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 ----

Nama : Muhammad Fajar
NIM : 192420037 (MTI AR2)

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 ----

Jawab :

1. Risk treatment bertujuan untuk menentukan tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara keseluruhan. Risk treatment merubah hasil evaluasi resiko atau analisis sebelumnya, risk identification dan risk assessment, menjadi tindakan substantif untuk mengurangi risiko.
Terdapat beberapa risk treatment yang umumnya digunakan, yaitu; Risk Avoidance (menghindari risiko) dengan tujuan untuk mengurangi secara substansial kemungkinan terjadinya risiko, Risk Reduction (pengurangan risiko) dengan tujuan untuk meminimalkan konsekuansi dari risiko, Risk Sharing/Transfer (berbagi risiko) dengan tujuan untuk memindahkan risiko tidak hanya ke organisasi lain namun juga ke entitas bisnis ataupin individu, dan Risk Retention (retensi risiko) atau dikenal juga sebagai penyerapan, toleransi, atau penerimaan risiko.

   Contohnya : pada saat di tahap risk treatment dilihat tindakan dari suatu perusahaan dalam mengatasi resiko yang telah teridentifikasi sebelumnya pada risk identification. Identifikasi yang dilakukan menghasilkan beberapa resiko yang mungkin terjadi pada setiap aspek yang dimiliki perusahaan, antara lain seperti *Application, Information, Infrastructure* dan *People*. Setelah di identifikasi lalu masuk ke risk assessment, merupakan risk analysis dan risk evaluation untuk mendapatkan level of risk

(tingkatan resiko). Di tahap ini akan di klasifikasi resikonya. Setelah di dapatkan hasil dari identifikasi barulah masuk ke risk treatment, contoh kasusnya seperti *Organization Risk Treatment* identifikasi risikonya *Inappropriate Access*, Threats nya adalah *Unauthorized Access*, Treatmentnya Menerapkan safety IT Procedure seperti mengakhiri setiap akses, melindungi pc dan terminal dengan password. Menerapkan policy on Use of Network service seperti hanya user dan third parties yang memiliki user-id yang dapat log-on kedalam sistem, tidak diizinkan melakukan aktifitas illegal pada komputer dan penggunaan komputer harus di monitor oleh organisasi.

2. Sesuai dengan ISO 27005:2008, tahapan awal yaitu Risk Identification dan Risk Estimation (Identifikasi Risiko dan Estimasi Risiko) yang termasuk ke dalam Risk Assessment dan Risk Analysis.
Untuk teknologi menggunakan aplikasi "Employee Monitoring Software" yaitu ActivTrak. Banyaknya orang bekerja dari rumah atau work from home (WFH), dikarenakan pandemic COVID-19, software monitoring pegawai bisa membantu mengatasinya untuk mentracking pegawai yang sedang bekerja. Menurut survey dari PC Mag, ActivTrac merupakan 10 aplikasi terbaik dikarenakan fitur yang lengap dan yang paling penting memiliki user privacy.

- Risk Identification dan Rsik Assesment

Pada proses identifikasi risiko dilakukan pemngelompokan risiko yang berhubungan dengan aplikasi Employee Monitoring Software yaitu ActivTrak.

Identifikasi Aset Perusahaan

No	Aset	Jenis Aset	Lokasi Aset
1.	Aplikasi Employee Monitoring Software ActivTrak	Aset Utama	Server Aplikasi
2.	*Windows Server/ Operating system*	Aset Pendukung	Ruangan Server
3.	*Firewall*	Aset Pendukung	Ruangan Server
4.	Personal Computer	Aset Pendukung	Ruangan Server (3 Unit)
5.	*Storage Server*	Aset Pendukung	Ruangan Server
6.	*Database Server*	Aset Pendukung	Ruangan Server
7.	UPS *(Uninterruptible Power Supply)*	Aset pendukung	Ruangan Server
8.	Cable and Equipment	Aset Utama	Ruangan Server
9.	Router, Switch Servers	Aset Pendukung	Ruangan Server

Nama : Muhammad Fajar
NIM : 192420037 (MTI AR2)

Identifikasi Threats

No	Aset	Ancaman	Penyebab Ancaman	Sumber Ancaman
1	Aplikasi Employee Monitoring Software ActivTrak	Layanaan Tidak Jalan	Aplikasi erorr/tidak bisa diakses karena proses *troubleshooting* membutuhkan waktu lebih lama	1. Teknisi 2. Pengembang Aplikasi
		Modifikasi	1. *Defacing* 2. DDoS *(Dsitributed Denial of Service)* 3. BOT 4. Spoofing	Pegawai yang curang / *Hacker*
2	*Windows Server* / Operating System	Windows/ Mac OS tidak berjalan dengan semestinya	Terdapat banyak virus di PC	Virus
3	*Firewall*	Layanan tidak jalan	Adanya kebijakan yang membatasi aplikasi. Power listik mati.	1. Teknisi 2. *Source Power*
		Password Lemah atau menggunakan *default password*	Mengubah konfigurasi yang tidak sesuai degan standar oleh pihak yang tidak berwenang	*Hacker*
4	PC	PC error	Banyaknya virus yang terdapat di PC. Terdapat kendala didalam *hardware* atau *software*.	Virus
5	*Storage Server*	*Password* Lemah atau menggunakan *default password*	Akses yang dilakukan oleh pihak yang tidak berwenang	1. Teknisi 2. Pengembang Aplikasi 3. *Hacker*
6	*Database Server*	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Akses yang dilakukan oleh pihak yang tidak berwenang untuk mengubah konfigurasi pada *database* server.	1. Teknisi 2. Pengembang Aplikasi 3. *Hacker*
7	UPS	Baterai pada ups tidak dapat menyimpan daya	UPS terlalu banyak beban untuk melakukan *cover* dari perangkat lunak yang melebihi dari ketentuan	Teknisi

Nama : Muhammad Fajar
NIM : 192420037 (MTI AR2)

Identifikasi Threats Infrastruktur

Kelompok Risiko	*Threats*	*Impact/ Consequences*	Klasifikasi
Physical Damage	Pencurian Terhadap *Physical Asset*	Ketidak tersediaan infrastruktur	*Availability*
	Kerusakan Terhadap *Physical Asset*	Kerusakan Aset	*Availability*
		Data Loss	*Availability*
	Water Damage	Kerusakan Aset	*Availability*
		Data Loss	*Availability*
	Heat	Hardware tidak aktif	*Availability*
		Corrupted Data	*Availability*
		Data Loss	*Availability*
Hardware Failure	*Electrical Dischagrge*	Korsleting	*Availability*
		Kerusakan pada hardware/ modul	*Availability*
		Sengatan Listrik	*Compliance*
	Short Circuit	Kerusakan pada hardware/ modul	*Availability*
	Power Surges	*Server Interupts*	*Availability*
		Hard Bad Sector	*Availability*
	Overheating	Hardware tidak aktif	*Availability*
		Corrupted Data	*Availability*
		Data Loss	*Availability*
	Bad Hardisk Sector	*Hard Bad Sector*	*Availability*
		Soft Bad Sector	*Performance*
		Corrupted Data	*Availability*
		Data Loss	*Availability*
	Corrupted File	*Corrupted Data*	*Availability*
		Data Loss	*Availability*
	Human Error	Kerusakan	*Availability*

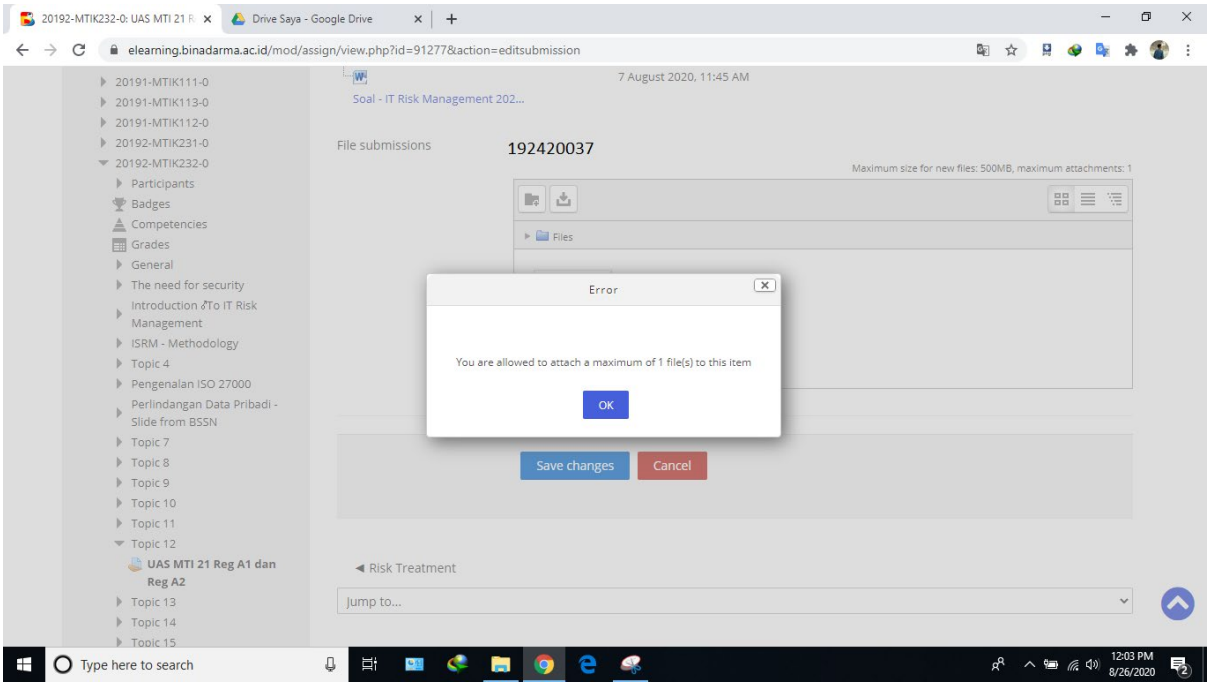
Nama : Muhammad Fajar
NIM : 192420037 (MTI AR2)

		Hardware	
		Data loss	*Availability*
Power Outage	*Power Cut/ Power Blackout/ Power Failure*	Ketidak tersediaan Infrastruktur	*Availability*
Force Majure	Bencana Alam	Kerusakan Infrastruktur	*Availability*
		Kerusakan Hardware	*Availability*
		Data Loss	*Availability*

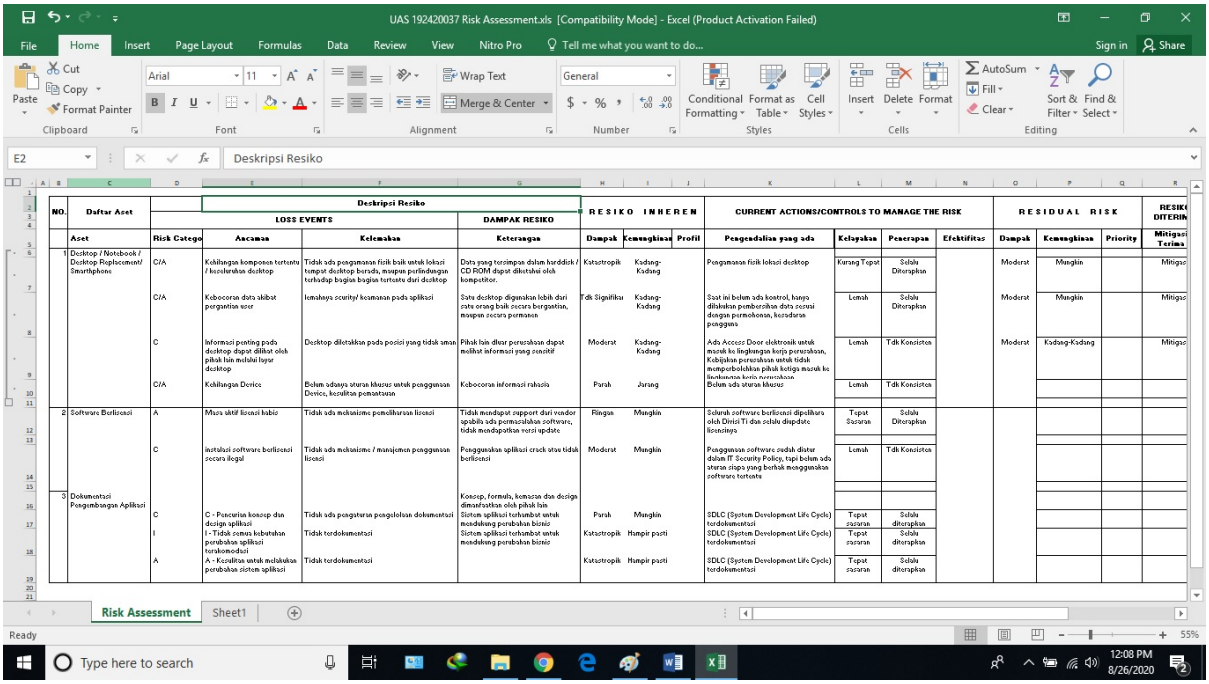
Selanjutnya Akan di lanjutkan ke file Excel untuk Risk Assesment.

