risk assessmen nantinya.

   Tahap Risk Idetification

   Dari kegiatan tersebtu dapat diidentifikasi risiko berupa:

1. Remote yang dilakukan oleh karyawan diluar jam kerja, yang berdampak pada kemungkinan pegawai melakukan fraud karena tidak adanya kontrol atasan
2. Authentikasi remote yang kemungkinan tidak disharing ke pihak lain yang tidak memiliki wewenang
3. Kurangnya kontrol terhadap operasi kerja atasan saat karyawan melakukan remote.
4. PC atau laptop rumah milik karyawan yang tidak aman, dapat memungkintkan timbulnya penularan virus atau malware
5. Control administrasi dan prosedur untuk penggunaan akses Teamviewer yang belum direview berdampak timbulnya celah yang dapat dimanfaatkan oleh karyawan yang tidak bertanggung jawab

Nama : Muhammad Iqbal Risky Tanjung
Kelas : MTI Reg B 21
Keterangan : UAS IT Risk Management

1. Hubungan antara Risk Treatment dengan evaluasi yang sebelumnya, risk treatment itu lebih mengindari kegiatan yang akan lebih meningkatkan resiko seperti:
   - **Risk Avoidance**
     Sebuah keputusan untuk menghapus sama sekali peluang kemungkinan terjadinya resiko. Contoh eris takut menaiki lift yang kurang meyakinkan, karena eris pernah terkurung di dalam lift. Maka eris jangan menaiki lift yang kurnag meyakinkan lagi.
   - **Risk Financing**
     Bentuk dari risk ini meliputi pengaturan penyediaan dana untuk memenuhi atau memodifikasi konsekunsi keuangan yang terjadi
   - **Risk Sharing**
     Risk Sahring ini merupakan system berbagi masalah denganc ara menanggung masalh bersama-sama.
   - **Risk Retention**
     Membiayai atau membayar kerugian seseorang dengan *self assumption* of risk atau *self insurance.* Contoh orang0orang tidak mengasuransikan kehilangan handphone atau volpen mahalnya. Jadi jika terjadi kehilangan maka di tangung oleh pemilik.
   - **Risk Residual**
     Risk ini adalah jumlah resiko atau bahaya yang terkait dengan suatu tindakan atau peristiwa yang tersisa setelah mengalami sebuah resiko.
   - **Risk Resilience**
     Adalah sebuah kemampuan adaptif suatu organisasi dalam seatu lingkungan yang berubah dan kompleks.

2. Memang dalam keadaan sepeti ini mengharuskan kita bekerja dari rumah, banyak aplikasi atau software yang dapat kita gunakan untuk melakukan meeting secara online. Contohnya, kita bias menggunkan zoom, cloudx, google meeting dan yang lainnya. Namun utnuk menjaga kehadian karyawan kita juga dapat menggunakan software absensi online yang banyak di gunakan oleh perusahaan atau organisasi lain. Namun kerugian dari berbagai fitur tadi, seperti absensi online software itu mengharuskan kita mendaftarkan nama

karyawan dan data yang lainnya. Itu dapat menjadi sebuah resiko bagi sebuah organisasi tau perusahaan yang sedang bersaing. Karna tidak semua software yang di buat oleh orang itu aman tanpa adanya hacking. Apalagi keadaan yang sekarang mengharuskan kita bekerjad dari rumah.

IT Risk Management

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

2. Monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah (WFH). Pihak perusahaan dituntut tetap dapat memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "*Employee Monitoring Software*" yang dapat dideploy sehubungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008!
   (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

--- Selamat bekerja ----

Jawaban 1:

ISO 27005-2008 merupakan pedoman mengenai Information Security Risk Management yang dapat digunakan perusahaan untuk mengantisipasi dan menproses Risk Business. Tahap-tahap tersebut terdiri dari context establishment, identifikasi resiko, analisis resiko, evaluasi resiko, risk treatment, dan risk acceptance. Pada tahap risk assesment, output yang didapatkan adalah hasil dari evaluasi resiko.

Hasil Evaluasi resiko berisikan daftar analisis resiko yang dihadapi perusahaan dan menjadi dasar pengambilan keputusan penanganan resiko. Setelah hasl evalusi resiko diketahui maka langkah berikutnya adalah risk treatment. Tahap risk treatment berisikan panduan untuk menyelesaikan daftar evaluasi resiko sesuai dengan keadaan dan priotitas penanganan. Berikut merupakan beberapa cara risk treatment: [1]

1. Risk Reduction

   Penanganan resiko dengan mengurangi dampak dari resiko.

2. Risk Retention

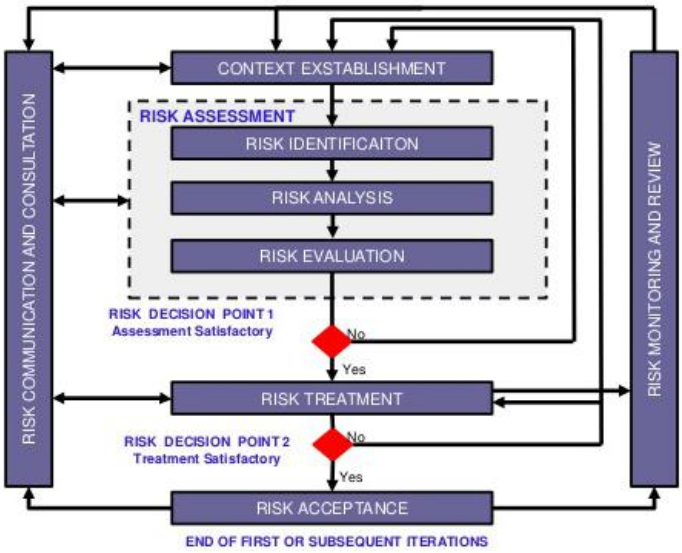
   Penanganan resiko tanpa melakukan tindakan apapun

3. Risk Avoidance

   Penanganan resiko dengan cara tidak melanjutkan kegiatan bisnis karena resiko yang dimunculkan.

4. Risk Transfer

   Penanganan resiko dengan cara mengurangi memberikan tanggung jawab penganganan ke pihak lain untuk mengurangi dampak resiko ke perusahaan



Gambar ISO 27005-2008 Information Security Risk Management

Sebagai studi kasus, di Indonesia ada sebuah perusahaan layanan transportasi dan jasa yang dinamakan GoJek. Gojek didirikan oleh Nadiem Makarim untuk membantu menghubungkan ojek dan pengguna jasa transportasi di Kota Jakarta. Proses pengenalan dan pengembangan sistem layanan transportasi ini dimulai dari tahun 2010 dan telah beroperasi sampai saat ini dan menjadi *super app.* Namun bila kita melihat sejarahnya pada tahun 2015, ada fenomena dimana aplikasi yang dibangun ini mendapat penolakan dari ojek konvensional. Setelah masalah ini dievalusi dan di*breakdown,* faktor yang diisukan pada fenomena penolakan ini seperti masalah ketimpangan ekonomi dan kecemburuan sosial. [2]

Pada saat itu pihak manajemen GoJek perlu menentukan langkah yang sesuai untuk menangani fenomena tersebut. Bila fenomena dihubungkan dengan risk treatment dan hasil evaluasi sesuai dengan cara penanganan resiko, maka dapat dijabarkan sebagai berikut

Hasil Evaluasi Resiko	Jenis Risk Treatment	Tindakan
Ketimpangan pendapatan ekonomi antar ojol dan ojek konvensional	Risk Reduction	Menyesuaikan nilai pokok perlayanan dan keuntungan operator sesuai dengan kebijakan dari Menhub
Munculnya kecemburuan sosial	Risk Reduction	Melakukan open recruitment dengan syarat yang sederhana serta melaksanakan

pada masyarakat		sharing informasi kebutuhan trend masyarakat dan finansial

Referensi :

[1] British Standard Institute. 2008. Information Technology — Security Techniques — Information Security Risk Management

[2] https://www.kompasiana.com/gianalfiani/5a02d7a38325cc4a7308e792/kontroversi-antara-gojek-dengan-ojek-konvensional

Jawaban 2:

Contoh Software "*Employee Monitoring Software*"***: Samepage*** *(https://www.samepage.io)*

1. CONTEXT ESTABLISHMENT

Analisis Software	Kriteria Penilaian	Analisis
Kriteria Dasar Evaluasi	Business Process	Aplikasi Collaboration Software
	Nilai strategis	Memiliki Group, timeline schedule, dan akses file secara online
	Operasional	Diperlukan sistem yang bersifat mobile dan terkontrol
	Kerahasiaan dan Integritas	Aplikasi hanya dapat diakses oleh manajer dan karyawan yang berkepentingan dengan akses login
Lingkup dan Batasan	Struktur Organisasi	Mampu diikuti seluruh staff perusahaan
	Assets	Device milik staff berupa smatphone atau PC
Organisasi Pelaksana	Penanggung jawab Pengguna Aplikasi	Masing-masing user
	Penanggung jawab Pemeliharaan Software	Pihak developer aplikasi
	Penanggung jawab Dokumentasi Proses	Masing-masing user dengan sistem sharing file / berkas

2. IDENTIFIKASI RESIKO

1. **Identifikasi Asset**

a) Asset Tangible : kantor, peralatan dan fasilitas, karyawan

b) Asset Intangible : software perusahaan yang sudah ada

2. **Identifikasi Ancaman**

Type	*Threat*	*Origin*
Physical Damage	Kerusakan Device	A,D,E
Loss of essential service	Hilang jaringan / tidak bisa mengakses internet	A,D,E
Compromise of information	Pencurian Data	D
Technical failure	Software Error	A
Unauthorised Actor	User tanpa akses atau Hacker	D
Compromise of Failure	Ketidakpahaman Pengguna	A,D

**) A=Acidental , D= Deliberate, E=Environment*

3. **Identifikasi Kontrol yang Berjalan**

Aplikasi Samepage merupakan aplikasi yang didedikasikan untuk media collaboration software. Beberapa fitur seperti Google Calendar, Sharing File (seperti google drive), chat, dan time schedule telah diintegrasi menjadi satu aplikasi. Penggunaan sistem tidak akan menggangu sistem yang sudah adaseperti Absensi atau finance karena bersifat sebagai aplikasi kontrol dan proggress report karyawan.

4. **Identifikasi Kelemahan**

Type	*Vulnerabilities*	*Threat*
Hardware	Device rusak	Bisnis terhambat
Software	Aplikasi memiliki bug	Bisnis terhambat
Network	Tidak ada jaringan internet	Bisnis terhambat
Personnel	Pengguna tidak ada	Bisnis terhambat
	Ketidakpahaman Pengguna	Bisnis terhambat

5. **Identifikasi Dampak**

Type	*Keadaan*	*Dampak*

Investigation and repair time	Aplikasi stable	Tidak Ada
(Work)time lost	Aplikasi stable	Tidak Ada
Opportunity lost	Aplikasi stable	Tidak Ada
Health and Safety	Aplikasi tidak berdampak pada kesehatan	Tidak Ada
Financial cost of specific skills to repair the damage	Aplikasi bersifat gratis dan dapat memberi masukan ke developer	Tidak Ada
Image reputation and goodwill	Aplikasi diciptakan dari luar negri	Data yang terdapat pada aplikasi dimuat pada database luar dan perlu dikontrol

Nama: Muhammad Ichsan
Kelas: B

IT Risk Management

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

2. Monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah (WFH). Pihak perusahaan dituntut tetap dapat memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "*Employee Monitoring Software*" yang dapat dideploy sehubungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

--- Selamat bekerja ----

1. **Hubungan Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko** karena dalam tahapan Risk Treatment telah dilakukan proses Risk Assessment dan Risk Assessment sendiri terdiri dari Risk Identification, Risk Analysis dan Risk Evaluation sehingga apabila kita telah menyelesaikan proses tahapan Risk Treatment maka kita lebih mudah untuk mengidentifikasi gejala resiko dan tempat dimana resiko yg akan timbul pada system keamanan kita sehingga dari hasil identifikasi dari resiko yang akan timbul tersebut kita dapat segera mengevaluasi segala bentuk ancaman resiko yang akan timbul terhadap system keamanan informasi pada perusahaan kita dikemudian hari.

   Contoh: perusahaan kita mengundang pihak auditor eksternal untuk mengaudit system keamanan kita dimana saja celah kelemahan pada system kemanan perusahaan kita sehingga kita dapat mengantisipasi kelemahan pada system perusahaan kita sebelum risiko tersebut terjadi.

2 A. Langkah pertama Communication and Consulting

Sebuah risk assessment bergantung kepada cara komunikasi dan cara berkonsultasi antara pihak yang melakukan risk assessment dengan pihak stakeholder yang terkait. stakeholder tersebut harus mengetahui seluk beluk apa saja yang mereka dalami dan mampu mengkomunikasikan resiko-resiko yang ada kepada pihak yang melakukan risk assessment. Proses ini berlangsung pada setiap risk management process, tidak hanya pada tahap risk assessment saja. Hal ini dilakukan agar masukan dan keluaran dari risk management proses sesuai dengan tujuan dari organisasi dan stakeholder dan tidak terjadi kesalahpahaman.

Stakeholder

Para stakeholders dari proyek EMS ini terdiri dari beberapa kelompok yang terlibat selama dalam pengembangan dari produk kami, yaitu :

- Pemilik Sistem (System Owner) : bertanggung jawab atas pendanaan, pengoperasian dan perawatan sistem.
- Pengguna Sistem (System User) : pihak yang akan menggunakan sistem EMS ini nantinya.
- Pembangun Sistem (System Builder), dalam proyek EMS ini adalah kami selaku pembangun sistem EMS ini dan terdiri atas :
    - Manajer Proyek
        - Bertanggung jawab atas kelancaran pembangunan proyek serta koordinasi antara pembangun sistem.
    - Sekretaris
        - Bertanggung jawab atas segala kelancaran administrasi selama pembangunan proyek
    - Finance
        - Bertanggung jawab atas anggaran dana, serta mengusahakan tersedianya dana selama proses pembangunan proyek
    - Analis Sistem
        - Sebagai penghubung komunikasi antara pemilik, pengguna, serta pembangun sistem
    - Designer
        - Bertanggung jawab atas desain antarmuka program, serta desain grafis terhadap segala sesuatu yang berhubungan dengan proyek EMS ini
    - Programmer
        - Sebagai pembangun sistem dalam hal teknis, spesialis dalam mengonversikan persyaratan dan prosedur bisnis ke dalam bahasa komputer
    - Database Administrator
        - Bertanggung jawab dalam mendesain dan mengkoordinasikan perubahan ke database perusahaan
    - Pakar Jaringan
        - Bertanggung jawab atas perancangan, instalasi, *troubleshooting,* dan pengoptimalan jaringan

B. Langkah Kedua Monitoring and review

Setelah dilakukan risk treatment, kemudian hasil setelah treatment tersebut akan di pantau dan dilakukan kontrol dan evaluasi. Evaluasi didasarkan dari tujuan risk management proses itu sendiri. terkadang sebuah proses risk management akan mempunyai resiko tambahan yang menyertainya, atau resiko baru akan muncul. Oleh karena itu, setelah proses monitoring, akan dilakukan kembali risk management proses untuk melakukan tanggapan terhadap resiko baru yang muncul.

UAS IT Risk Management

Nama : Muhammad Wahyudi

NIM : 192420023

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

2. Monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah (WFH). Pihak perusahaan dituntut tetap dapat memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "*Employee Monitoring Software*" yang dapat dideploy sehubungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

--- Selamatbekerja ----

Jawaban

1 A.Perlakuan risiko (risk treatment)

Proses untuk memodifikasi risiko. Risk treatment dapat meliputi:

-Menghindari risiko dengan memutuskan tidak memulai atau melanjutkan kegiatan yang dapat meningkatkan

risiko;

-mengambil atau meningkatkan risiko untuk mengejar opportunity;

-mengilangkan sumber risiko;

-mengubah likelihood;

-mengubah konsekuensi;

-membagi risiko debfab pihak lain;

-mempertahankan risiko dengan keputusan yang terinformasi.

Risk treatment untuk menghadapi konsekuensi negatif adalah meliputi “risk mitigation”, “risk elimination”, “risk prevention” dan “risk reduction”.

Kontrol (control)

Tindakan yang memodifikasi risiko. Kontrol meliputi proses, kebijakan, perangkat, praktik, atau tidakan lainnya yang memodifikasi risiko. Kontrol mungkin tidak selalu dapat menghasilkan efek modifikasi sesuai dengan yang diasumsikan atau diinginkan.

Penghindaran risiko (risk avoidance)

Keputusan untuk tidak terlibat dalam, atau untuk menarik diri dari, kegiatan supaya tidak terkena suatu resiko tertentu. Risk avoidance dapat didasarkan pada hasil evaluasi risiko dan/atau peraturan dan kewajiban hukum.

Pembagian risiko (risk sharing)

Bentuk dari risk treatment yang meliputi ditribusi risiko yang telah disepakati dengan pihak lain. Hukum atau persyaratan peraturan dapat membatasi, melarang atau mandat risk sharing. Risk sharing dapat dilakukan melalui asuransi atau bentuk lain dari kontrak. Sejauh mana risiko didistribusikan dapat bergantung pada keandalan dan kejelasan pengaturan pembagian. Transfer risiko adalah bentuk dari risk sharing.

Pembiayaan risiko (risk financing)

Bentuk dari risk tratment meliputi pengaturan kontingen untuk penyediaan dana untuk memenuhi atau memodifikasi konsekuensi keuangan yang terjadi.

Retensi risiko (risk retention)

Penerimaan terhadap keuntungan yang berpotensi dari keuntungan, atau beban kerugian, dari risiko tertentu. Risk retention meliputi penerimaan dari residual risk, dan level of risk yang dipelihara tergantung pada risk criteria.

Risiko residual (residual risk)

Risiko yang tersisa setelah dilakukan risk treatment. Residual risk dapat mengandung risiko yang belum teridentifikasi dan residual risk juga sering disebut sebagai “retained risk”.

Ketahanan (resilience)

Kemampuan adaptif suatu organisasi dalam suatu lingkungan yang berubah dan kompleks.

. Istilah yang berhubungan dengan pengawasan dan pengukuran (monitoring and measurement)

Pengawasan (monitoring)

Pemeriksaan berkelanjutan, pengawasan, pengamatan kritis atau penentuan status untuk mengidentifikasi perubahan dari tingkat kinerja yang diperlukan atau diharapkan. Pemantauan dapat

diaplikasikan dalam sebuah framework manajemen risiko, proses manajemen risiko, risiko, atau kontrol.

Rapat (review)

Kegiatan yang dilakukan untuk menentukan keberlanjutan, kelayakan, dan efektivitas dari suatu hal dalam mencapai tujuan yang ditentukan. Rapat (review) dapat diaplikasikan dalam sebuah framework manajemen risiko, proses manajemen risiko, risiko, atau kontrol.

Pelaporan risiko (risk reporting)

Bentuk komunikasi ditujukan untuk menginformasikan suatu stakeholder internal atau eksternal dengan menyediakan informasi terkait kondisi terkini terkait risiko dan manajemennya.

Register risiko (risk register)

Catatan informasi tentang risiko yang teridentifikasi. Istilah “risk log” lebih sering digunakan dibandingkan “risk register”.

Profil risiko (risk profile)

Deskripsi himpunan dari risiko. Himpunan dari risiko dapat mengandung risiko yang berhubungan terhadap organisasi secara keseluruhan, sebagian dari organisasi, atau hal lain yang didefinisikan.

. Audit manajemen risiko (risk management audit)

Proses yang sistematik, mandiri, dan terdokumentasi untuk mengumpulkan bukti dan mengevaluasinya secara objektif untuk menentukan sejauh mana framework manajemen risiko dapat memadai dan efektif.

B. Istilah yang berhubungan dengan risk evaluation

Evaluasi risiko (risk evaluation)

Proses membandingkan hasil dari analisis risiko dengan kriteria risiko untuk menentukan apakah risiko dan ukurannya dapat diterima dan ditoleransi. Evaluasi risiko akan membantu penentuan risk treatment.

Perilaku risiko (risk attitude)

Pendekatan organisasi untuk menilai dan mengejar, mempertahankan, mengambil atau berpaling dari risiko.

Risk appetite

Jumlah dan jenis risiko yang akan dipertahankan atau dikejar oleh organisasi.

Toleransi risiko (risk tolerance)

Kesiapan stakeholder atau organisasi untuk menanggung risiko setelah dilakukan risk treatment untuk mencapai tujuannya. Toleransi risijo dapat dipengaruhi oleh persyaratan peraturan atau hukum

Risk aversion

Tindakan untuk berpaling dari risiko.

Agregasi risiko (risk aggregation)

Kombinasi beberapa risiko ke dalam sebuah risiko untuk mengembangkan pemahaman terhadap risiko secara keseluruhan.

penerimaan risiko (risk acceptance)

Keputusan terinformasi untuk mengambil sebuah risiko tertentu. Penerimaan risiko dapat terjadi tanpa risk treatment atau selama proses pelaksanaan risk treatment.