Dikarenakan Upload tidak boleh lebih dari satu maka akan saya kasih link google drive file excelnya

https://drive.google.com/file/d/1a_pcz6nwO9mddMudIOv66OkXrlIOYCms/view?usp=sharing



Nama : Muhammad Fajar
NIM : 192420037 (MTI AR2)



UAS 192420037 Risk Assessment.xls [Compatibility Mode] - Excel (Product Activation Failed)

E2: Deskripsi Resiko

NO.	Daftar Aset	Deskripsi Resiko				RESIKO INHEREN			CURRENT ACTIONS/CONTROLS TO MANAGE THE RISK				RESIDUAL RISK			RESIKO DITERIM
		LOSS EVENTS			DAMPAK RESIKO											
	Aset	Risk Catego	Ancaman	Kelemahan	Keterangan	Dampak	Kemunginan	Profil	Pengendalian yang ada	Kelayakan	Penerapan	Efektifitas	Dampak	Kemunginan	Priority	Mitigasi Terima
1	Desktop / Notebook / Desktop Replacement/ Smartphone	C/A	Kehilangan komponen tertentu / kesalahan desktop	Tidak ada pengamanan fisik baik untuk lokasi tempat desktop berada, maupun perlindungan terhadap bagian bagian tertentu dari desktop	Data yang tersimpan dalam harddisk / CD ROM dapat dikutahui oleh kompetitor.	Katastropik	Kadang-Kadang		Pengamanan fisik lokasi desktop	Kurang Tepat	Sebiknya Diterapkan		Moderat	Mungkin		Mitigas
		C/A	Kebocoran data akibat pergantian user	lemahnya security/ kemanan pada aplikasi	Satu desktop digunakan lebih dari satu orang baik secara bergantian, maupun secara permanen	Tdk Signifikan	Kadang-Kadang		Saat ini belum ada kontrol, hanya dilakukan pemberahan data secara dengan permohonan, keruduran panggung	Lemah	Sebiknya Diterapkan		Moderat	Mungkin		Mitigas
		C	Informasi penting pada desktop dapat dilihat oleh pihak lain melalui layar desktop	Desktop diletakkan pada posisi yang tidak aman	Pihak lain diluar perusahaan dapat melihat informasi yang sensitif	Moderat	Kadang-Kadang		Ada Access Door elektronik untuk masuk ke lingkungan kerja perusahaan, Kebijakan perusahaan untuk tidak memperbolehkan pihak ketiga masuk ke lingkungan kerja perusahaan	Lemah	Tdk Konsisten		Moderat	Kadang-Kadang		Mitigas
		C/A	Kehilangan Device	Belum adanya aturan khusus untuk penggunaan Device, kesalitan pemantauan	Kebocoran informasi rahasia	Parah	Jarang		Belum ada aturan khusus	Lemah	Tdk Konsisten					
2	Software Berlicensi	A	Mass aktif licensi habis	Tidak ada mekanisme pemeliharaan licensi	Tidak mendapat support dari vendor apabila ada permasalahan software, tidak mendapatkan versi update	Ringan	Mungkin		Seluruh software berlicensi dipelihara oleh Divisi TI dan selalu diupdate licensinya	Tepat Sasaran	Sebiknya Diterapkan					
		C	instalasi software berlicensi secara illegal	Tidak ada mekanisme / manajemen penggunaan licensi	Penggunakan aplikasi crack atau tidak berlicensi	Moderat	Mungkin		Penggunaan software sudah diatur dalam IT Security Policy, tapi belum ada aturan siapa yang berhak menggunakan software tertentu	Lemah	Tdk Konsisten					
3	Dokumentasi Pengembangan Aplikasi				Konsep, formula, komposisi dan desiga dimanfaatkan oleh pihak lain											
		C	C - Pencurian konsep dan design aplikasi	Tidak ada pengaturan pengelolaan dokumentasi	Sistem aplikasi terhambat untuk mendukung perubahan bisnis	Parah	Mungkin		SDLC (System Development Life Cycle) terdokumentasi	Tepat sasaran	Sebiknya diterapkan					
		I	I - Tidak semua kebutuhan perubahan aplikasi terakomodasi	Tidak terdokumentasi	Sistem aplikasi terhambat untuk mendukung perubahan bisnis	Katastropik	Hampir pasti		SDLC (System Development Life Cycle) terdokumentasi	Tepat sasaran	Sebiknya diterapkan					
		A	A - Kesalitan untuk melakukan perubahan sistem aplikasi	Tidak terdokumentasi		Katastropik	Hampir pasti		SDLC (System Development Life Cycle) terdokumentasi	Tepat sasaran	Sebiknya diterapkan					

Sheets: Risk Assessment | Sheet1

Ready

Type here to search

12:08 PM
8/26/2020

UAS IT Risk Management

Nama : Muhammad Hadrifiansyah

Kelas : MTI21AR1

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!

   Jawab :
   Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko karena dalam Risk Treatment Options harus dipilih berdasarkan hasil penilaian risiko, biaya dalam penerapan dan manfaat yang di harapakan. Sehingga dari hasil tersebut bisa terlaksananya Evaluasi Resiko guna memperbaiki dan menanggulangi resiko yang akan terjadi.
   Contoh :
   Di dalam susatu prusahaan ingin melakukan audit Management sehingga harus melakukan beberapa pase proses menanggulangan resiko dengan adanya beberapa Opsi-opsi pendukung Risk Treatment (*Risk Treatment Options*). dalam menentukannya *Risk Treatment Options* meliputi yaitu :
   - Risk Reduction
   - Risk Retention
   - Risk Avoidance
   - Risk Transfer

   Dari Options di atas perusahaan akan mendapakan nilai hasil untuk melakukan evaluasi resiko, sehingga memperbaiki system yang bermasalah.

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

   Sebagai seorang manager IT anda di minta 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)

   Jawab :

   Penggunaan aplikasi Zoom Meeting di Perusahaan X, Seorang IT manager membuat Risk Management dari penggunaan Software Zoom Meeting. penggunaan maliputi beberapa tahapan yang harus di lakukan dalam Proses Information Security Risk Management menggunakan ISO 27005-2008.

Adapun penilaian dalam Risk Management yang harus di ketahui yaitu ;

1. **Analisis Risiko,** Menganalisis beberapa resiko yang akan terjadi ketika menggunakan aplikasi Zoom Meeting. Adapun pembagian Analisis resiko sebagai berikut ;
   a. **Identifikasi Resiko,** yang dimana ;
      - Mengenali Identifikasi Resiko yang mengancam User.
      - Identifikasi Aset-aset pengunaan data yang akan di gunakan melalui aplikasi
      - Identifikasi Ancaman yang kemungkinan terjadinya kebocoran data.
      - Identifikasi Kontrol, yang dimana penggunaan Aplikasi Zoom Meeting di monitorin oleh staff IT atau Manager IT
      - Identifikasi Kerentanan, Seorang IT Mananger di perusahaan X, Melakukan Identifikasi Kerentanan yang mengancam yang akan membahayakan Aset yang harus di identifikasi.
      - Identifikasi Konsekuensi, bahwa kerugian atas kerahasiaan, integritas dan ketersediaan terhadap aset harus diidentifikasi oleh IT Manager.
   b. **Estimasi Resiko,** yang dimana meliputi ;
      - Metodologi estimasi risiko, IT manager menentukan Metodologi yang tepat untuk Analisis risiko dapat dilakukan dalam berbagai tingkat detail tergantung pada kritikalitas aset, jangkauan kerentanan yang diketahui, dan keterlibatan insiden sebelumnya dalam organisasi. Metodologi estimasi bisa kualitatif atau kuantitatif, atau kombinasi dari keduanya, tergantung pada keadaan. Dalam prakteknya, estimasi kualitatif sering digunakan mulanya untuk mendapatkan indikasi umum level risiko dan untuk mengungkapkan risiko utama dari aplikasi.
      - Penilaian konsekuensi, Dampak bisnis pada organisasi yang mungkin timbul dari informasi insiden keamanan yang mungkin atau aktual harus dinilai, dengan mempertimbangkan konsekuensi dari pelanggaran keamanan informasi seperti hilangnya kerahasiaan, integritas atau ketersediaan aset melalui Aplikasi Zoom Meeting.
2. **Evaluasi Risiko,** dalam perusahaan X harus mengetahui Tingkat risiko harus dibandingkan dengan kriteria evaluasi risiko dan kriteria penerimaan risiko. Sehingga mendapatkan hasil kelayakan Penggunaan Aplikasi Zoom Meeting layak atau tidak.

UAS IT Risk Management

Nama : M.Nang Alhafiz

Nim :192420008

Dosen : Dedy Syamsuar, MIT, PhD

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!

   Risk treatment adalah proses menanggulangi segala resiko yang akan terjadi dengan cara menghindari, menurunkan resiko, dan menghadapi resiko yang akan terjadi untujk melindungi asset, hal ini sangat berhubungan erat dengan hasil evalusi resiko yang telah ditetapkan dengan cara dilakukan penilaian apakah efektif atau tidaknya pencegahan yang dilakukan atau resiko mana yang paling tinggi akan terjadi

   Contoh : risk treatment pada ruang server, salah satu resiko yang akan terjadi adalah bencana alam seperti banjir gempa bumi, atau terjadinya pencurian, dan kebakaran. Dengan ancaman yang mungkin akan terjadi kita dapat mengevaluasi resiko tersebut dengan cara back up data, ruangan dengan suhu yang dingin, menyediakan pemadam api, kamera CCTV dan akses masuk ke ruang server yang ketat. lalu kita dapat hasil dari evaluasi tersebut seperti keamanan hardware yang pertama kita gunakan gembok, lalu dievaluasi dikarenakan resiko yang lain lalu ditambah jeruji pelindung lalu dievaluasi lagi, penambahan akses dengan kartu pegawai atau scan sidik jari dan kamera cctv.

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)

Risk management Google hangouts meet.

Rencana yang dilakukan dengan memberikan layanan akses kepada karyawan ke google hangouts, Menggunakan password saat memasuki konfrensi video, dan menggunakan data pribadi yang benar dan diketahui oleh perusahaan. Dan tidak men share file yang penting secara sembarang.
Resiko yang akan dihadapi berupa penambahan biaya yang akan digunakan , dikarenakan untuk mendapatkan akses berupa paket 100 pengguna atau pun fitur yang lain pada google hangouts meet harus melakukan pembayaran , di karenakan jumlah karyawan yang banyak.

Membutuhkan jaringan internet yang stabil.

Resiko yang lainya, pihak yang tidak bertanggung jawab mengakses atau mengawasi konfrensi yang dilakukan oleh perusahaan kita. Walaupun google hangouts meet telah memberikan layanan enkripsi video tetapi masih tetap harus waspada.