2 A. Pastikan Channel Komunikasi Tersedia dan Lancar

Saat menerapkan *work from home*, Anda harus tetap berkomunikasi, terutama dengan partner kerja. Untuk itu, pastikan semua channel komunikasi seperti Whatsapp, Telegram, atau Slack selalu *standby*. Jangan tidak ada jawaban ketika teman kantor membutuhkan Anda.

Jika perlu, Anda bisa melakukan *video call* atau *conference call* dengan menggunakan *tools* seperti Zoom, Skype, atau Google Meeting. Memastikan ketersediaan *channel* komunikasi adalah hal utama yang harus dipenuhi oleh setiap orang ketika melakukan *work from home*.

Selain itu, penyampaian informasi juga harus cepat dan tepat sasaran. Anda bisa menggunakan *channel* komunikasi seperti *social messaging* ataupun aplikasi internal yang Anda gunakan di kantor. Jika Anda menggunakan **Talenta**, Anda bisa menggunakan fitur seperti **Broadcast Message** untuk melakukan hal tersebut.

B. Pastikan Kehadiran Karyawan Terkontrol

Anda harus memastikan kehadiran karyawan tetap terkontrol meski menerapkan *work from home*. Salah satu caranya adalah dengan menggunakan aplikasi Human Resources Information System (HRIS) yang memiliki fitur absensi dari mobile seperti Talenta.

Fitur absensi mobile atau **Live Attendance** dapat membantu HR seperti Anda untuk memantau langsung kehadiran karyawan yang bekerja dari rumah. Prinsipnya adalah melalui *check–in* dan *check–out* yang dapat dilakukan langsung dari ponsel karyawan. Setiap kali karyawan bekerja, mereka dapat melakukan *check–in*. Begitu pun setelah selesai bekerja, mereka dapat melakukan *check–out*. Live Attendance dalam Talenta juga dilengkapi dengan fitur *selfie check–in*. Anda sebagai HR dapat melihat lokasi absen mereka melalui *dashboard* yang terupdate secara *real-time* setiap kali

karyawan melakukan *clock–in* atau *clock–out*. Dengan begitu, Anda tetap bisa mengawasi apakah karyawan bekerja atau tidak.

IT Risk Management

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!
   ⇨ Sebuah Perawatan Resiko (Risk Treatment) berkaitan dengan bagaimana resiko perlu ditangani (berdasarkan evaluasi sebelumnya yaitu risk assessment). Opsi Risk Treatment harus dipilih berdasarkan hasil penilaian risiko, biaya yang diharapkan untuk menerapkan opsi ini dan manfaat yang diharapkan dari opsi ini.

   Bagaimana kita mengetahui rencana kita benar –benar berjalan? Tentu jika belum melewati proses risk assessment, hal ini sulit atau opsi ini sulit untuk diterapkan, karena buta informasi akan objek dan yang kita tak bisa melakukan suatu perawatan tanpa mengetahui informasi dari objek sendiri, tanpa melakukan analisis dan evaluasi sendiri (risk assessment) oleh sebab itu perlunya menentukan identifikasi risiko dengan tujuan untuk menentukan apa yang dapat terjadi yang menyebabkan potensi kerugian, dan untuk mendapatkan wawasan tentang bagaimana, di mana, dan mengapa kerugian tersebut dapat terjadi.

   Sebab dalam penerepannya, evaluasi resiko (risk assessment) menjelaskan penilaian atau evaluasi dimana ini sangat berpengaruh pada tindakan yang akan dilakukan selanjutnya. Setiap spesifikasi yang dijelaskan pada evaluasi sebelumnya memberikan gambaran keadaan dari objek itu sendiri dimana hal ini menjelaskan bahwa bagaimana keadaan objek apakah perlu dirawat atau tidak? Mana yang perlu dirawat? Bagian mana yang beresiko? Dll.

   Selain itu dari evaluasi sebelumnya kita dapat memperkirakan biaya dan manfaat setelah melakukan perawatan. Apakah memiliki dampak berbeda atau tidak. Tentunya ini dipertimbangkan.

   Seperti pada contohnya, dalam sebuah perusahaan surat kabar dan berita – berita seputar negara. Terdapat 20-30 pc menggunakan windows. Setelah dilakukan identifikasi (risk assesment) didapat bahwa microsoft masih dalam versi lama yaitu windows 7 sehingga jika dokumen masuk dalamnya akan berubah format. Hal ini mendapat himbauan bahwa pemakaian windows berlisensi dengan harga dan manfaat yang setidaknya dapat terjangkau oleh pendapatan dari printing. dan tentunya ada penanggung jawab ketika terdapat penambahan masa lisensi, serta training dan setidaknya terdapat seseorang yang dapat ditanyai mengenai permasalah jika salah satu karyawan mendapati ketidak mengertian dalam interaksi manusia dan komputer. Dari sini dapat diidentifikasi harga dan manfaatnya. Dan tentu hal ini perlu dibicarakan dengan perusahaan.

2. Monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah (WFH). Pihak perusahaan dituntut tetap dapat memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "*Employee Monitoring Software*" yang dapat dideploy sehub0ungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

--- Selamat bekerja ----

UNIVERSITAS BINA DARMA

A. Sejarah Universitas

Gambar 2.1. Universitas Bina Darma

Universitas Bina Darma (UBD) memiliki 4 (empat) gedung kampus yang terletak di Jalan Jenderal A. Yani Palembang. Kampus Utama terletak di no. 12 menempati lahan seluas 3057 m2, Kampus B terletak di no 3 seluas 4723 m2, Kampus C terletak di no 15 seluas 1206 m2, Kampus D terletak di no 24 seluas 238 m2. Atas prakarsa Prof. Ir. H. Bochari Rachman, M.Sc. dan kawan-kawan pada tanggal 28 Desember 1993 didirikan Yayasan Bina Darma dengan Akte Notaris Alia Ghani, S.H. Nomor: 95. Kemudian tanggal 10 Maret 2001 terjadi perubahan pendiri Yayasan Bina Darma berdasarkan akte notaris Thamrin nomor :6. Maksud dan tujuan didirikannya Yayasan ini antara lain untuk turut serta secara aktif membantu pemerintah dalam melaksanakan program pembangunan nasional dalam rangka mewujudkan cita-cita nasional dan turut serta membantu pemerintah dalam upaya mencerdaskan kehidupan bangsa. Kemudian pada tanggal 30 April 2001 berdasarkan Akte Notaris Thamrin nomor : 36, Yayasan Bina Darma mengambil alih pengelolaan Sekolah Tinggi Bahasa Asing (STBA) Graha Darma. Untuk itu Yayasan Bina Darma mengubah nama Sekolah Tinggi Bahasa Asing (STBA) Graha Darma menjadi Sekolah Tinggi Bahasa Asing (STBA) Bina Darma berdasarkan Surat Keputusan Menteri Pendidikan Nasional Republik Indonesia nomor : 143/D/0/2001 tanggal 27 Agustus 2001.

Pada perkembangan selanjutnya atas segala usaha dan prestasi semua unsur yang ada di ketiga Sekolah Tinggi yang berada dalam pimpinan Yayasan Bina Darma yaitu Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Bina Darma, Sekolah Tinggi Ilmu Ekonomi (STIE) Bina Darma dan Sekolah Tinggi Bahasa Asing (STBA) Bina Darma digabung menjadi Universitas berdasarkan Surat Keputusan Menteri Pendidikan Nasional Republik Indonesia Nomor : 112/D/0/2002 tanggal 7 Juni 2002 tentang Penggabungan 3 (tiga) Sekolah Tinggi menjadi Universitas dan Penambahan Izin Penyelenggaraan Program Studi Baru yang diselenggarakan oleh Yayasan Bina Darma di Palembang. Berhubungan dengan itu maka untuk Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Bina Darma berubah menjadi Fakultas Ilmu Komputer, Sekolah Tinggi Ilmu Ekonomi (STIE) Bina Darma berubah menjadi Fakultas Ekonomi, dan Sekolah Tinggi Bahasa Asing (STBA) berubah menjadi Fakultas Bahasa dan Sastra, dan ditambah dua Fakultas lagi yaitu Fakultas Teknik dengan program studi Teknik Sipil, Teknik Elektro, dan Teknik Industri jenjang studi strata satu (S1), dan Fakultas

Psikologi dengan program studi Psikologi jenjang studi strata satu (S1). Sejalan waktu UBD menambah 2 Fakultas Baru yaitu Fakultas Ilmu Komunikasi dan Fakultas Keguruan dan Ilmu Pendidikan, sehingga UBD saat ini mengasuh dan mengembangkan ilmu dan keahlian profesional pada 7 (tujuh) Fakultas dengan 19 program studi yang mempunyai komitmen untuk menciptakan lulusan yang siap kerja dan dapat diterima di masyarakat.

B. Visi dan Misi Universitas
   1) Visi
      - Menjadi Universitas Berstandar Internasional Berbasis Teknologi Informasi Pada Tahun 2025.
   2) Misi
      - Menyelenggarakan program pendidikan yang berstandar internasional,
      - Menyelenggarakan proses pembelajaran yang berstandar internasional melalui pemanfaatan teknologi informasi,
      - Membangan komunitas intelektual yang berkualitas,
      - Melakukan penelitian yang berstandar internasional,
      - Melakukan pengabdian guna meningkatkan kemandirian masyarakat,
      - Menyelenggarakan kerjasama dengan pihak lain yang saling menguntungkan.

RISK MANAGEMENT – ISO 27005

WARNING! (**INI HANYA PERMISALAN DAN PERUMPAMAAN, MAAF JIKA TIDAK SESUAI KARENA SAYA MEMBUATNYA DENGAN KETERBATASAN DAN KETERBATASAN. TERIMA KASIH!)**

A. KONTEKS

A.1. Universitas Bina Darma di masa pandemi

Konteks manajemen resiko keamanan informsi harus ditetapkan, yang melibatkan penetapan kriteria dasar yang diperlukan untuk manajemen, resiko kemananan informasi, mendefinisikan ruang lingkup dan batasan – batasan, dan membentuk sebuah organisasi yang layak menjalankan managemen resiko keamanan informasi. Maka dalam kasus ini, ditentukan terlebih dahulu konteks yang akan ditetapkan, yakni mengenai memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya.

A.2. Daftar kendala yang mempengaruhi organisasi

- ✓ Sebab karena pandemi tentu ada beberapa hal yang mempengaruhi universitas, seperti kerugian dll
- ✓ Tingkat klasifikasi aset informasi yang terkena dampak
- ✓ Tingkat klasifikasi aset informasi (misalnya hilangnya kerahasiaan integritas dan ketersediaan)
- ✓ Gangguan operasional (pihak internal dan ekternal)
- ✓ Kerugian bisnis dalam hal nilai keuangan
- ✓ Gangguan rencana dan tenggat waktu
- ✓ Keruskan reputasi
- ✓ Pelanggaran terhadap persyaratan hukum, peraturan atau kontrak

Berikut ini kemungkinan yang terdampak pada kriteria tampak pada universitas bina darma pada masa pandemi ini:

Tingkat dampak	Penjelasan
Tinggi	1. Sistem tak dapat dikendalikan dari jarak jauh

	2. Tidak ada link backup dan redudancy
	3. Terdapat informasi rahasia tersebar
	4. Akses oleh pihak luar yang tidak dapat diketahui oleh pihak sub team
	5. Tidak diketahui Kehilangan data atau kerusakan data karena penggunaan jarak jauh
	6. Reputasi Universitas dalam proses bisnis
	7. Kinerja karyawan yang tak lagi dapat dimonitor
	8. Kestabilan Sistem informasi selama jam kerja sistem
	9. Anggaran
Sedang	1. Sistem down memerlukan remote
	2. Belajar mengajar memerlukan sistem daring
	3. Sistem daring yang memiliki gangguan
Ringan	1. Registrasi online

A.3. daftar Referensi legislatif dan persyaratan yang berlaku bagi Universitas bina darma

Pengendali Data Pribadi harus melindungi dan memastikan keamanan Data Pribadi, termasuk:

• persiapan dan implementasi tindakan teknis operasional yang sesuai untuk melindungi Data Pribadi dari kebocoran, kerusakan, atau pelanggaran Hukum;

• menentukan tingkat keamanan Data Pribadi dengan mempertimbangkan sifat dan risiko Pemrosesan Data Pribadi

• Pengendali Data Pribadi harus melakukan pengawasan yang tepat terhadap pihak-pihak yang terlibat dalam pemrosesan Data Pribadi;

• Pengendali Data Pribadi harus memastikan perlindungan Data Pribadi dari pemrosesan Data Pribadi yang tidak sah.

• Pengendali Data Pribadi akan mencegah Data Pribadi dari diakses secara ilegal dengan menciptakan sistem keamanan Data Pribadi.

Pengendali Data Pribadi harus memberi tahu Pemilik data privasi oleh Pribadi atau organisasi dalam hal-hal berikut:

a. Sebuah Data pribadi yang terungkap(pengungkapan atau pelanggaran);

b. kapan dan bagaimana Data Pribadi diungkapkan;

c. Menangani respons dan pemulihan pengungkapan Data Pribadi oleh Pengontrol Data Pribadi;

d. Laporkan ke komunitas CSIRT dan Badan Penegakan Hukum ketika itu merupakan pelanggaran dan memiliki dampak besar seperti dampak keuangan dan sebagainya.

Dasar Hukum

• Undang-Undang Dasar 1945

• Undang-undang No 19 Tahun 2016 tentang perubahan atas Undang-undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

• Undang-undang No. 14 tahun 2008 tentang Keterbukaan Informasi Publik

• Undang-Undang no. 24 tahun 2013 tentang Adminduk

• Peraturan Pemerintah No 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

• Peraturan menteri kominfo no.20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Hal ini mencakup data pribadi, transaksi elektronik dll

Tujuan : adalah memberikan perlindungan yang lebih baik terhadap kerahasiaan data (data privacy) dalam ekonomi digital saat ini dengan memberikan keleluasaan lebih untuk individual terhadap datanya dan memberikan peraturan yang lebih ketat kepada pihak yang mengelola atau menyimpannya

Sanksi Pelanggaran GDPR

• Dibandingkan dengan Pedoman Perlindungan Data sebelumnya, GDPR telah meningkatkan hukuman atas pelanggaran. Apabila terjadi kebocoran data, maka perusahaan dikenai denda 20 juta Euro atau empat persen dari pendapatan global. Kasus kebocoran data yang lebih kecil akan dikenai denda 10 juta Euro atau dua persen dari pendapatan global perusahaan.

A.4. Daftar kendala yang mempengaruhi ruang lingkup

Kendala yang muncul dari proses yang sudah ada. Hal ini seperti akses sistem yang diharuskan dari jarak jauh. Dan sistem dapat dikendalikan selama 24 jam atau selama jam kerja sistem. Apakah ini berbenturan dengan sistem yang telah ada ketika sistem remote control diterapkan

Kendala teknis

Berkas (persyaratan mengenai organisasi, manajemen media, aturan pengelolaan
akses, dll);

- ✓ Arsitektur umum (persyaratan mengenai topologi (terpusat, distribusi, *client-server*), arsitektur fisik, dll);
- ✓ Aplikasi perangkat lunak (persyaratan mengenai desain perangkat lunak tertentu, strandar pasar, dll);
- ✓ Paket perangkat lunak (persyaratan mengenai standar, tingkat evaluasi, kualitas, kepatuhan terhadap norma, keamanan, dll);
- ✓ Perangkat keras (persyaratan mengenai standar, kualitas, kepatuhan terhadap norma, dll);
- ✓ Jaringan komunikasi (persyaratan mengenai jangkauan, standar, kapasitas, keandalan, dll);
- ✓ Infrastruktur bangunan (persyaratan mengenai teknik sipil, konstruksi, voltase tinggi, voltase rendah, dll).
- ✓ kendala Keuangan

Pada dasarnnya sistem jarak jauh dan sistem jarak dekat dengan pembelajaran e-learning dan model pemantau kinerja karyawan tetap dilakukan. Apakah memiliki dampak pada anggaran yang ada.

Sebagai contohnya mungkin pengurangan karyawan dikantor namun kinerja dosen yang masih terus melakukan belajar mengajar perlu diperhatikan. Mungkin listrik tidak begitu membengkak namun bagaimana gaji karyawan dan pengeluaran atas sistem belajar mengajar tetap tidak merugikan pengajar. Atau bagaimana memastikan bahwa pengajar tetap mengajar dan dapat dipantau jadwalnya. Karena berkaitan dengan upah dan anggaran yang masuk.

B. Identifikasi Aset dan Ancaman

Identifikasi dan evaluasi penilaian aset dan dampak (Contoh saja)

Aset utama = Gedung Universiras Bina Darma

Proses bisnis dan Kegiatan	Proses belajar mengajar Proses Pembayaran Elektronik Sistem Informasi Pemantauan Kinerja SDM
Informasi	Data yang bersifat elektronik dan Non elektronik termasuk data pada sistem informasi (SDM, Akademik, Keuangan, dll)

Aset Pendukung

Kategori	Aset	Ancaman	Kelemahan
Perangkat Lunak	Sistem Informasi	Down, Data hilang, Akses diluar sub team (yang sudah ditentukan)	Teknisi Jaringan Listrik
	Database	Password	Hacker Human Error
	Database Server	Standar Keamanan	Teknisi Listrik
	Storage Server	Password	Teknisi Listrik
	e-Learning	Down	Teknisi Hacker Sistem Pengembangan Tracking terlu banyak Listrik
	Firewall	Layanan tidak jalan	Teknisi Source power
		Password	Hacker
Perangkat Keras	PC	Error	Virus
	Labtop	Error	Virus
Network	Router	Error	Bencana Alam Teknis
	Switch	Error	Bencana Alam Teknis
	Kabel	Error	Bencana Alam Teknis Hewan
Personel	Dosen	Tidak Mengajar	Lupa

			Teknis Salah jadwal Kuota
		Password	Human Error
	Sub Team	Password	Human Error Hacking
		Data dan Informasi penting	Human Error Hacking
	Satpam	Keamanan Gedung	Human Error Pihak Luar Listrik
	Program Studi	Keterlambatan/Kelalaian	Human Error Teknis
	Administrasi	Data dan informasi penting	Human Error Hacking Listrik Kuota
	Teknisi Jaringan	Kebocoran data	Teknisi Hacker Human Error
Tempat	Gedung/ Rumah karyawan	Mengalami masalah	Human error Kecelakaan Listrik Pihak Luar Bencana alam

C. RISK ASSESMENT

Kategori	**Aset**	**Ancaman**	**Kelemahan**	**Risk Mitigation**
Perangkat Lunak	Sistem Informasi	Down, Data hilang, Akses diluar sub team (yang sudah ditentukan)	Teknisi	Menerapkan BCP/DRP, Pelatihan Kecakapan dan Keterampilan, pembentukan Sub-Team solid, Pembekalan help desking dan Problem solving, dll
			Jaringan	Team Solid
			Listrik	Bantuan Listrik Otomatis jika mati lampu
	Database	Password	Hacker Human Error	Memastikan user sudah menerapkan SDLC, ITSM, SMKI melalui proteksi yang dibuat oleh sistem
	Database Server	Standar Keamanan	Teknisi	Menyusun konfigurasi standar minimal, menerapkan konfigurasi kemanan diatas standar yang ada, ditempatkan data center yang telah memenuhi standar keamanan
			Listrik	Bantuan Listrik Otomatis jika mati lampu

	Storage Server	Password	Teknisi	Memastikan user sudah menerapkan SDLC, ITSM, SMKI melalui proteksi yang dibuat oleh sistem. Ditempatkan didata center yang telah memenuhi standar keamanan
			Listrik	Bantuan Listrik Otomatis jika mati lampu
	e-Learning	Down	Teknisi	Menerapkan BCP/DRP, Pelatihan Kecakapan dan Keterampilan, pembentukan Sub-Team solid, Pembekalan help desking dan Problem solving, dll
			Hacker Sistem Pengembangan Tracking terlu banyak	Menyusun konfigurasi standar minimal, menerapkan konfigurasi kemanan diatas standar yang ada, ditempatkan data center yang telah memenuhi standar keamanan
			listrik	Bantuan Listrik Otomatis jika mati lampu
	Firewall	Layanan tidak jalan	Teknisi Source power	Menerapkan BCP/DRP, Pelatihan Kecakapan dan Keterampilan, pembentukan Sub-Team solid, Pembekalan help desking dan Problem solving, melakukan konfigurasi policy, dll
		Password	Hacker	
Perangkat Keras	PC	Error	Virus	Install Antivirus, Port USB Disable, tidak bisa akses program ilegal, dibatasi pada akses internet manapun hanya pada akses terkait saja.
	Labtop	Error	Virus	Install Antivirus, Port USB Disable, tidak bisa akses program ilegal, dibatasi pada akses internet manapun hanya pada akses terkait saja.
Network	Router	Error	Bencana Alam	Cadangan
			Teknis	Install Antivirus, Port USB Disable, tidak bisa akses program ilegal, dibatasi pada akses internet manapun hanya pada akses terkait saja.
	Switch	Error	Bencana Alam	Cadangan
			Teknis	Install Antivirus, Port USB Disable, tidak bisa akses program ilegal, dibatasi pada akses internet manapun hanya pada akses terkait saja.
	Kabel	Error	Bencana Alam	Cadangan
			Teknis	Install Antivirus, Port USB Disable, tidak bisa akses program ilegal, dibatasi pada akses internet manapun hanya pada akses terkait saja.
			Hewan	Dalam gedung, atau pengaman
Personel	Dosen	Tidak Mengajar	Lupa	Dijawdwal, Reminders, dan ada team pengelola
			Teknis Salah jadwal	Lebih aktif berinteraksi dengan team pengelola
			Kuota	Minimalisirkan penggunaan berulang
		Password	Human Error	Lebih aktif berinteraksi dengan team pengelola