UAS IT RISK MANAGEMENT
NAMA : NIZAR FIRLIANSA
NIM : 192420005
KELAS : MTI Reguler AR1

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)

Jawab :

1. Penanganan Risiko (Risk Treatment) melibatkan identifikasi atas berbagai pilihan/opsi untuk menangani risiko , menilai opsi tersebut, serta persiapan dan pelaksanaan rencana penanganan risiko.
   Contoh hubungan erat Risk Treatment dengan hasil evaluasi resiko: Ada suatu perusahaan yang mengalami penurunan omset akibat dari pandemic covid-19 ini, sebagai akibatnya perusahaan tersebut tidak mampu untuk memberi gaji semua karyawannya seperti sebelumnya, dan akhirnya untuk menangani resiko tersebut perusahaan harus memilih opsi untuk menangani resiko ini salah satunya pengurangan jumlah karyawan. Setelah pilihan tersebut diambil nanti akan di evaluasi apakah perusahaan tersebut dapat tetap berjalan, apakah dapat mensejahterahkan karyawannya, dan mampu melewati kondisi tersebut. Penanganan risiko dapat dengan sendirinya memperkenalkan risiko baru yang perlu diidentifikasi, dinilai, diatasi dan dipantau. Jika, setelah penanganan, terdapat risiko residual, keputusan harus diambil mengenai apakah untuk mempertahankan risiko ini atau mengulangi proses penanganan risiko.

2. Tahapan dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008

   Pertama Plan, yaitu menetapkan kebijakan, sasaran, proses dan prosedur Sistem Manajemen Keamanan Informasi yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran perusahaan secara keseluruhan.

   Kedua Penerapan dan Pengoperasian kebijakan pengendalian, proses dan prosedur Sistem Manajemen Keamanan Informasi.

   Mengukur kinerja proses terhadap kebijakan, sasaran Sistem Manajemen Keamanan Informasi.dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian.

   Mengambil tindakan korektif dan pencegahan berdasarkan hasil internal audit Sistem Manajemen Keamanan Informasi.dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam Sistem Manajemen Keamanan Informasi.

Terimakasih ☺

Nama : Rachmat Akbar

Nim : 192420036

Kelas : MTI Ar 2

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 ----

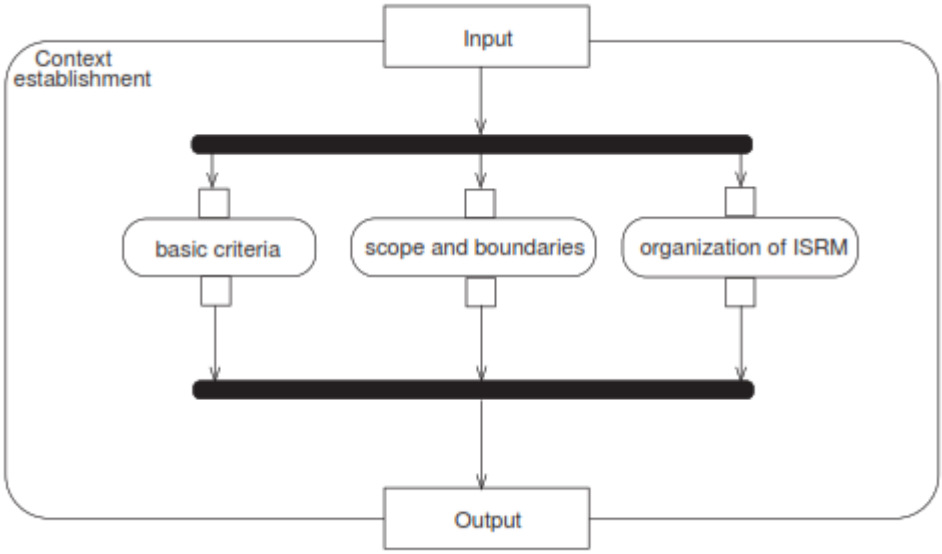
1. Risk treatment berhubungan erat dengan Hasil evaluasi resiko. Dapat dijelaskan sebagai berikut ; Hasil Evaluasi risiko berisikan pemahaman risiko yang diperoleh dengan proses identifikasi resiko dan proses analisis risiko untuk mengambil keputusan tentang tindakan apa yang harus dilakukan. Hasil Evaluasi resiko akan berisi Prioritas risk treatment dengan mempertimbangkan perkiraan tingkat risiko.
   Ada 4 opsi yang tersedia pada risk treatment, untuk mengurangi , menjaga, menghindari, dan men transfer resiko berdasarkan criteria hasil evaluasi resiko yang didapatkan pada proses sebelumnya. Pemilihan risk treatment haruslah didapatkan berdasarkan hasil penilaian risiko, biaya yang akan diperlukan untuk menerapkan opsi ini dan manfaat yang diharapkan dari opsi ini. Ketika pengurangan resiko yang besar bias dicapai dengan menggunakan cost yang rendah, opsi tersebut haruslah diimplementasikan.
   Sehingga dapat disimpulkan untuk mendapatkan risk treatment yang memuaskan maka perlulah dilakukan risk assessment sehingga akan menghasilkan hasil evaluasi resiko yang akan digunakan sebagai input pada proses risk treatment.
   Contoh : Dari hasil risk assessment didapatkan bahwa adanya resiko kehilangan data penting akibat back up data yang dilakukan jarang dilakukan, maka pada risk treatment dapat

dilakukan risk reduction dengan melakukan penerapan back up yang lebih sering (semi synchronous back up / a synchronous back up)

2. Tahapan-tahapan pada proses information security risk management adalah
   a. Establishing the context
   b. Risk assessment
   c. Developing risk treatment plan
   d. Risk acceptance

a. Context Extablisment

Konteks untuk information security risk management haruslah ditetapkan terlebih dahulu, yang melibatkan pengaturan basic criteria yang diperlukan untuk manajemen risiko keamanan informasi), mendefinisikan scope and boundaries dan membangun organisasi yang tepat yang mengoperasikan manajemen risiko keamanan informasi .



1. Basic Criteria

Basis criteria dibuat dengan serangkaian sumber daya, yang harus diperoleh sebelum pembuatan suatu system, seperti aset apa yang diperlukan agar system berjalan. Dalam hal ini adalah *Employee Monitoring Software ,* aset – aset yang diperlukan seperti desktop / notebook , jaringan internet yang baik serta software lain yang mendukung pekerjaan work from home.

2. Scope and boundaries

Cakupan proses manajemen risiko keamanan informasi perlu ditetapkan untuk memastikan bahwa semua relevan aset diperhitungkan dalam penilaian risiko. Selain itu, perlu diidentifikasi batasan-batasannya. Pada employee monitoring software ini scope dan boundariesnya hanya akan berfokus pada resiko yang bisa dialami ketika melakukan penerapan work from home .

3. Organization of ISRM

Organization of isrm berisikan stakeholder yang terlibat dalam employee monitoring software dalam hal ini adalah pegawai yang bekerja dari rumah dan stakeholder yang bertugas memonitoring kerja dari pegawai tersebut.

b. Risk assessment pada employee monitoring software selanjutnya akan saya jelaskan pada file excel

Nama : Rachmat akbar
Nim 192420036

NO.	Daftar Aset		LOSS E
	Aset	**Risk Category**	**Ancaman**
1	Desktop / Notebook / Desktop Replacement	C/A	Kehilangan komponen tertentu / keseluruhan desktop / notebook
		C/A	Tidak bisanya diterapkan remote enployee monitoring software
		C	Rusaknya Desktop akibat tegangan listrik yang tidak stabil
2	Software Berlisensi	A	Masa aktif lisensi habis
		C	instalasi software berlisensi secara ilegal

Nama : Rachmat akbar
Nim 192420036

Deskripsi Resiko	
EVENTS	**DAMPAK RESIKO**
Kelemahan	**Keterangan**
Kesulitan pemantuan karena pegawai yang bekerja dari rumah	Data yang tersimpan dalam harddisk / CD ROM dapat diketahui oleh orang lain
Desktop / notebook pegawai yang tidak mencapai minimum kriteria sehingga tidak bisa menjalankan aplikasi employee monitoring software	tidak bisa menyelesaikan pekerjaan secara work from home
Tidak dilengkapinya desktop / notebook dengan pengaman tegangan listrik seperti upsi	tidak bisa menyelesaikan pekerjaan secara work from home
Tidak ada mekanisme pemeliharaan lisensi	Tidak mendapat support dari vendor apabila ada permasalahan software, tidak mendapatkan versi update
Tidak ada mekanisme / manajemen penggunaan lisensi	virus / malware / ransomware yang akan berakibat hilangnya data / dicurinya data perusahaan

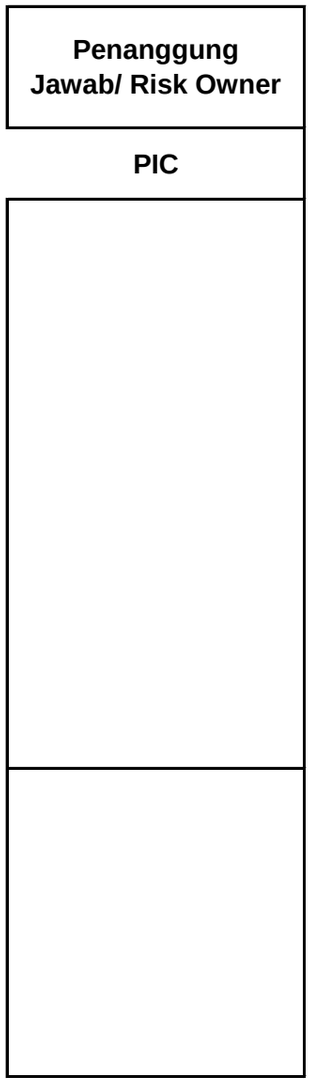
Risk assessment pada employee monitoring

RESIKO INHEREN			CURRENT ACTIONS/CO
Dampak	**Kemungkinan**	**Profil**	**Pengendalian yang ada**
Katastropik	Kadang-Kadang		Belum ada aturan khusus
Parah	Kadang-Kadang		Pinjam pakai notebook / desktop kepada pegawai yang membutuhkan
Moderat	Kadang-Kadang		belum ada aturan khusus
Ringan	Mungkin		Seluruh software berlisensi dipelihara oleh Divisi Ti dan selalu diupdate lisensinya
Katastropik	Mungkin		Penggunaan software sudah diatur dalam IT Security Policy, tapi belum ada aturan siapa yang berhak menggunakan software tertentu

software

NTROLS TO MANAGE THE RISK			RESIDUAL RIS	
Kelayakan	**Penerapan**	**Efektifitas**	**Dampak**	**Kemungkinan**
Kurang Tepat	Tdk Konsisten		Moderat	Mungkin
Tepat Sasaran	Selalu Diterapkan		Moderat	Mungkin
Lemah	Tdk Konsisten		Moderat	Kadang-Kadang
Tepat Sasaran	Selalu Diterapkan			
Lemah	Tdk Konsisten			

K	RESIKO DITERIMA	R I S K M I T I G A T I O N
Priority	**Mitigasi / Terima / Transfer**	**Rekomendasi & Pengendalian Baru**
	Mitigasi	Melakukan back up data penting dan melakukan enkripsi terhadap data yang ada sehingga data tersebut akan aman .
	Mitigasi	melakukan list pengecekan spesifikasi hardware desktop / notebook pegawai sebelum memberlakukan work from home
	Mitigasi	Mewajibkan Pegawai dari rumah melengkapi perangkat yang mereka punya dengan ups untuk menghindari kerusakan dan tidak selesainya pekerjaan
		Melakukan pengecekan berkala atas lisensi software yang digunakan
		Mencegah pegawai menggunakan software bajakan guna menghindari virus / malware / ransomware yang dapat merusak data pada desktop dan mencuri data penting perusahaan


Penanggung Jawab/ Risk Owner
PIC

Nama : Ria Aprinda

NIM : 192420022

Kelas : MTI 21 Regular A R1

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. Evaluasi Resiko (*Risk Evaluation*) adalah proses dalam membandingkan risiko yang telah diperkirakan dengan kriteria risiko yang telah ditentukan. Evaluasi risiko memperhitungkan apakah risiko dapat ditoleransi atau tidak didasarkan pada *level of risk* (tingkatan risiko) pada matriks risiko. Sedangkan *Risk Treatment* bertujuan untuk menentukan tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara keseluruhan. Hubungan *risk evaluation* dengan *risk treatment* yaitu *risk treatment* merubah *risk evaluation* yang merupakan analisis sebelumnya menjadi tindakan substantif untuk mengurangi risiko. Apabila risiko yang telah dinilai masuk kedalam kriteria yang ditetapkan maka risiko tersebut harus mendapatkan *treatment* (perlakuan) sebaliknya apabila risiko tidak termasuk kedalam kriteria yang ditetapkan maka perlakuan terhadap risiko tidak perlu dipertimbangkan lagi.
   Contoh : Hasil penelitian *level of risk* berdasarkan sebaran resiko dan *likelihood impact* pada suatu *document management system* menunjukkan bahwa dari identifikasi terhadap 13 resiko yang ada, 7 resiko memiliki tingkatan rendah dan 6 resiko mendapatkan tingkatan resiko medium. Maka untuk 6 resiko medium tersebut perlu adanya *treatment*. Misal 1 dari 6 resiko medium adalah resiko *Power Outage*, maka *treatment*nya adalah penggunaan UPS atau *power generator*.

2. Analisis Risk Management untuk monitoring produktifitas karyawan WFH dengan *Employee Monitoring Software:*

Dua tahapan awal dari ISO 27005-2008 merupakan Penetapan Konteks dan Penilaian Risiko.

1. Penetapan Konteks

Konteks manajemen risiko harus ditetapkan, yang melibatkan penetapan kriteria dasar yang diperlukan untuk manajemen risiko, mendefinisikan ruang ruang lingkup dan batasan-batasan, dan membentuk sebuah organisasi yang layak menjalankan manajemen risiko.

1.1 Kriteria Dasar

Work From Home (WFH) adalah pelaksanaan bekerja jarak jauh dan tidak harus di kantor atau adanya kebutuhan tertentu yang mengharuskan berada di rumah seperti saat pandemic COVID19 ini. Dibutuhkan persyaratan minimum yang sebaiknya terpenuhi sebagai pendukung agar *work from home* menjadi berkualitas. Penelitian ini membahas tentang Analisis Risk Management untuk monitoring produktifitas karyawan WFH dengan *Employee Monitoring Software.*

1.2 Ruang Lingkup dan Batasan

Penelitian dibatasi pada pegawai *Work From Home* berupa manajemen jam kerja, kehadiran, dan efektivitas kinerja menggunakan *Employee Monitoring Software*.

1.3 Organisasi Manajemen Risiko

Pihak-pihak yang terlibat dalam penelitian ini adalah pegawai yang melakukan *Work From Home* (end user) dan organisasi/perusahaan (pihak manajemen) sebagai pengguna *Employee Monitoring Software*.

2. Penilaian Risiko

Penilaian risiko menentukan nilai aset informasi, mengidentifikasi ancaman-ancaman yang berlaku dan kerentanan yang ada (atau bisa ada), mengidentifikasi kontrol yang ada dan efeknya pada risiko yang teridentifikasi, menentukan konsekuensi potensial dan akhirnya memprioritaskan risiko yang diperoleh dan menggolongkan mereka terhadap kriteria evaluasi risiko yang diatur dalam penetapan konteks.

2.1 Analisis dan Evaluasi Risiko

Analisis risiko sebagai proses penilaian terhadap risiko yang telah teridentifikasi dalam rangka mengestimasi kemungkinan munculnya dan besaran dampak untuk menetapkan level atau status risikonya. Evaluasi Resiko (*Risk Evaluation*) adalah proses dalam membandingkan risiko yang telah diperkirakan dengan kriteria risiko yang telah ditentukan. Evaluasi risiko memperhitungkan apakah risiko dapat ditoleransi atau tidak didasarkan pada *level of risk* (tingkatan risiko) pada matriks risiko. Status risiko ditentukan berdasarkan kombinasi antara kemungkinan (probabilitas/frekuensi) terjadinya risiko dan dampak (efek) jika risiko terjadi. Masing-masing dinyatakan dalam satuan nilai kualitatif berupa low (L), medium (M), dan high (H).

No.	Risiko	Probabilitas	Efek
1	Kesulitan komunikasi/menghubungi pegawai	M	M
2	Produktifitas pegawai berkurang karena tercampur dengan urusan rumah	H	H
3	Menambah beban kerja rekan yang WFO	M	M
4	Keamanan data dan informasi perusahaan terancam	H	H
5	Perangkat tidak lengkap atau kurangnya dukungan teknis	H	H

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 ----

Jawab 1:

Keterikatan antara risk treatment dan risk evaluation itu sangat erat erat, Karena sebelum tidak bisa melakukan risk treatment jika belum menyelesaikan tahapan *risk assesment.*

Konteksnya ditetapkan terlebih dahulu. Kemudian penilaian risiko dilakukan. Jika hal ini memberikan informasi yang cukup untuk secara efektif menentukan tindakan yang diperlukan untuk memodifikasi risiko ke tingkat yang dapat diterima, maka tugas selesai dan selanjutnya menentukan *Risk Treatment*.

Contoh : Fitur Informasi Nomor HP Resto atau Merchant GoFood yg tertera di Aplikasi GoFood Customer disalah gunakan untuk penipuan.
Resikonya adalah banya modus penipuan yang mengatasnamakan Gojek. Seperti meminta Nomor ATM dan Kode VCC 3 Digit yg digunakan untuk Debit online oleh si penipu, jika tidak memberikan data tersebut resto merchant akan di tutup paksa.

Jawaban 2:

Identifikasi Risiko

Tujuan dari identifikasi risiko adalah untuk menentukan apa yang bisa terjadi untuk menyebabkan potensi kerugian, dan untuk mendapatkan wawasan tentang bagaimana, di mana dan mengapa kerugian yang mungkin terjadi. Untuk melakukan identifikasi risiko, maka harus dilakukan identifikasi aset terlebih dahulu pada level rincian yang tepat.

Data Aset

No	Aspek Keamanan Teknologi Informasi	Aset	Jenis Aset	Pemilik Aset	Lokasi Aset
1	Teknologi	Aplikasi Monitoring WFH	Aset Utama	PT. Xyz	Data Center Kantor Pusat
2		Database			
3		Server			
4		PC			
5		OS			
6		Antivirus			
7		VPN			
8	SDM	Manager Pusat	Aset Utama	PT. Xyz	Data Center Kantor Pusat
9		Manager Cabang		Cabang	
10		Staft Sales		Cabang	
11	Proses Bisnis	Proses input data pengguna	Aset Utama	Kantor Pusat	Data Center
12		Proses input task yang harus dikerjakan sales		Kantor Cabang	Kantor Cabang
13		Proses Input hasih pekerjaan		Kantor Cabang	Kantor Cabang

Tabel ancaman pada setiap aset

No	Asset	Ancaman	Penyebab Ancaman	Sumber
1	Aplikasi Monitoring WFH	Layanan Tidak Berjalan	- Aplikasi Error / Tidak Bisa di Akses Karena Proses - Troubleshooting Lama - BCP Gagal terimplementasi	-Teknisi - Pengembang Aplikasi
2	Database	- Password Lemah	- Akses oleh pihak yang tidak berwenang	- Teknisi - Pengembang Aplikasi
3	Server	- Server aplikasi dan database tidak ada konfigurasi standar keamanan minimal (baseline security standard)	- Adanya perubahan konfigurasi oleh salah seorang SIP yang tidak di ketahui oleh staf SIP lainnya	- Teknisi - Pengembang Aplikasi
4	PC	PC error	- Banyak Virus di PC	Virus Computer
5	OS	OS tidak berjalan dengan semestinya	- Banyak Virus di PC	Virus Computer
6	Antivirus	Antivirus tidak up-to-date	- Banyak Virus baru tidak terdeteksi	Teknisi
7	VPN	Link Bermasalah	- Link VPN Mati - Link Lambat	- Force Majeur - Teknisi
8	Manager	- Penyalahgunaan otoritas - Kesalahan dan kelalaian yang disengaja atau tidak disengaja (contoh : Kesalahan entri data)	-Penyalahgunaan komputer- Input dipalsukan - Menyebarkan virus - Penjualan informasi pribadi - Sistem akses yang tidak sah	Orang Dalam (karyawan yang kurang terlatih, lalai atau tidak jujur)
9	Staft Sales	Laporan Tugas tidak tercatat	Proses Pelaporan gangguan tidak ter eskalasi	Staft Sales Force Majeur
10	Proses input data pengguna	Kesalahan pemilihan Manager dan Sales	Kelalaian, Ketidak pahaman	Manager Pusat

11	Proses input task yang harus dikerjakan sales	Terlambat menginput tugas	Kelalaian	Manager Cabang
12	Proses Input hasih pekerjaan	Terlambat Mengirimkan Laporan	Kelalaian	Staft Sales

Nama : Ryan Andrian
NIM : 192420006
Kelas : MTI A R1
Mata Kuliah : IT Risk Management & Disaster Recovery (ITRM & DR)

U A S

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 !

   Jawab :
   Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko karena risk treatment merupakan langkah-langkah yang akan ditempuh untuk menanggulangi segala resiko yang mungkin akan terjadi pada suatu sistem yang telah di identifikasi sebelumnya (berdasarkan hasil evaluasi risiko). Misal mengenai backup data, pada hasil evaluasi resiko mendapat skor “resiko tinggi” apabila tidak dilakukan yang akan menyebabkan hilangnya data-data penting ketika diserang virus seperti ransomware, data yg hilang tersebut tidak akan dapat di recover kembali, sehingga risk treatment yang dilakukan adalah dengan melakukan backup data secara periodik dan pengujian backup tersebut untuk memastikan file dan data aman jika diperlukan untuk proses recovery.

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)

   Jawab :
   Contoh Employee Monitoring software misalnya Teramind yaitu aplikasi yang memungkinkan bisnis owner atau administrator untuk memantau segala aktivitas yang dikerjakan di komputer setiap karyawannya.

❖ Tahap pertama yang harus dilakukan adalah mengidentifikasi segala resiko yang mungkin terjadi dalam penggunaan aplikasi Teramind tersebut. Baik dari segi user, perangkat (sisi server / sisi client), jaringan komunikasi (LAN / internet), dan software itu sendiri.

Kemungkinan resiko user :
- Kecerobohan user admin dalam pembuatan / penyimpanan sehingga password dapat bocor dan diketahui user client
- Kurangnya pemahaman user admin dalam konfigurasi aplikasi menyebabkan kurang maksimalnya penggunaan aplikasi tersebut
- Longgarnya keamanan di ruangan admin sehingga dapat dimasuki sembarang orang

Kemungkinan resiko perangkat :
- Kerusakan perangkat menyebabkan aplikasi tidak dapat dijalankan

Kemungkinan resiko jaringan komunikasi :
- Putusnya jaringan menyebabkan computer client tidak dapat dipantau aplikasi

Kemungkinan resiko software :
- Kebocoran data kepada pihak ketiga (vendor software)

❖ Tahap kedua yang harus dilakukan adalah mengidentifikasi risk treatment berdasarkan hasil dari risk identification pada tahap pertama untuk menentukan langkah apa saja yang harus diambil apabila salah satu atau beberapa kemungkinan resiko diatas terjadi.