	Sub Team	Password	Human Error Hacking	Lebih aktif berinteraksi dengan team pengelola
		Data dan Informasi penting	Human Error Hacking	Membentuk team yang ahli dalam bidangnya, dan telah ditraining, memastikan bahwa team dapat bertanggung jawab atas segala sesuatu.
	Satpam	Keamanan Gedung	Human Error Pihak Luar Listrik	Memastikan bahwa satpam bekerja dengan baik dengan adanya pelapor harian.
	Program Studi	Keterlambatan/Kelalaian	Human Error Teknis	Asissten
	Administrasi	Data dan informasi penting	Human Error Hacking Listrik	Membentuk team yang ahli dalam bidangnya, dan telah ditraining, memastikan bahwa team dapat bertanggung jawab atas segala sesuatu. Dan mendapatkan salah satu team solid dari pihak dalam atau intern guna menghadapi keadaan yang tak diinginkan
			Kuota	Menghindari kegiatan berulang
	Teknisi Jaringan	Kebocoran data	Teknisi Hacker Human Error	Membentuk team yang ahli dalam bidangnya, dan telah ditraining, memastikan bahwa team dapat bertanggung jawab atas segala sesuatu. Dan mendapatkan salah satu team solid dari pihak dalam atau intern guna menghadapi keadaan yang tak diinginkan
Tempat	Gedung/ Rumah karyawan	Mengalami masalah	Human error Kecelakaan Listrik Pihak Luar Bencana alam	Auransi

RIKA SEFTIANA / 192420033 – MTI21 B
UAS IT Risk Management

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

2. Monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah (WFH). Pihak perusahaan dituntut tetap dapat memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "Employee Monitoring Software" yang dapat dideploy sehubungan dengan kegiatan ini.

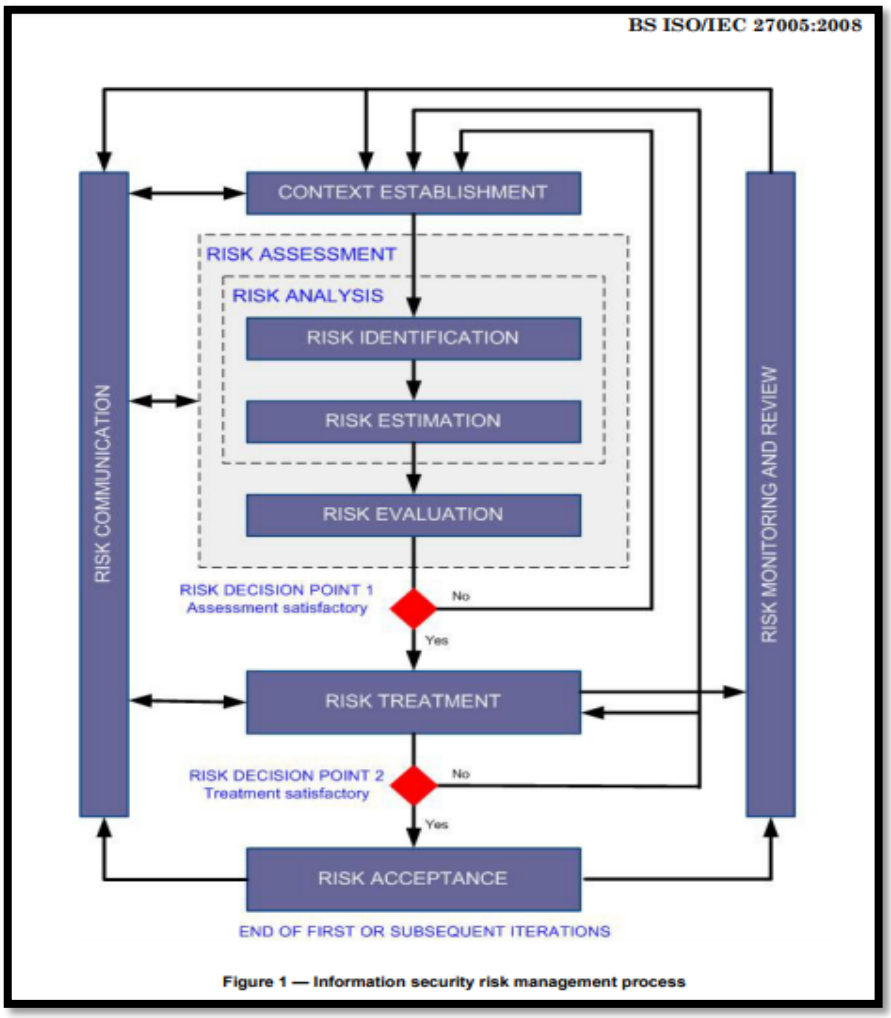
   Sebagai seorang manager IT anda diminta pertimbangan berupa risk management dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses information security risk management untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

--- Selamat bekerja ----

Jawaban:

1. Hubungan antara hasil evaluasi resiko yang dilakukan sebelumnya dengan *risk treatment* memang berhubungan erat. Hubungan keduanya terjalin karena apabila pada suatu organisasi terjadi kendala atau kejadian yang tidak diinginkan, maka perlu adanya daftar resiko terlebih dahulu sebagai antisipasi ancaman. Setelah mengetahui resiko apa saja yang akan terjadi, selanjutnya membuat keputusan. Keputusan-keputusan yang diambil bertujuan untuk menilai ancaman yang tidak diinginkan nanti, hasil dari keputusan tersebut berupa suatu evaluasi resiko. Dan apabila suatu organisasi telah melakukan evaluasi resiko, maka selanjutnya melakukan tahapan risk treatment. Pada tahapan risk treatment ini akan tahu bagaimana menentukan resiko yang bisa di treatment berdasarkan hasil dari evaluasi resiko yang telah diputuskan sebelumnya. Dengan melakukan *risk treatment* ini tentunya untuk melindungi informasi yang berkaitan dengan IT agar tetap aman dan terlindungi dari berbagai ancaman-ancaman baik secara internal maupun eksternal.

2. Tahapan dalam proses *information security risk management* menurut ISO 27005-2008, sebagai berikut :



Gambar 1 *Information Security Risk Management Proccess*

Terdapat sebuah kasus bahwa disni suatu perusahaan dituntut tetap dapat memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Hal demikian dilakukan karena monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah (WFH).

Pada kasus ini, Jika saya sebagai seorang manager IT diminta untuk mempertimbangkan *risk management* dari penggunaan *"Employee Monitoring Software"* yang dapat dideploy sehubungan dengan kasus yang terjadi. Dalam *risk management* memiliki beberapa tahapan seperti terlihat pada gambar 1. Namun, disini saya akan menggunakan dua tahapan awal saja dalam proses *information security risk management* yaitu dengan tahapan awalnya *Context Establishment* yang terdiri dari *risk assessment* dan *risk analysis (risk identification, risk estimation,* dan *risk evaluation).*

Risk identification dalam kasus ini, perlu kita ketahui terlebih dahulu konsekuensi atas kejadian-kejadian tidak diingikan apa saja yang akan terjadi. Disini, perlu adanya daftar resiko atau ancaman yang akan terjadi baik itu ancaman dari alam dan manusia yang disengaja ataupun tidak disengaja. Seperti halnya pada kasus sekarang ini, semula aktifitas kerja karyawan dilaksanakan dikantor namun dengan adanya pandemic virus corona yang sedang melanda memaksa karyawan diminta untuk melaksanakan aktifitas kerjanya dari rumah (WFH). Pada kasus ini terlihat bahwa perusahaan sedang terindentifikasi ancaman dari Alam. Karyawan dituntut tetap dapat dimonitor, ditracking atau bahkan direkam aktifitas kerjanya dengan menggunakan software yaitu *"Employee Monitoring Software".* Jika saya sebagai seorang manager IT, saya merasa dengan adanya *software* ini adalah pilihan tepat bagi perusahaan karena dapat membantu melindungi aset perusahaan dengan pemantauan karyawan, pelacakan dan menganalisis kinerja karyawan, menghasilkan laporan, membuat saya tahu siapa datang lebih awal dan yang meninggalkan lebih awal, yang menganggur dan siapa yang efisien, yang harus dipecat dan siapa yang layak kenaikan gaji. Hal ini dilakukan karena monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan agar tetap aman dan terlindungi serta tetap berjalan dengan baik.

Selanjutnya *risk estimation*, Kegagalan dapat disebabkan oleh berbagai faktor baik teknologi, *software, hardware*, jadwal, dan biaya. Oleh karena itu, jika saya sebagai seorang manager IT perlunya mengestimasi peluang keberhasilan *software* yang dikelola saat ini yaitu "*Employee Monitoring Software"*. Dalam prakteknya, proses estimasi ini tidaklah mudah karena setiap faktor resiko selalu mengandung unsur ketidakpastian, sehingga proses estimasi resiko merupakan satu tantangan tersendiri bagi saya sebagai manager IT. Dalam analisis resiko dapat dilakukan dalam berbagai tingkatan tergantung pada luasnya resiko yang akan mengancam dan resiko yang terjadi sebelumnya. Metodologi estimasi itu sendiri terbagi menjadi kualitatif, kuantitatif atau kombinasi dari semuanya, tergantung pada keadaannya.

Setelah mengetahui *risk indentification* dan *risk estimation* yang mempunyai *value* tersendiri bagi perusahaan maka, dilanjutkan dengan melakukan *risk evaluation* sebelum melakukan tahap-tahap selanjutnya. Dalam *risk evaluation*, saya akan mengambil keputusan-keputusan terhadap resiko mana saja yang memiliki nilai ancaman bagi perusahaan. Hal demikian dilakukan agar perusahaan tetap memenuhi standarisasi dan tetap efektif dalam melindungi serta mengantisipasi ancaman yang akan terjadi, baik itu ancaman dari internal maupun eksternal terhadap asset informasi yang berkaitan dengan IT dalam mendukung Visi/Misi perusahaan.