Treatment resiko user :
- Membaca dan memahami petunjuk penggunaan aplikasi teramind, baik panduan teks, gambar maupun video tutorial
- Lebih hati-hati dan teliti dalam penyimpanan password dan memahami konsep pembuatan password dan cara memanage password yang baik dan benar
- Menggunakan pengamanan kartu akses atau pengenalan biometric untuk memastikan hanya admin / bisnis owner yang bisa masuk

Treatment resiko perangkat :
- Dilakukan proses perawatan secara berkala / perbaikan perangkat yang rusak

Treatment resiko jaringan komunikasi :

- Monitoring secara berkala baik software pemantau traffic jaringan, hardware (router, switch, wireless hotspot), dan instalasi kabel jaringan

Treatment resiko software :

- Pastikan membaca dengan teliti mengenai terms & agreement penggunaan aplikasi

Nama : **Sela Taramita**

NIM : **192420038**

Kelas : **R1**

"IT Risk Management"

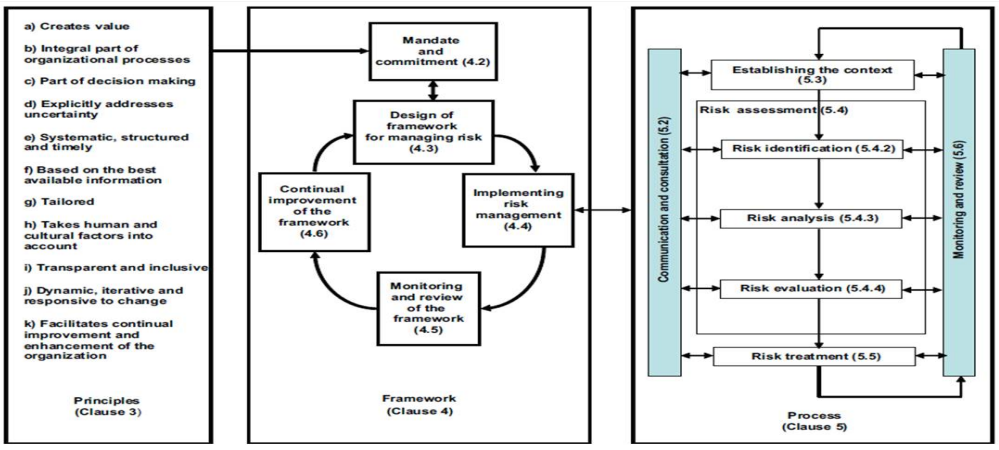
Pertanyaan:

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. Berdasarkan ISO 31000 : 2009
   Risk Treatment dan hasil evaluasi resiko sangat berhubungan seperti pada table di bawah ini :



Relationships between the risk management principles, framework and process based on ISO 31000:2009

Pada Risk assessment (Penilaian resiko) terdiri dari 3 bagian yaitu :

a. Identifikasi resiko : mengidentifikasi risiko apa saja yang dapat mempengaruhi pencapaian sasaran organisasi
b. Analisis resiko : menganalisa kemungkinan dan dampak dari risiko yang telah diindentifikasi
c. Evaluasi resiko : membandingkan hasil analisis risiko dengan kriteria risiko untuk menentukan bagaimana penanganan risiko yang akan diterapkan

Sedangkan untuk Risk treatment (Penanganan risiko) didalam organisasi terdiri dari :

a. Menghindari risiko (Risk avoidance)
b. Mitigasi risiko (Risk reduction) : dapat dilakukan dengan mengurangi kemungkinan atau dampak yang akan terjadi
c. Transfer risiko kepada pihak ketiga
d. Menerima risiko (risk acceptance)

Untuk hubungan risk treatment dan hasil evaluasi risiko sangat berhubungan dikarenakan untuk menentukan bagaimana penanganan risiko yang akan diterapkan membutuhkan risk treatment. Pada contoh sistem pembelajaran daring.

Sistem pembelajaran daring dimana orang-orang melakukan kegiatan belajar mengajar menggunakan media internet. Pada sistem pembelajaran daring ini ada beberapa permasalahan yang ada yaitu risiko yang terjadi. Dalam sistem pembelajaran daring kita sering mendapat beberapa kendala misalnya jaringan internet yang tidak stabil, kurangnya pemahaman dalam menggunakan media daring bagi beberapa orang yang awam dengan internet dan sulitnya untuk media yang digunakan untuk pembelajaran daring. Dengan kendala yang ada seperti ini perlunya penanganan risiko (Risk Treatment) dimana kita harus bisa menghindari risiko yang ada pada pembelajaran daring ini misalnya dengan menggunakan jaringan provider yang stabil, belajar dengan teman atau saudara agar bisa menggunakan internet dalam pembelajaran daring dan menyiapkan media pembelajaran daring seperti laptop (computer) dan kuota. Selain kita menghindari risiko yang terjadi kita harus bisa memitigasi risiko yang akan terjadi, jika proses pembelajaran daring ini bermasalah. Selain itu berbagi risiko kepada pihak ketiga misal disini bersama sama dengan teman untuk saling membantu proses belajar daring dan juga menerima risiko apapun yang terjadi. Dengan adanya risk treatment ini kita dapat menarik kesimpulan untuk dapat menentukan bagaimana penanganan risiko agar sistem pembelajaran daring dapat dilakukan tanpa adanya kendala.

2. Software atau teknologi yang digunakan Refog Employee Monitoring

   Risk management dalam penggunaan software ini :

   a. Penggunaan aplikasi atau software yang legal dan terpecaya

      Dengan menggunakan aplikasi atau software yang legal dan terpecaya dapat menciptakan rasa aman baik dari perusahaan ataupun karyawan. Data data dan informasi yang berkaitan dengan kerahasiaan perusahaan atau karyawan dapat terjamin dan terhindar dari pencurian data perusahaan atau karyawan.

b. Tetap menjaga privasi karyawan

   Penggunaan software employee monitoring sangat baik bagi perusahaan dalam hal mengawasi kinerja atau produktivitas karyawan. Ditengah pandemi dimana dibuat sistem kerja dirumah (WFH), pengguna software atau aplikasi ini sangat membantu dalam hal memonitor aktivitas kerja setiap karyawan dirumah mereka masing-masing. Karyawan berkerja dengan baik dan disiplin ketika mereka diawasi. Namun perlu diperhatikan pengawas secara berlebihan dapat membuat karyawan merasa privasi mereka sedikit terganggu (merasa kurang nyaman). Bukankah menciptakan rasa saling percaya lebih baik daripada saling mencurigai ? karyawan yang mencurigai atasan yang sedang santai tidak berkerja dirumah saat work from home (WFH) atau atasan yang mencurigai karyawan yang tidak disiplin bekerja dirumah saat work from home (WFH).

c. Cyber Attack Awareness

   Software atau aplikasi yang digunakan harus aman dari virus, malware yang dapat mengancam data perusahaan. Tetap menggunakan anti virus yang baik dalam hal memproteksi computer.

Menurut ISO 27005-2008 : dua tahapan awal dalam dalam proses *information security risk management* dalam software atau teknologi : Refog Employee Monitoring yaitu :

1. Plan : establishing the context, risk assessment, developing risk treatment plan and risk acceptance
2. Do : implementation of risk treatment plan
3. Check : continual monitoring and reviewing of risks
4. Act : maintain and improve the information security risk management process

Untuk software atau teknologi : Refog Employee Monitoring dalam proses *information security risk management* dilakukannya :

1. Rencana : dalam menggunakan software ini harus melihat dan menganalisa dari segi penggunaannya, risiko yang terjadi, bagaimana menangani risik dan dapat menerima risiko tersebut
2. Lakukan : merencanakan penanganan risiko

Dua tahapan awal ini yang dilakukan dalam proses *information security risk management.*

IT RISK MANAGEMENT & DISASTER RECOVERY

Dedy Syamsuar, MIT, PhD

KELAS MTI AR 21

NAMA: SURIANI

NIM : 192420011

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 sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya karena merupakan elemen inti dari manajemen risiko, sebuah proses yang memungkinkan manager untuk menyeimbangkan biaya operasional dari tindakan perlindungan untuk mencapai keuntungan dengan melindungi sistem dan data TI yang mendukung misi sebuah organisasi.

   Risk Treatment menghubungkan Risk Assessment dengan identifikasi dan desain pengendalian yang sesuai, sehingga pendekatan risiko yang ditetapkan telah diterapkan, diuji, dan ditingkatkan. Untuk organisasi mana pun, proses dua fase ini sangat penting - proses ini mempersiapkan, menilai, dan memelihara keamanan setiap aset informasi.

2. Tahapan awal dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008 yaitu :
   a. Penetapan Konteks, Pada penetapan konteks dilakukan pemilihan kriteria dasar, yakni kriteria evaluasi risiko yang dipilih, kriteria dampak yang ditentukan oleh organisasi tersebut, dan kriteria penerimaan risiko agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran perusahaan secara keseluruhan.

      Contohnya :

      - Pada aplikasi zoom

        Zoom merupakan aplikasi komunikasi dengan menggunakan video. Aplikasi tersebut dapat digunakan dalam berbagai perangkat seluler, desktop, hingga telepon dan sistem ruang aplikasi Zoom pada iOS juga diketahui membagikan data-data analitik milik pengguna kepada Facebook, meski sang pengguna tersebut tak memiliki akun Facebook. Zoom memberikan notifikasi kepada Facebook ketika pengguna sedang membuka aplikasi. Selain itu, data-data seperti model perangkat yang digunakan, jam, operator seluler, hingga data-data yang bisa digunakan untuk iklan juga disetorkan kepada Facebook.Zoom juga sempat mendapat protes keras saat diketahui memiliki fitur "attention tracking". Dengan fitur ini, sang "host" video konferensi dapat mengetahui siapa saja anggota yang tidak memperhatikan video konferensi tersebut. Fitur ini dapat memberikan pemberitahuan kepada host tersebut ketika salah seorang anggota membuka windows lain selama lebih dari 30 detik. Zoom juga memiliki kebijakan privasi yang kontroversial. Sebelum kemudian diubah beberapa waktu lalu, kebijakan tersebut memungkinkan Zoom untuk menyimpan segala bentuk informasi yang ada pada saat panggilan video dilakukan.

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. Risk Treatmen adalah suatu kegiatan yang dilakukan untuk mengatur suatu kegiatan yang bisa menimbulkan suatu resiko.

   Sebelum melakukan kegiatan yang mengandung resiko, langkah yang dilakukan adalah menganalisa tingkatan resiko dan mengantisipasi resiko apa yang akan terjadi. Suatu kegiatan sebelum dilempar ke publik diharuskan melakukan terlebih dahulu simulasi resiko di kalangan sendiri dengan memberikan perlakuan yang akan berakibat kerusakan dengan tingkatan paling kecil sampai paling besar. Hal ini dilakukan agar dampak perlakuan tersebut dapat diantisipasi jika kegiatan tersebut dilempar ke publik atau diserahkan ke khalayak umum.

   Contoh:

   Server dengan IP publik yang akan di akses oleh umum, seorang administrator server membuat rule-rule tertentu agar server tersebut aman dari serangan yang dapat menimbulkan crash dari server tersebut, bisa data hilang, data rusak atau data di ambil alih oleh orang yang tidak berhak memiliki data tersebut.

2. Agar kegaitan karyawan dapat termonitoring dan ter trackng dengan baik, sebaiknya memang suatu perusahaan harus menyiapkan sendiri software yang dipakai khusu di kalangan perusahaan tersebut utk meminimalisir tingkat resiko kebocoran data.
   Untuk saat ini mungkin sebagian besar perusahaan belum memiliki software sendiri, analisa saya perusahaan masih wait and see dengan pandemi saat ini. Kemungkinan ke depan bisa saja suatu perusahaan memiliki software sendiri.
   Contoh software berbayar yang saya ketahui untuk memonitor karyawan dan juga kinerja karyawan adalah software ***Trello*****,** Software ini di desain untuk semua kegiatan karyawan baik perorangan ataupun kelompok. Setiap hari karyawan wajib input keiatan (Task), detail task, target waktu, status task sampai ke bukti penyelesaian jika tercapai atau kendala yang ada jika tercapai. Setiap kegiatan akan termonitoring oleh admin perusahaan, walau tanpa tatap muka setiap kegiatan akan terlihat. Dengan penggunaan software ini maka progres karyawan dapat di tracking sampai ke penilaian persentase kinerja yang dapat dievaluasi per hari, per bulan samapi per tahun berjalan

The assignment of IT Risk Management & Disaster Recovery
From Mr. Dedy Syamsuar, MIT, Ph.D.

Yudy Pranata
AR2 192420001
Magister Teknik Informatika
Universitas Bina Darma

Soal:

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

2. Monitoring produktifitas seorang karyawan merupakan hal yang penitng 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 sangat berhubungan erat dengan hasil evaluasi resiko dikarenakan risk treatment adalah langkah selanjutnya dalam proses information security risk management pada ISO 27005-2008. Contoh apabila terdapat celah resiko yang muncul pada suatu aplikasi contoh Gojek. Sering kali beberapa pengendara ojek online mendapatkan "Fake order" pada fasilitas Gofood, setelah melalui proses identifikasi (risk analysis) kita mendapatkan hasil evaluasi resiko tersebut dan setelahnya mencari solusi untuk meminimalisir resiko yang akan terjadi lagi kedepannya apakah setiap pemesanan Gofood harus menggunakan Gopay dan sebagainya.

2. Dengan adanya teknologi "*Employee Monitoring Software*" memang kita dapat memonitor dan mentracking pekerjaan yang dilakukan oleh karyawan tersebut, tetapi terdapat beberapa resiko yang akan dialami. Contoh apabila menggunakan teknologi seperti Google Drive yang bisa langsung update pekerjaan yang telah dikerjakan setelah disimpan. Pada pihak perusahaan pasti mempertanyakan privasi dari file yang telah di simpan dalam Google Drive tersebut apakah aman ataukah file tersebut dapat diakses oleh pihak Google tersebut. Begitupun dengan teknologi yang diberikan oleh perusahaan tersebut yang akan dideploy keseluruh karyawan dengan konteks merekam seluruh aktifitas karyawan apakah tindakan tersebut tidak melanggar privasi karyawan tersebut. Jadi dengan adanya batasan mungkin diluar waktu kerja teknologi "*Employee Monitoring Software*" tersebut bisa dinonaktifkan agar aktifitas diluar waktu kerja karyawan tersebut tidak dapat di monitor dan juga membatasi akses teknologi tersebut pada PC atau laptop karyawan.

UAS

IT RISK MANAGEMENT & DISASTER RECOVERY
Dedy Syamsuar, MIT, PhD

KELAS MTI AR 21

NAMA : Yuliza Aryani

NIM : 192420021

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengenal, 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 adalah proses menanggulangi risiko dengan:

   1. Menghindari risiko
   2. Menurunkan risiko (mitigation)
   3. Meniadakan sumber risiko
   4. Menurunkan konsekuensi dan atau kemungkinan
   5. Tetap mepertahankan risiko yang ada
   6. Berbagi (sharing) risiko dengan pihak lain

Evaluasi risiko dimaksudkan untuk membantu proses pengambilan keputusan berdasarkan hasil analisis risiko. Evaluasi risiko merupakan proses pembandingan antara level risiko yang ditemukan selama proses analisis dengan kriteria risiko yang ditetapkan sebelumnya.

Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas risiko-risiko tersebut dengan mengacu pada “kriteria risiko”. Dengan kata lain hasil dari evaluasi risiko menunjukkan peringkat risiko yang memerlukan penanganan (mitigasi) lebih lanjut dengan mengacu pada tingkat risiko yang dapat diterima.

2. Risk Management penggunaan aplikasi zoom

a. Zoom merupakan aplikasi komunikasi dengan menggunakan video. Aplikasi tersebut dapat digunakan dalam berbagai perangkat seluler, desktop, hingga telepon dan sistem ruang

   aplikasi Zoom pada iOS juga diketahui membagikan data-data analitik milik pengguna kepada Facebook, meski sang pengguna tersebut tak memiliki akun Facebook. Zoom memberikan notifikasi kepada Facebook ketika pengguna sedang membuka aplikasi. Selain itu, data-data seperti model perangkat yang digunakan, jam, operator seluler, hingga

   data-data yang bisa digunakan untuk iklan juga disetorkan kepada Facebook. Zoom juga sempat mendapat protes keras saat diketahui memiliki fitur "attention tracking". Dengan fitur ini, sang "host" video konferensi dapat mengetahui siapa saja anggota yang tidak memperhatikan video konferensi tersebut. Fitur ini dapat memberikan pemberitahuan kepada host tersebut ketika salah seorang anggota membuka windows lain selama lebih dari 30 detik. Zoom juga memiliki kebijakan privasi yang kontroversial. Sebelum kemudian diubah beberapa waktu lalu, kebijakan tersebut memungkinkan Zoom untuk menyimpan segala bentuk informasi yang ada pada saat panggilan video dilakukan.

b. Aplikasi Telemedis memberikan kesempatan kepada dokter dan pasien untuk saling berinteraksi dari jarak jauh. Layanan telemedis antara dokter dan dokter telah lama berkembang dalam bentuk konsul, dan saat ini telesurgery dan teleradiologi merupakan fitur yang potensial untuk dikembangkan.

   Layanan telemedis mengundang berbagai topik yang berpotensi menjadi masalah etik, yang relevan dengan pelaksanaannya di Indonesia antara lain masalah privasi dan konfidensialitas pasien, serta berubahnya interaksi tatap muka dokter-pasien

   Peretasan keamanan konfidensialitas data pasien termasuk data teks, audio, dan visual/video adalah salah satu risiko utama sistem telemedis. Hal ini sangat perlu untuk diperhatikan, lebih-lebih bila ada data-data sensitif pasien yang akan sangat merugikan

jika terpublikasi, seperti riwayat penyakit menular seksual dan gangguan jiwa. Hendaknya keamanan data yang bersifat konfidensial ini dijaga semaksimal mungkin, misalnya dengan memastikan dokter yang dikonsulkan berada di tempat yang dapat menjaga kerahasiaan (seperti dalam ruangan pribadi) bila menggunakan telepon, untuk mencegah orang yang mencuri dengar. Atau bila dilakukan dengan aplikasi chatting melalui ponsel pintar, hendaknya menggunakan aplikasi yang bereputasi baik dalam hal konfidensialitas,

Sementara itu, layanan telemedis juga menyebabkan perubahan interaksi tatap muka klasik dokter dan pasien. Secara positif, interaksi ini berarti pasien dapat menjangkau dokternya dengan lebih mudah, cepat, murah, dan sering. Pasien dapat terus mengkonsultasikan keadaan kesehataannya dengan dokter.

Nama : Yuni Astuti
NIM : 192420004
Mata Kuliah : IT Risk Management
Dosen : Dedy Syamsuar, PhD

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. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya karena merupakan elemen inti dari manajemen risiko, sebuah proses yang memungkinkan manager untuk menyeimbangkan biaya operasional dari tindakan perlindungan untuk mencapai keuntungan dengan melindungi sistem dan data TI yang mendukung misi sebuah organisasi. Tanpa Risk Assessment, Risk Treatment tidak

dapat dilakukan dan sebaliknya, Risk Treatment tidak dapat dilakukan tanpa Risk Assessment. Risk Assessment dan Risk Treatment tidak dapat dipisahkan.

- Risk Assessment memungkinkan untuk mengidentifikasi ancaman dan menilai kemungkinan ancaman tersebut, memanfaatkan beberapa kerentanan organisasi serta potensi dampak dari peristiwa tersebut yang terjadi. Setelah risiko diidentifikasi dan dinilai, proses penilaian berhenti.
- Risk treatment adalah proses tindakan atas risiko yang teridentifikasi. Diperlukan oleh ISO 27001 Standar, rencana perlakuan risiko mengidentifikasi tindakan, tanggung jawab, dan prioritas manajemen yang tepat untuk mengelola risiko keamanan informasi.

Risk Treatment menghubungkan Risk Assessment dengan identifikasi dan desain pengendalian yang sesuai, sehingga pendekatan risiko yang ditetapkan telah diterapkan, diuji, dan ditingkatkan. Untuk organisasi mana pun, proses dua fase ini sangat penting - proses ini mempersiapkan, menilai, dan memelihara keamanan setiap aset informasi.

2. Tahapan awal dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008 yaitu :

   Contoh softwarenya yaitu menggunakan Zoom Meeting

   a. Penetapan Konteks, Pada penetapan konteks dilakukan pemilihan kriteria dasar, yakni kriteria evaluasi risiko yang dipilih, kriteria dampak yang ditentukan oleh organisasi tersebut, dan kriteria penerimaan risiko agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran perusahaan secara keseluruhan. Dalam Zoom Video, memberikan layanan hingga hingga 10.000 peserta yang menyajikan video, audio, dan berbagi layar. Konferensi video ini menampilkan opsi pendaftaran, pelaporan, Q / A, polling, angkat tangan, indikator perhatian, dan perekaman MP4 / M4A). Penggunaan zoom meeting ini, karyawan diberikan password dan id meeting dengan memperhatikan risiko keamanan
   b. Identifikasi Resiko, pada tahap ini melakukan identifikasi aset-aset yang terkait dengan yang akan dilakukan manajemen risiko, baik itu aset utama maupun aset pendukungnya. API tersedia untuk mengintegrasikan Zoom dengan aplikasi pelanggan khusus dan aplikasi pihak ketiga. Setiap akun pelanggan dapat menyertakan kredensial kunci integrasi API yang dikelola oleh admin akun

pelanggan. Panggilan API dikirim dengan aman melalui layanan web yang aman dan otentikasi API diperlukan.

Nama : A.Firdaus
NIM : 192420043
Kelas : MTIR2

UAS
IT RISK MANAGEMENT & DISASTER RECOVERY

1. **Hubungan Risk Treatment dengan hasil evaluasi resiko**

   Risk Treatment adalah Sebuah Perawatan Resiko yang berkaitan dengan bagaimana resiko perlu ditangani dengan tahapan pengurangan risiko, retensi risiko, penghindaran resiko dan transfer resiko

   Hasil Evaluasi Resiko adalah Penilaian hasil indentifikasi dan pengemlompokan resiko ancaman resiko yang terjadi

   Hubungan yang ada pada risk treatment dengan hasil evaluasi ialah mencari potensi bahaya yang ada dan diklasifikasikan menurut jenis bahayanya, mengetahui akibat atau dampak apa saja yang ada karena bahaya tersebut dan mengetahui bagaimana terjadinya bahaya tersebut, melakukan evaluasi atau perbaikan terhadap risiko atau bahaya yang ada, mencatat semua temuan yang ada serta menilai atau mengkaji kembali hasil penilaian risiko tersebut untuk melakukan evaluasi sehingga tercapai pengendalian resiko yang sangat kecil kemungkinan terjadi.

   Sebagai contoh pada perguruan tinggi melakukan analisa risiko berdasarkan sumber daya manusia, aset IT, dokumen arsip, aplikasi yang dipakai dan database perguruan tinggi dengan Melakukan struktur kerja dalam pengelompokan bidang dengan memberikan tanggung jawab yang sesuai dengan kebutuhan aplikasi yang digunakan.

SOAL 2

Teknik Keamanan Sistem Infromasi WFH Selama Pandemi Covid-19

A. Pendahuluan

Perkembangan dan penyebaran Virus Corona (COVID-19) di Indonesia semakin mengkhawatirkan sejak 2 WNI dari Depok dinyatakan positif terinfeksi. Data terbaru per Akhir Juli yang dirilis pemerintah daerah melalui situs siaga covid - 19 total kasus positif Virus Corona (COVID-19) di Palembang menjadi 3000 orang. Untuk kasus yang meninggal dunia disebutkan diangka 150

Mengantisipasi perkembangan dan penyebaran Virus Corona (COVID-19) yang sangat cepat ini, Presiden Joko Widodo menerapkan kebijakan untuk menekan tingkat penyebaran virus yang mendunia ini dengan mengijinkan kepada para pekerja untuk bekerja di rumah atau Work From Home (WFH).

Lewat konferensi pers di Istana Kepresidenan Bogor pada hari Minggu, 15 Maret 2020, Jokowi meminta agar masing-masing kepala daerah untuk membuat kebijakan agar para pekerja bisa bekerja di rumah.