Nama : Rudy Seftiawan
NIM : 192420029
Kelas : MTI Reguler B

Soal

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

2. Monitoring produk atifita seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah(WFH). Pihak perusahaan dituntut tetap dapat memonitor,mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "*Employee Monitoring Software*" yang dapat dideploy sehubungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008!
   (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

Jawaban

1. Hubungan dijelaskan sebagai berikut:
A. Perlakuan risiko (risk treatment)
Proses untuk memodifikasi risiko. Risk treatment dapat meliputi:
-Menghindari risiko dengan memutuskan tidak memulai atau melanjutkan kegiatan yang dapat meningkatkan risiko;
-mengambil atau meningkatkan risiko untuk mengejar opportunity;
-mengilangkan sumber risiko;
-mengubah likelihood;
-mengubah konsekuensi;
-membagi risiko debfab pihak lain;
-mempertahankan risiko dengan keputusan yang terinformasi.
Risk treatment untuk menghadapi konsekuensi negatif adalah meliputi "risk mitigation", "risk elimination", "risk prevention" dan "risk reduction".

Kontrol (control)
Tindakan yang memodifikasi risiko. Kontrol meliputi proses, kebijakan, perangkat, praktik, atau tidakan lainnya yang memodifikasi risiko. Kontrol mungkin tidak selalu dapat menghasilkan efek modifikasi sesuai dengan yang diasumsikan atau diinginkan.

Penghindaran risiko (risk avoidance)
Keputusan untuk tidak terlibat dalam, atau untuk menarik diri dari, kegiatan supaya tidak terkena suatu resiko tertentu. Risk avoidance dapat didasarkan pada hasil evaluasi risiko dan/atau peraturan dan kewajiban hukum.

Pembagian risiko (risk sharing)
Bentuk dari risk treatment yang meliputi ditribusi risiko yang telah disepakati dengan pihak lain. Hukum atau persyaratan peraturan dapat membatasi, melarang atau mandat risk sharing. Risk sharing dapat dilakukan melalui asuransi atau bentuk lain dari kontrak. Sejauh mana risiko didistribusikan dapat bergantung pada keandalan dan kejelasan pengaturan pembagian. Transfer risiko adalah bentuk dari risk sharing.

Pembiayaan risiko (risk financing)
Bentuk dari risk tratment meliputi pengaturan kontingen untuk penyediaan dana untuk memenuhi atau memodifikasi konsekuensi keuangan yang terjadi.

Retensi risiko (risk retention)
Penerimaan terhadap keuntungan yang berpotensi dari keuntungan, atau beban kerugian, dari risiko tertentu. Risk retention meliputi penerimaan dari residual risk, dan level of risk yang dipelihara tergantung pada risk criteria.

Risiko residual (residual risk)
Risiko yang tersisa setelah dilakukan risk treatment. Residual risk dapat mengandung risiko yang belum teridentifikasi dan residual risk juga sering disebut sebagai “retained risk”.

Ketahanan (resilience)
Kemampuan adaptif suatu organisasi dalam suatu lingkungan yang berubah dan kompleks.

Pengawasan (monitoring)

Pemeriksaan berkelanjutan, pengawasan, pengamatan kritis atau penentuan status untuk mengidentifikasi perubahan dari tingkat kinerja yang diperlukan atau diharapkan. Pemantauan dapat diaplikasikan dalam sebuah framework manajemen risiko, proses manajemen risiko, risiko, atau kontrol.

Rapat (review)
Kegiatan yang dilakukan untuk menentukan keberlanjutan, kelayakan, dan efektivitas dari suatu hal dalam mencapai tujuan yang ditentukan. Rapat (review) dapat diaplikasikan dalam sebuah framework manajemen risiko, proses manajemen risiko, risiko, atau kontrol.

Pelaporan risiko (risk reporting)
Bentuk komunikasi ditujukan untuk menginformasikan suatu stakeholder internal atau eksternal dengan menyediakan informasi terkait kondisi terkini terkait risiko dan manajemennya.

Register risiko (risk register)
Catatan informasi tentang risiko yang teridentifikasi. Istilah “risk log” lebih sering digunakan dibandingkan “risk register”.

Profil risiko (risk profile)
Deskripsi himpunan dari risiko. Himpunan dari risiko dapat mengandung risiko yang berhubungan terhadap organisasi secara keseluruhan, sebagian dari organisasi, atau hal lain yang didefinisikan.

Audit manajemen risiko (risk management audit)
Proses yang sistematik, mandiri, dan terdokumentasi untuk mengumpulkan bukti dan mengevaluasinya secara objektif untuk menentukan sejauh mana framework manajemen risiko dapat memadai dan efektif.

B. Istilah yang berhubungan dengan risk evaluation

Evaluasi risiko (risk evaluation)
Proses membandingkan hasil dari analisis risiko dengan kriteria risiko untuk menentukan apakah risiko dan ukurannya dapat diterima dan ditoleransi. Evaluasi risiko akan membantu penentuan risk treatment.

Perilaku risiko (risk attitude)
Pendekatan organisasi untuk menilai dan mengejar, mempertahankan, mengambil atau berpaling dari risiko.

Risk appetite
Jumlah dan jenis risiko yang akan dipertahankan atau dikejar oleh organisasi.

Toleransi risiko (risk tolerance)
Kesiapan stakeholder atau organisasi untuk menanggung risiko setelah dilakukan risk treatment untuk mencapai tujuannya. Toleransi risijo dapat dipengaruhi oleh persyaratan peraturan atau hukum

Risk aversion
Tindakan untuk berpaling dari risiko.

Agregasi risiko (risk aggregation)
Kombinasi beberapa risiko ke dalam sebuah risiko untuk mengembangkan pemahaman terhadap risiko secara keseluruhan.

Penerimaan risiko (risk acceptance)
Keputusan terinformasi untuk mengambil sebuah risiko tertentu. Penerimaan risiko dapat terjadi tanpa risk treatment atau selama proses pelaksanaan risk treatment.

2 Pastikan Channel Komunikasi Tersedia dan Lancar

Saat menerapkan *work from home*, Anda harus tetap berkomunikasi, terutama dengan partner kerja. Untuk itu, pastikan semua channel komunikasi seperti Whatsapp, Telegram, atau Slack selalu *standby*. Jangan tidak ada jawaban ketika teman kantor membutuhkan Anda.

Jika perlu, Anda bisa melakukan *video call* atau *conference call* dengan menggunakan *tools* seperti Zoom, Skype, atau Google Meeting. Memastikan ketersediaan *channel* komunikasi adalah hal utama yang harus dipenuhi oleh setiap orang ketika melakukan *work from home*.

Selain itu, penyampaian informasi juga harus cepat dan tepat sasaran. Anda bisa menggunakan *channel* komunikasi seperti *social messaging* ataupun aplikasi internal yang Anda gunakan di kantor. Jika Anda menggunakan **Talenta**, Anda bisa menggunakan fitur seperti **Broadcast Message** untuk melakukan hal tersebut.

2.B Pastikan Kehadiran Karyawan Terkontrol

Anda harus memastikan kehadiran karyawan tetap terkontrol meski menerapkan *work from home*. Salah satu caranya adalah dengan menggunakan aplikasi Human Resources Information System (HRIS) yang memiliki fitur absensi dari mobile seperti Talenta.

Fitur absensi mobile atau **Live Attendance** dapat membantu HR seperti Anda untuk memantau langsung kehadiran karyawan yang bekerja dari rumah. Prinsipnya adalah melalui *check–in* dan *check–out* yang dapat dilakukan langsung dari ponsel karyawan. Setiap kali karyawan bekerja, mereka dapat melakukan *check–in*. Begitu pun setelah selesai bekerja, mereka dapat melakukan *check–out*. Live Attendance dalam Talenta juga dilengkapi dengan fitur *selfie check–in*. Anda sebagai HR dapat melihat lokasi absen mereka melalui *dashboard* yang terupdate secara *real-time* setiap kali karyawan melakukan *clock–in* atau *clock–out*. Dengan begitu, Anda tetap bisa mengawasi apakah karyawan bekerja atau tidak.

Nama : Sapardi

NIM : 19240026

Kelas : MTI Reg B 21

Soal :

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!
2. Monitoring produk atifita seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah(WFH). Pihak perusahaan dituntut tetap dapat memonitor,mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "Employee Monitoring Software" yang dapat dideploy sehubungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa risk management dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses information security risk management untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

Jawaban:

1. Perlakuan risiko (risk treatment)
   Proses untuk memodifikasi risiko. Risk treatment dapat meliputi:
   - Menghindari risiko dengan memutuskan tidak memulai atau melanjutkan kegiatan yang dapat meningkatkan risiko;
   - mengambil atau meningkatkan risiko untuk mengejar opportunity;
   - mengilangkan sumber risiko;
   - mengubah likelihood;
   - mengubah konsekuensi;
   - membagi risiko debfab pihak lain;
   - mempertahankan risiko dengan keputusan yang terinformasi.

   - **Kontrol (control)**
     Tindakan yang memodifikasi risiko. Kontrol meliputi proses, kebijakan, perangkat, praktik, atau tidakan lainnya yang memodifikasi risiko. Kontrol mungkin tidak selalu dapat menghasilkan efek modifikasi sesuai dengan yang diasumsikan atau diinginkan.

   - **Pengawasan (monitoring)**
     Pemeriksaan berkelanjutan, pengawasan, pengamatan kritis atau penentuan status untuk mengidentifikasi perubahan dari tingkat kinerja yang diperlukan atau diharapkan.

Pemantauan dapat diaplikasikan dalam sebuah framework manajemen risiko, proses manajemen risiko, risiko, atau kontrol.

- **Rapat (review)**
  Kegiatan yang dilakukan untuk menentukan keberlanjutan, kelayakan, dan efektivitas dari suatu hal dalam mencapai tujuan yang ditentukan. Rapat (review) dapat diaplikasikan dalam sebuah framework manajemen risiko, proses manajemen risiko, risiko, atau kontrol.

- **Pelaporan riskio (risk reporting)**
  Bentuk komunikasi ditujukan untuk menginformasikan suatu stakeholder internal atau eksternal dengan menyediakan informasi terkait kondisi terkini terkait risiko dan manajemennya.

- **Register riskio (risk register)**
  Catatan informasi tentang risiko yang teridentifikasi. Istilah “risk log” lebih sering digunakan dibandingkan “risk register”.