Kebijakan presiden ini kemudian ditindaklanjuti untuk membangun sistem informasi yang dapat membantu para pekerja untuk dapat bekerja seperti biasa walaupun ditempat yang berbeda. Untuk itu bagian Unit IT Terpadu merancang sebuah kebijakan – kebijakan dalam sistem informasi dimana dapat dipergunakan dan dirancang khusus dalam penggunaan baik dari keamanan dan fungsi sesuai standar ISO 27005-2008 tentang teknik keamanan resiko sistem informasi.

B. Cangkupan

Adapun cangkupan dalam sistem informasi ini yang bertanggung jawab dalam keamanan dan sistem informasi adalah Manager dan bagian IT terpadu dan dipergunakan untuk seluruh karyawan yang memungkinkan untuk bisa bekerja di rumah

C. Jenis Layanan Sistem Informasi

Adapun jenis informasi yang dipergunakan untu WFH antara lain :

No	Jenis Software	Kegunaan	Pengguna
1	Google Form	Absensi	Seluruh Karyawan
2	Email	Surat Menyurat	karyawan Administrasi
3	Chatting / Video Confrence	Meeting	Seluruh Karyawan
4	System Application and Product in Data Processing (SAP)	Operasional	Karyawan Penjualan

D. Proses Pelayanan Pendukung Sistem Infromasi saat WFH

1. Layanan Infrastruktur dan Teknikal

No	Layanan	Deskripsi	Pengguna Utama	Jenis Resiko
1	Server Web Hosting	Hardware , Software	Divisi IT	High
2	Jaringan Internet	Hardware , Software	Divisi IT	High

2. Layanan Perproses

No	Layanan	Deskripsi	Pengguna Utama	Jenis Resiko
1	Internet	Internet karyawan	Semua Divisi	Medium
2	Email	Email Karyawan	Semua Divisi	High
3	Aplikasi SAP	Akun karyawan	Semua Divisi	High
4	Absensi	Absensi Karyawan	Semua Divisi	Mediuml

E. Manajemen Resiko

1. Dampak
   Pekerjaan yang dilakukan saat WFH berdampak pada keamanan data saat esksekusi aplikasi.

2. Resiko Keamanan
   Resiko keamanan yang terjadi dengan kebocaran data yang dapat dibuka dari mana saja baik dari keteledoran akun pekerja baik dari komputer masing2 pekerja

3. Pencegahan Resiko
   Pencegahan resiko dapat dilakukan dengan penrgantian passwrd berkala dengan kombinasi huruf besar dan kecil, angka dan karakter dan menggunakan sistem operasi original dengan antivirus permium.

4. Komunikasi Resiko
   Pada komunikasi resiko untuk pemegang kendali dipertanggung jawabkan oleh Kepala Bidang IT dan diketahui oleh Manager Perusahaan

5. Indentifikasi Resiko
   Adapaun indentifikasi resiko tentang penyebaran data untuk bagian internal pada komunikasi resiko dan karyawan sendiri dan untuk bagian eksternal ditunjukan kepada oknum2 hacker yang tidak bertanggung jawab

IT Risk Management

Nama : Andrian Perdana

NIM : 192420017

Kelas : MTI21 AR1

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 ----

Jawab

1. Hasil evaluasi resiko sangat berpengaruh terhadap penanganan resiko itu sendiri, karena pada saat melakukan evaluasi dapat menggambarkan kelemahan-kelemahan yang dimiliki oleh suatu organisasi apakah resiko itu dalam kategori dapat diminimalisir, dapat diterima, dapat dihindari maupun di pindahkan.

   Misalnya dalam meminimalisir resiko asset elektronik yang dimiliki, pada saat evaluasi ditemukan beberapa masalah yang pernah terjadi di tempat kami yaitu beberapa kali peralatan jaringan sampai server mengalami kerusakan karena gangguan petir maupun tegangan listrik yang tidak stabil, padahal di gedung sudah terinstall alat anti petir. Hal ini diambil kesimpulan bahwa peralatan anti petir tersebut mungkin sudah tidak berfungsi karena factor umur. Akhirnya ditetapkan bahwa organisasi kami harus menganggarkan kegiatan evaluasi jaringan kelistrikan dan pembelian alat anti petir agar resiko pada saat terjadinya gangguan petir dan tegangan listrik yang tidak stabil bisa meminimalkan kerusakan pada asset peralatan yang dimiliki. Akan tetapi, karena penerapannnya membutuhkan anggaran yang lumayan besar tetapi system harus berjalan terus, maka diambil keputusan hanya pembelian dan instalasi alat anti petir

saja yang di lakukan. Sehingga resiko kerusakan peralatan karena tidak stabilnya tegangan yang dalam hal ini tergantung supply yang diberikan PLN dan tidak bisa kami kontrol walaupun sudah diupayakan dengan peralatan stabilizer tegangan, maka resiko ini masuk kategori resiko yang diterima oleh organisasi.

2. Adapun langkah yang pertama harus dilakukan adalah ;
    a. Identifikasi kemungkinan resiko yang ditimbulkan.
    Pencarian jawaban saya lakukan dengan memperhatikan sebuah aplikasi online yaitu workplus, dimana aplikasi ini bekerja dengan cara mendeteksi aplikasi yang tampil di monitor client sehingga apa yang dilakukan karyawan dapat diketahui tingkat produktivitasnya tergantung aplikasi yang dibuka yang keterkaitannya dengan aplikasi pendukung untuk bekerja.
        - Setelah saya perhatikan aplikasi ini memiliki resiko kemungkinan besar bocornya data yang dikerjakan oleh karyawan apabila di aplikasi ini tidak menerapkan data enkripsi pada proses pengiriman data dari karyawan sampai ke pimpinan manajemen perusahaan.
        - Selain itu dapat terjadi penggunaan aplikasi ini berbahaya apabila client atau staf melakukan transaksi keuangan melalui jaringan computer yang dipakainya sehingga dapat menimbulkan kerugian finansial bagi perusahaan maupun staf tersebut.

    b. Estimasi Resiko
    Dari dua kemungkinan resiko tersebut masuk dalam kategori resiko sedang karena apabila aplikasi tersebut menggunakan transfer data yang telah dienkripsi sehingga membutuhkan waktu yang lama untuk pencurian data tersebut.

IT RISK MANAGEMENT AND DISASTER RECOVERY

DEDY SYAMSUAR, M.T., PH.D.

ARDIANSYAH
192420013
MAHASISWA MTI AR1

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!

Jawaban:

1. Kita tidak pernah akan tahu apa yang akan terjadi pada perusahaan kita terkhusus dalam penggunaan *Information Technology*. Perlu suatu Analisa yang baik dan matang di dalam menghadapi hal-hal yang tidak diinginkan, dengan antisipasi Analisa yang baik dan akurat. Serta jalur koordinasi dalam tahapan penanganannya. Risk assessment merupakan proses keseluruhan dari *Risk Idnetification, Risk Analsis, Dan Risk Evaluation*

   Risk evaluation adalah proses dalam **membandingkan risiko yang telah diperkirakan dengan kriteria risiko yang telah ditentukan.** Evaluasi risiko memperhitungkan apakah risiko dapat ditoleransi atau tidak didasarkan pada level of risk (tingkatan risiko) pada matriks risiko. Bow-tie analysis pada risk analysis merupakan metode analisis yang digunakan untuk menggambarkan kegiatan manajemen risiko agar lebih mudah dimengerti dan diakses.

   Risk treatment bertujuan untuk menentukan **tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara keseluruhan**. Risk treatment merubah analisis sebelumnya, risk identification dan risk assessment, menjadi tindakan substantif untuk mengurangi risiko. Terdapat beberapa risk treatment yang umumnya digunakan, yaitu; risk prevention (pencegahan risiko) dengan tujuan untuk mengurangi secara substansial kemungkinan terjadinya risiko, risk mitigation (mitigasi risiko) dengan tujuan untuk meminimalkan konsekuansi dari risiko, risk sharing (berbagi risiko) dengan tujuan untuk memindahkan risiko tidak hanya ke organisasi lain namun juga ke entitas bisnis ataupin individu, dan risk retention (retensi risiko) atau dikenal juga sebagai penyerapan, toleransi, atau penerimaan risiko. Risk Treatment yang perlu dilakukan yaitu: menghindari risiko, menurunkan risiko, meniadakan sumber risiko, menurunkan konsekuensi dan atau kemungkinan – tetap mempertahankan risiko yang ada – berbagi risiko dengan pihak lain.

   Jadi dari penjelasan diatas maka dapatlah disimpulkan bahwa Risk Treatment dan Risk Evaluation merupakan bagian analisa Risk dalam Risk Management. Risk evaluation merupakan sebuah pernyataan untuk membandingkan tingkat dari resiko yang diestimasi dengan kriteria resiko yang telah ditetapkan pada saat context ditentukan. Hal ini dilakukan untuk menentukan seberapa pengaruh resiko tersebut terhadap organisasi dan untuk menentukan tipe dari resiko tersebut. Setelah melakukan sebuah risk assessment, risk treatment merupakan porses untuk memilih dan menyetujui satu atau lebih opsi untuk mengubah probabilitas terjadinya resiko tersebut. seperti yang telah dijelaskan pada ISO 31000, resiko dibagi menjadi resiko positif dan resiko negatif. dengan adanya risk treatment, diharapkan terdapat langkah-langkah yang tepat yang dapat dilakukan organisasi untuk mengurangi resiko negatif dan menoptimalkan resiko positif.

   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.

Contoh Risk Treatment pada Adira Finance

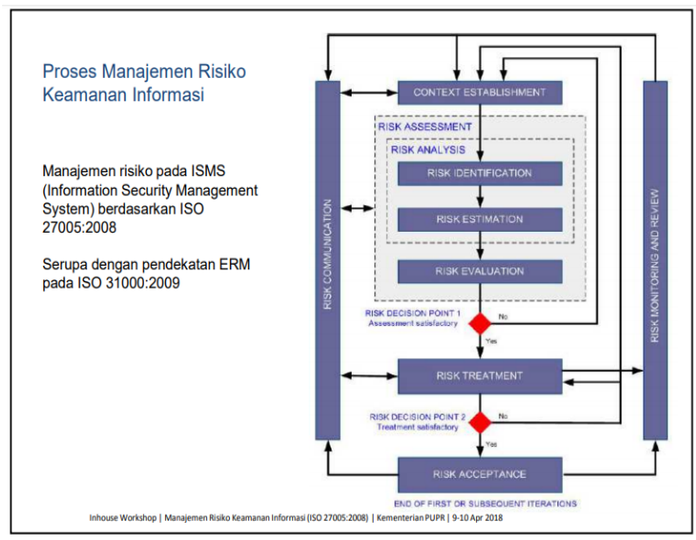
Berikut ini merupakan contoh sebagian risiko dan pengelolaannya oleh Adira Finance: Risk Event Action Risk Treatment 1. Risiko Kredit Konsumen tidak Reduce 1. Penerimaan mampu memenuhi Aplikasi Kredit kewajiban dalam yang selektif meluasi kredit 2. Penerapan Prinsip Mengenal Nasabah pada Lembaga Keuangan Non Bank 3. Analisis Portofolio dan sistem manajemen informasi 4. Pendelegasian wewenang persetujuan kredit 2. Risiko 1. Tidak Reduce 1. Pelaksanaan risk Operasional berfungsinya control self proses internal assessment 2. Kegagalan sistem 2. Pengelolaan kecurangan 3. Kesalahan manusia 3. Tinjauan terhadap kebijakan dan SOP secara rutin 4. Menetapkan Pedoman pengelolaan kelangsungan usaha 3. Risiko Pasar Kenaikan tingkat Mitigasi Penerapan bunga kredit pengelolaan tingkat bunga tetap secara konsisten dengan menyesuaikan tingkat bunga kredit terhadap tingkat bunga pinjaman dan beban dana 4. Risiko Tidak mematuhi atau Mitigasi Membuat divisi Kepatuhan melaksanakan peraturan sekretaris perusahaan untuk perundang-undangan melakukan dan peraturan lain pengawasan yang berlaku 5. Risiko Hukum Adanya tuntutan Mitigasi Membuat divisi hukum hukum untuk melakukan pengelolaan risiko hukum 6. Risiko Reputasi Adanya publikasi Mitigasi Membentuk tim dan Risiko negatif khusus untuk strategis mendukung penanganan kasus Risiko yang dikelola adalah berdasarkan pada selera risiko Adira Finance. Pada tahap ini Adira Finance mengelola risiko dengan mempertimbangkan dampak, frekuensi, biaya dan manfaat.