- **Profil riskio (risk profile)**
  Deskripsi himpunan dari risiko. Himpunan dari risiko dapat mengandung risiko yang berhubungan terhadap organisasi secara keseluruhan, sebagian dari organisasi, atau hal lain yang didefinisikan.

- **Audit manajemen risiko (risk management audit)**
  Proses yang sistematik, mandiri, dan terdokumentasi untuk mengumpulkan bukti dan mengevaluasinya secara objektif untuk menentukan sejauh mana framework manajemen risiko dapat memadai dan efektif.

Evaluasi Risiko (Riskevaluation)

Proses membandingkan hasil dari analisis risiko dengan kriteria risiko untuk menentukan apakah risiko dan ukurannya dapat diterima dan ditoleransi. Evaluasi risiko akan membantu penentuan risk treatment.

- Prilaku riskio (risk attitude)
  Pendekatan organisasi untuk menilai dan mengejar, mempertahankan, mengambil atau berpaling dari risiko.
- Risk appetite
  Jumlah dan jen9is risiko yang akan dipertahankan atau dikejar oleh organisasi.
- Toleransi risiko (risk tolerance).
  Kesiapan stakeholder atau organisasi untuk menanggung risiko setelah dilakukan risk treatment untuk mencapai tujuannya. Toleransi risijo dapat dipengaruhi oleh persyaratan peraturan atau hukum.

- Risk aversion
  Rindak untuk berpaling dari risiko.
- Agregasi risiko (risk aggregation)
  Kombinasi beberapa risiko ke dalam sebuah risiko untuk mengembangkan pemahaman terhadap risiko secara keseluruhan.
- Penerimaan risiko (risk Acceptance)
  Keputusan terinformasi untuk mengambil sebuah risiko tertentu. Penerimaan risiko dapat terjadi tanpa risk treatment atau selama proses pelaksanaan risk treatment.

2. Saat menerapkan work from home, Anda harus tetap berkomunikasi, terutama dengan partner kerja. Untuk itu, pastikan semua channel komunikasi seperti Whatsapp, Telegram, atau Slack selalu standby. Jangan tidak ada jawaban ketika teman kantor membutuhkan Anda. Jika perlu, Anda bisa melakukan video call atau conference call dengan menggunakan tools seperti Zoom, Skype, atau Google Meeting. Memastikan ketersediaan channel komunikasi adalah hal utama yang harus dipenuhi oleh setiap orang ketika melakukan work from home.

   Anda harus memastikan kehadiran karyawan tetap terkontrol meski menerapkan work from home. Salah satu caranya adalah dengan menggunakan aplikasi Human Resources Information System (HRIS) yang memiliki fitur absensi dari mobile seperti Talenta Fitur absensi mobile atau Live Attendance dapat membantu HR seperti Anda untuk memantau langsung kehadiran karyawan yang bekerja dari rumah. Prinsipnya adalah melalui check–in dan check–out yang dapat dilakukan langsung dari ponsel karyawan. Setiap kali karyawan bekerja, mereka dapat melakukan check–in. Begitu pun setelah selesai bekerja, mereka dapat melakukan check–out. Live Attendance dalam Talenta juga dilengkapi dengan fitur selfie check–in. Anda sebagai HR dapat melihat lokasi absen mereka melalui dashboard yang terupdate secara real-time setiap kali karyawan melakukan clock–in atau clock–out. Dengan begitu, Anda tetap bisa mengawasi apakah karyawan bekerja atau tidak.

Nama : ade saputra
NIM : 192420027
Kelas : MTI Reguler B

Soal

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

2. Monitoring produk atifita seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah(WFH). Pihak perusahaan dituntut tetap dapat memonitor,mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "*Employee Monitoring Software*" yang dapat dideploy sehubungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

Jawaban

1 A.Perlakuan risiko (risk treatment)

Proses untuk memodifikasi risiko. Risk treatment dapat meliputi:

-Menghindari risiko dengan memutuskan tidak memulai atau melanjutkan kegiatan yang dapat meningkatkan

risiko;

-mengambil atau meningkatkan risiko untuk mengejar opportunity;

-mengilangkan sumber risiko;

-mengubah likelihood;

-mengubah konsekuensi;

-membagi risiko debfab pihak lain;

-mempertahankan risiko dengan keputusan yang terinformasi.

Risk treatment untuk menghadapi konsekuensi negatif adalah meliputi “risk mitigation”, “risk elimination”, “risk prevention” dan “risk reduction”.

Kontrol (control)

Tindakan yang memodifikasi risiko. Kontrol meliputi proses, kebijakan, perangkat, praktik, atau tidakan lainnya yang memodifikasi risiko. Kontrol mungkin tidak selalu dapat menghasilkan efek modifikasi sesuai dengan yang diasumsikan atau diinginkan.

Penghindaran risiko (risk avoidance)

Keputusan untuk tidak terlibat dalam, atau untuk menarik diri dari, kegiatan supaya tidak terkena suatu resiko tertentu. Risk avoidance dapat didasarkan pada hasil evaluasi risiko dan/atau peraturan dan kewajiban hukum.

Pembagian risiko (risk sharing)

Bentuk dari risk treatment yang meliputi ditribusi risiko yang telah disepakati dengan pihak lain. Hukum atau persyaratan peraturan dapat membatasi, melarang atau mandat risk sharing. Risk sharing dapat dilakukan melalui asuransi atau bentuk lain dari kontrak. Sejauh mana risiko didistribusikan dapat bergantung pada keandalan dan kejelasan pengaturan pembagian. Transfer risiko adalah bentuk dari risk sharing.

Pembiayaan risiko (risk financing)

Bentuk dari risk tratment meliputi pengaturan kontingen untuk penyediaan dana untuk memenuhi atau memodifikasi konsekuensi keuangan yang terjadi.

Retensi risiko (risk retention)

Penerimaan terhadap keuntungan yang berpotensi dari keuntungan, atau beban kerugian, dari risiko tertentu. Risk retention meliputi penerimaan dari residual risk, dan level of risk yang dipelihara tergantung pada risk criteria.

Risiko residual (residual risk)

Risiko yang tersisa setelah dilakukan risk treatment. Residual risk dapat mengandung risiko yang belum teridentifikasi dan residual risk juga sering disebut sebagai “retained risk”.

Ketahanan (resilience)

Kemampuan adaptif suatu organisasi dalam suatu lingkungan yang berubah dan kompleks.

. Istilah yang berhubungan dengan pengawasan dan pengukuran (monitoring and measurement)

Pengawasan (monitoring)

Pemeriksaan berkelanjutan, pengawasan, pengamatan kritis atau penentuan status untuk mengidentifikasi perubahan dari tingkat kinerja yang diperlukan atau diharapkan. Pemantauan dapat diaplikasikan dalam sebuah framework manajemen risiko, proses manajemen risiko, risiko, atau kontrol.

Rapat (review)

Kegiatan yang dilakukan untuk menentukan keberlanjutan, kelayakan, dan efektivitas dari suatu hal dalam mencapai tujuan yang ditentukan. Rapat (review) dapat diaplikasikan dalam sebuah framework manajemen risiko, proses manajemen risiko, risiko, atau kontrol.

Pelaporan risiko (risk reporting)

Bentuk komunikasi ditujukan untuk menginformasikan suatu stakeholder internal atau eksternal dengan menyediakan informasi terkait kondisi terkini terkait risiko dan manajemennya.

Register risiko (risk register)

Catatan informasi tentang risiko yang teridentifikasi. Istilah “risk log” lebih sering digunakan dibandingkan “risk register”.

Profil risiko (risk profile)

Deskripsi himpunan dari risiko. Himpunan dari risiko dapat mengandung risiko yang berhubungan terhadap organisasi secara keseluruhan, sebagian dari organisasi, atau hal lain yang didefinisikan.

. **Audit manajemen risiko (risk management audit)**

Proses yang sistematik, mandiri, dan terdokumentasi untuk mengumpulkan bukti dan mengevaluasinya secara objektif untuk menentukan sejauh mana framework manajemen risiko dapat memadai dan efektif.

B. Istilah yang berhubungan dengan risk evaluation

Evaluasi risiko (risk evaluation)

Proses membandingkan hasil dari analisis risiko dengan kriteria risiko untuk menentukan apakah risiko dan ukurannya dapat diterima dan ditoleransi. Evaluasi risiko akan membantu penentuan risk treatment.

Perilaku risiko (risk attitude)

Pendekatan organisasi untuk menilai dan mengejar, mempertahankan, mengambil atau berpaling dari risiko.

Risk appetite

Jumlah dan jenis risiko yang akan dipertahankan atau dikejar oleh organisasi.

Toleransi risiko (risk tolerance)

Kesiapan stakeholder atau organisasi untuk menanggung risiko setelah dilakukan risk treatment untuk mencapai tujuannya. Toleransi risijo dapat dipengaruhi oleh persyaratan peraturan atau hukum

Risk aversion

Tindakan untuk berpaling dari risiko.

Agregasi risiko (risk aggregation)

Kombinasi beberapa risiko ke dalam sebuah risiko untuk mengembangkan pemahaman terhadap risiko secara keseluruhan.

penerimaan risiko (risk acceptance)

Keputusan terinformasi untuk mengambil sebuah risiko tertentu. Penerimaan risiko dapat terjadi tanpa risk treatment atau selama proses pelaksanaan risk treatment.

2

Pastikan Channel Komunikasi Tersedia dan Lancar

Saat menerapkan *work from home*, Anda harus tetap berkomunikasi, terutama dengan partner kerja. Untuk itu, pastikan semua channel komunikasi seperti Whatsapp, Telegram, atau Slack selalu *standby*. Jangan tidak ada jawaban ketika teman kantor membutuhkan Anda.

Jika perlu, Anda bisa melakukan *video call* atau *conference call* dengan menggunakan *tools* seperti Zoom, Skype, atau Google Meeting. Memastikan ketersediaan *channel* komunikasi adalah hal utama yang harus dipenuhi oleh setiap orang ketika melakukan *work from home*.

Selain itu, penyampaian informasi juga harus cepat dan tepat sasaran. Anda bisa menggunakan *channel* komunikasi seperti *social messaging* ataupun aplikasi internal yang Anda gunakan di kantor. Jika Anda menggunakan **Talenta**, Anda bisa menggunakan fitur seperti **Broadcast Message** untuk melakukan hal tersebut.

2.B Pastikan Kehadiran Karyawan Terkontrol

Anda harus memastikan kehadiran karyawan tetap terkontrol meski menerapkan *work from home*. Salah satu caranya adalah dengan menggunakan aplikasi Human Resources Information System (HRIS) yang memiliki fitur absensi dari mobile seperti Talenta.

Fitur absensi mobile atau **Live Attendance** dapat membantu HR seperti Anda untuk memantau langsung kehadiran karyawan yang bekerja dari rumah. Prinsipnya adalah melalui *check–in* dan *check–out* yang dapat dilakukan langsung dari ponsel karyawan. Setiap kali karyawan bekerja, mereka dapat melakukan *check–in*. Begitu pun setelah selesai bekerja, mereka dapat melakukan *check–out*. Live Attendance dalam Talenta juga dilengkapi dengan fitur *selfie check–in*. Anda sebagai HR dapat melihat lokasi absen mereka melalui *dashboard* yang terupdate secara *real-time* setiap kali karyawan melakukan *clock–in* atau *clock–out*. Dengan begitu, Anda tetap bisa mengawasi apakah karyawan bekerja atau tidak.

Bhagaskara
192420028
IT Risk Management

Pertanyaan:

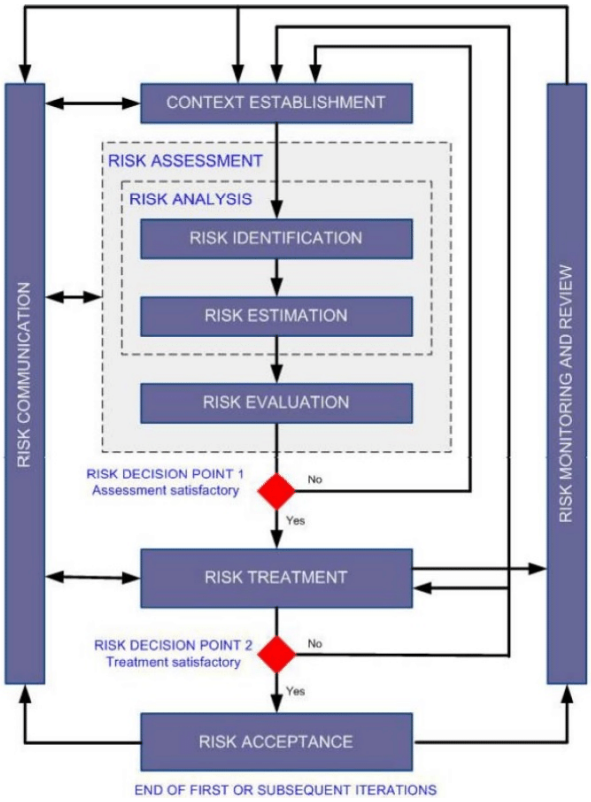
1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

2. Monitoring produktifitas seorang karyawan merupakan hal yang penting bagi suatu perusahaan. Hal ini semakin meningkat dengan adanya pandemic virus corona yang sedang melanda dimana karyawan diminta untuk bekerja dari rumah (WFH). Pihak perusahaan dituntut tetap dapat memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Secara teknologi terdapat "*Employee Monitoring Software*" yang dapat dideploy sehubungan dengan kegiatan ini.

   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008!
   (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

--- Selamat bekerja ----

Bhagaskara
192420028
IT Risk Management



Gambar 1. ISO 27005 Risk Management Workflow

Tahap Risk Assessment merupakan bagian sentral dari manajemen keamanan informasi untuk mengidentifikasi kerentanan dan ancaman suatu keputusan. Berdasarkan Gambar 1. Tahap dari risk assesment berupa identifikasi resiko, analisis resiko dan evaluasi resiko. Hasil dari evaluasi resiko tersebut akan menjasi landasan penanganan risk treatment. Hasil evaluasi resiko akan dijabarkan menjadi beberapa tingkat prioritas, dimulai dari prioritas kecil sampai prioritas tinggi, sesuai dengan dampak resiko yang ditimbulkan. Setelah hasl evalusi resiko diketahui maka langkah risk treatment akan disesuaikan dengan kebutuhan. Berdasarkan Jea Yu [2], Risk Treatment dapat dikategorikan menjadi 5 kategori, yaitu:

- Risk Avoidance
Risk Avoidance merupakan metode penanganan resiko dengan tidak melanjutkan proses kerja karena nilai resiko dievaluasi terlalu besar.

- Risk Retention
Risk Retention merupakan metode penanganan resiko dengan cara mengurangi dampak dari resiko berdasarkan aspek-aspek pembuat resiko

- Risk Sharing
Risk Sharing merupakan metode penanganan resiko dengan cara membagi tanggung jawab pengananan dengan partner untuk mengurangi tingkat resiko yang ada.

- Risk Transfer
Risk Transfer merupakan metode penanganan resiko dengan memindahkan tanggung jawab pencara mengurangi dampak dari resiko berdasarkan aspek-aspek pembuat resiko

Bhagaskara
192420028
IT Risk Management

- Risk Reduction

Risk Reduction merupakan metode penanganan resiko dengan cara mengurangi dampak dari resiko berdasarkan aspek-aspek pembuat resiko

Contoh: Pengembangan Aplikasi Transaksi Toko Buah dan Sayur Segar Online

1. Resiko Teknis

a) Masalah Human Resources

Tingkat Prioritas Evaluasi	:	Tinggi
Jenis Risk Treatment	:	Risk Sharing
Tindakan	:	Akan dilakukan pelatihan sistem kepada admin toko untuk dapat menerima dan melayani pesanan

b) Masalah Pembayaran

Tingkat Prioritas Evaluasi	:	Tinggi
Jenis Risk Treatment	:	Risk Transfer
Tindakan	:	Pembayaran akan dihubungkan dengan perusahaan uang elektronik

c) Masalah Pengantaran

Tingkat Prioritas Evaluasi	:	Tinggi
Jenis Risk Treatment	:	Risk Transfer
Tindakan	:	Pengantaran akan dihubungkan dengan transportasi ojol lokal, dengan biaya pengiriman tertera pada saat pemesanan

2. Resiko Sosial

Tingkat Prioritas Evaluasi	:	Rendah
Jenis Risk Treatment	:	Risk Retention
Tindakan	:	Belum ada isu sosial yang dominan, sehingga dapat diabaikan

3. Resiko Peraturan Pemerintah

Tingkat Prioritas Evaluasi	:	Rendah
Jenis Risk Treatment	:	Risk Retention
Tindakan	:	Belum ada isu peraturan yang spesifik mengenai onlineshop, sehingga dapat diabaikan

[1]https://www.researchgate.net/publication/308887387_Current_Established_Risk_Assessment_Methodologies_and_Tools

Bhagaskara
192420028
IT Risk Management

[2] https://www.investopedia.com/articles/investing-strategy/082816/methods-handling-risk-quick-guide.asp

Studi Kasus Information Security Risk Management: Zoom

TAHAP 1 - CONTEXT ESTABLISHMENT

Tahap konteks manajemen risiko menetapkan kriteria identifikasi resiko, penanggung jawab risiko, dampak resiko terhadap kerahasiaan perusahaan, integritas dan ketersediaan informasi, dan bagaimana dampak risiko yang dapat dihitung.

Context Bisnis

1. Kriteria Dasar Evaluasi
    a) Business Process

        Media Teleconference antar manajer dan karyawan untuk proses interaksi bisnis

    b) Nilai strategis dari proses informasi bisnis

        Aplikasi dapat membantu penyebaran informasi di tengah pandemi COVID-19

    c) Operasional dan kepentingan bisnis dari ketersediaan, kerahasiaan dan integritas

        Aplikasi telah mendapat pembaruan enkripsi untuk meningkatkan kerahasiaan percakapan

    d) Harapan dan persepsi para pemangku kepentingan, dan konsekuensi negatif untuk niat baik dan reputasi

        Aplikasi dapat dilanjutkan baik selama dan setelah pandemi COVID-19

2. Lingkup dan Batasan
    a) Struktur Organisasi/ Pengguna

        Manajer sebagai Host dan karyawan sebagai member

    b) Assets

        Masing-masing device pengguna berupa Mobile (Android / iOS) dan PC

3. Organisasi Pelaksana
    a) Penanggung jawab Pengguna Aplikasi

        Setiap User (Manajer dan karyawan)

    b) Penanggung jawab Pemeliharaan Software

        Pihak Pengembang Aplikasi (Pihak ketiga)

    c) Penanggung jawab Dokumentasi Proses

        Setiap User dengan fitur Record

TAHAP 2 - IDENTIFIKASI RESIKO

Bhagaskara
192420028
IT Risk Management

1. Identification of assets

Asset yang dimiliki sekolah berupa gedung kantor, inventory sekolah, dan staff

2. Identification of threats

Type	Threat	Origin
Physical Damage	Barang berupa aplikasi dan bersifat non-fisik. Kerusakan terletak pada kerusakan device	A,D,E
Natural Event	Bencana alam yang menyebabkan kerusakan device	E
Loss of essential service	Hilang jaringan / tidak bisa mengakses internet	A,D,E
Compromise of information	Pencurian Data	D
Technical failure	Software Error	A
	Device Error	A
Unauthorised Actor	Pengguna Illegal	D
Compromise of Failure	Ketidakpahaman Pengguna	A,D

3. Identification of existing controls ***: No Risk***

Aplikasi Zoom merupakan aplikasi ekternal dan tidak menggangu sistem yang sudah ada. Zoom dipilih karena tingkat pengguna yang tinggi dan ukuran app yang tidak besar

4. Identification of vulnerabilities

Type	Vulnerabilities	Threat
Hardware	Device rusak/ hilang	Tidak bisa melakukan operasi
Software	Sistem device atau aplikasi error	Tidak bisa melakukan operasi
Network	Tidak ada jaringan / tidak bisa mengakses internet	Tidak bisa melakukan operasi
Personnel	Pengguna tidak ada	Tidak bisa melakukan operasi
	Ketidakpahaman Pengguna	Tidak bisa melakukan operasi

5. Identification of consequences

a) *Investigation and repair time* ***: No Risk***

Aplikasi sudah bersifat stable dan siap digunakan

b) *(Work)time lost* ***: No Risk***

Aplikasi sudah bersifat stable dan siap digunakan

c) *Opportunity lost* ***: No Risk***

Sesuai dengan aturan pemerintah, penggunaan aplikasi video conference sangat dianjurkan

d) *Health and Safety* ***: No Risk***

Sesuai dengan aturan pemerintah, penggunaan aplikasi video conference sangat dianjurkan

e) *Financial cost of specific skills to repair the damage* ***: No Risk***

Aplikasi dapat diunduh gratis pada platform apapun

f) Image reputation and goodwill ***: No Risk***

Penggunaan aplikasi ditujukan untuk menjaga keamanan dan kenyamanan user