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 dimintau ntuk 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:

2. Dalam masa pandemi saat ini, pekerjaan dialihkan dari kantor kerumah dengan program yang disebut *Work From Home*. Hal ini tentunya akan membawa sebuah perubahan dalam sebuah system kerja. Banyak perusahaan telah menggunakan suatu system dibidang *information technology* didalam membantu proses pemantauan para karyawan yang bekerja WFH. Berbagai software telah dikembangkan, sehingga kita sebagai seorang managerial dibidang IT dituntut untuk menganalisa sebuah aplikasi dalam penggunaannya di perusahaan. Berdasarkan ISO 27005-2008 terhadap proses *information security risk management* adalah sebagai berikut:

   ISO/IEC 27005 dirancang sebagai panduan untuk Manajemen Risiko Keamanan Informasi dalam sebuah organisasi, khususnya untuk mendukung persyaratan ISMS (information System Managamenet Security) sesuai dengan ISO/IEC 27001 (BS ISO 27005, 2008). ISMS merupakan bagian yang terintegrasi dengan struktur organisasi dan proses manajemen secara keseluruhan, keamanan informasi terdapat pada desain proses, sistem informasi, dan kontrol (BS ISO 27001, 2005). Proses manajemen risiko keamanan informasi terdiri dari context establishment, risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and review.



   Dari alur diagram yang ada, maka kita dapat merumuskan bahwa dalam sebuah tahapan yang digunakan menggunakan acuan standar yang berlaku untuk menguji sebuah hal terkhusus penggunaan atau penerapan sebuah aplikasi pada perusahaan, sehingga hal baik yang positif maupun negative dapat teridentifikasi, sehingga kita dapat menentukan atau mencarikan solusi yang terbaik diseluruh bidang. Apalagi dengan pemantauan para karyawan yang bekerja malas. Sehingga dapat memacu kinerja karyawan. Tetapi dengan hal tersebut kita diharapkan mampu memberkan Analisa yang baik sehingga risk yang terburuk dapat teridentfikasi sehingga dapat dicarikan solusinya

3. D
4.

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)

Jawab :

1. Pada tahap evaluasi risiko, risiko yang telah teridentifikasi dievaluasi apakah risiko tersebut dapat ditoleransi atau tidak berdasarkan level of risk atau tingkatan risiko. Apabila risiko yang telah dinilai masuk kedalam kriteria yang ditetapkan maka risiko tersebut harus mendapatkan treatment (perlakuan) sebaliknya apabila risiko tidak termasuk kedalam kriteria yang ditetapkan maka perlakuan terhadap risiko tidak perlu dipertimbangkan lagi.

2. Dua tahapan awal saja dalam proses *information security risk management*

   - Analisis Resiko

   berikut Asset yang telah berhasil teridentifikasi

Asset ID	Asset Name
A1	Hardware
A2	Software
A3	Lingkungan Situs
A4	Jaringan
A5	Pegawai
A6	Organisasi

- Evaluasi Resiko (Risk Evaluation)

Evaluasi disini yaitu dengan membuat tabel yang berisi input data Asset yang terkena dampak, lalu memasukan nilai resikonya dan nilai dampak. tingkat resiko di ambil dari Threat Measure x Impact Value. Setelah itu resiko dapat di susun berdasarkan ranking dan di prioritaskan.

Asset ID	Threat ID	Threat Measure	Impact Value	Measure of Risk	Risk Ranking
A1	T1	4	4	16	7
	T2	4	3	12	9
	T3	4	3	12	9
A2	T1	6	3	18	6
	T2	4	4	16	7
	T3	5	3	15	8
A3	T1	4	2	8	11
	T2	2	4	8	11
	T3	5	4	9	11
A4	T1	4	2	8	5
	T2	5	3	15	11
	T3	5	4	20	9
A5	T1	5	3	15	8
	T2	6	3	18	3
	T3	5	3	15	9
A6	T1	3	2	6	12
	T2	3	2	6	12
	T3	3	2	6	12

UAS *IT RISK MANAGEMENT & DISASTER RECOVERY*
Dedy Syamsuar, MIT, PhD

NAMA : HASIRUL QODAR

NIM : 192420014

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengenal, 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 adalah proses menanggulangi risiko dengan:

   1. Menghindari risiko
   2. Menurunkan risiko (mitigation)
   3. Meniadakan sumber risiko
   4. Menurunkan konsekuensi dan atau kemungkinan
   5. Tetap mempertahankan risiko yang ada
   6. Berbagi (sharing) risiko dengan pihak lain

Evaluasi risiko dimaksudkan untuk membantu proses pengambilan keputusan berdasarkan hasil analisis risiko. Evaluasi risiko merupakan proses pembandingan antara level risiko yang ditemukan selama proses analisis dengan kriteria risiko yang ditetapkan sebelumnya.

Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas risiko-risiko tersebut dengan mengacu pada "kriteria risiko". Dengan kata lain hasil dari evaluasi risiko menunjukkan peringkat risiko yang memerlukan penanganan (mitigasi) lebih lanjut dengan mengacu pada tingkat risiko yang dapat diterima.

2. Risk Management penggunaan aplikasi zoom

a. Zoom merupakan aplikasi komunikasi dengan menggunakan video. Aplikasi tersebut dapat digunakan dalam berbagai perangkat seluler, desktop, hingga telepon dan sistem ruang aplikasi Zoom pada iOS juga diketahui membagikan data-data analitik milik pengguna kepada Facebook, meski sang pengguna tersebut tak memiliki akun Facebook. Zoom memberikan notifikasi kepada Facebook ketika pengguna sedang membuka aplikasi. Selain itu, data-data seperti model perangkat yang digunakan, jam, operator seluler, hingga data-data yang bisa digunakan untuk iklan juga disetorkan kepada Facebook. Zoom juga sempat mendapat protes keras saat diketahui memiliki fitur "attention tracking". Dengan fitur ini, sang "host" video konferensi dapat mengetahui siapa saja anggota yang tidak memperhatikan video konferensi tersebut. Fitur ini dapat memberikan pemberitahuan kepada host tersebut ketika salah seorang anggota membuka windows lain selama lebih dari 30 detik. Zoom juga memiliki kebijakan privasi yang kontroversial. Sebelum kemudian diubah beberapa waktu lalu, kebijakan tersebut memungkinkan Zoom untuk menyimpan segala bentuk informasi yang ada pada saat panggilan video dilakukan.
b. Aplikasi Telemedis memberikan kesempatan kepada dokter dan pasien untuk saling berinteraksi dari jarak jauh. Layanan telemedis antara dokter dan dokter telah lama berkembang dalam bentuk konsul, dan saat ini telesurgery dan teleradiologi merupakan fitur yang potensial untuk dikembangkan.

   Layanan telemedis mengundang berbagai topik yang berpotensi menjadi masalah etik, yang relevan dengan pelaksanaannya di Indonesia antara lain masalah privasi dan konfidensialitas pasien, serta berubahnya interaksi tatap muka dokter-pasien

   Peretasan keamanan konfidensialitas data pasien termasuk data teks, audio, dan visual/video adalah salah satu risiko utama sistem telemedis. Hal ini sangat perlu untuk diperhatikan, lebih-lebih bila ada data-data sensitif pasien yang akan sangat merugikan jika terpublikasi, seperti riwayat penyakit menular seksual dan gangguan jiwa. Hendaknya keamanan data yang bersifat konfidensial ini dijaga semaksimal mungkin, misalnya dengan memastikan dokter yang dikonsulkan berada di tempat yang dapat menjaga kerahasiaan (seperti dalam ruangan pribadi) bila menggunakan telepon, untuk mencegah orang yang mencuri dengar. Atau bila dilakukan dengan aplikasi chatting melalui ponsel pintar, hendaknya menggunakan aplikasi yang bereputasi baik dalam hal konfidensialitas,

Sementara itu, layanan telemedis juga menyebabkan perubahan interaksi tatap muka klasik dokter dan pasien. Secara positif, interaksi ini berarti pasien dapat menjangkau dokternya dengan lebih mudah, cepat, murah, dan sering. Pasien dapat terus mengkonsultasikan keadaan kesehataannya dengan dokter.

UAS Kelas AR2

Nama : Hendri Donan, ST

(Asal Institusi STIKes Muhammadiyah Palembang, Operator PDDIKTI))

NIM : 192420039

Program Studi Magister Teknik Informatika

Mata Kuliah : IT RISK MANAGEMENT & DISASTER RECOVERY

Dosen MK : Dedy Syamsuar, MIT, PhD

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!

Jawab

Sejumlah pilihan penanganan dapat dipertimbangkan dan diterapkan baik secara individual atau dalam kombinasi. Organisasi biasanya bisa mendapatkan keuntungan dari penerapan kombinasi pilihan penanganan tersebut. Ketika memilih opsi penanganan risiko, organisasi harus mempertimbangkan nilai-nilai dan persepsi pemangku kepentingan dan cara yang paling tepat untuk berkomunikasi dengan mereka. Dimana pilihan penanganan risiko dapat berdampak pada risiko di tempat lain dalam organisasi atau dengan para pemangku kepentingan, harus dilibatkan dalam keputusan. Meskipun sama-sama efektif, beberapa penanganan risiko dapat lebih diterima oleh beberapa stakeholder daripada yang lainnya.

Rencana penanganan risiko harus secara jelas mengidentifikasi urutan prioritas di mana penanganan risiko individu harus diimplementasikan. Perlakuan resiko itu sendiri dapat menimbulkan risiko. Sebuah risiko yang signifikan dapat menjadi kegagalan atau ketidakefektifan tindakan penanganan risiko. Pemantauan perlu menjadi bagian integral dari rencana penanganan risiko untuk memberikan jaminan bahwa langkah-langkah penanganan tetap efektif.

Penanggung jawab dari penanganan risiko terbagi menurut masing-masing level risikonya, yaitu:

a. Risiko dengan potensi level “risiko tinggi”: Ketua Manajemen Risiko dan Pemilik Risiko

b. Risiko dengan potensi level “risiko sedang”: Pemilik Risiko

c. Risiko dengan potensi level “risiko tinggi”: Koordinator Manajemen pada masing-masing UPR dibawah pemantauan pemilik risiko

Hasil atau output dari tahapan penanganan risiko adalah Laporan Penanganan Risiko yang mencakup:
a. Hasil identifikasi berbagai opsi penanganan risiko
b. Penilaian atas opsi-opsi tersebut; dan
c. Rencana penanganan, persiapan serta implementasinya

contoh sebagian risiko dan pengelolaannya oleh Adira Finance:

Risk	Event	Action	Risk Treatment
1. Risiko Kredit	Konsumen tidak mampu memenuhi kewajiban dalam meluasi kredit	Reduce	1. Penerimaan Aplikasi Kredit yang selektif 2. Penerapan Prinsip Mengenal Nasabah pada Lembaga Keuangan Non Bank 3. Analisis Portofolio dan sistem manajemen Informasi 4. Pendelegasian wewenang persetujuan kredit
2. Risiko Operasional	1. Tidak berfungsinya proses internal 2. Kegagalan sistem 3. Kesalahan manusia	Reduce	1. Pelaksanaan risk control self assessment 2. Pengelolaan 3. kecuranganTinjauan terhadap kebijakan dan SOP secara ruti 4. Menetapkan Pedoman pengelolaa kelangsungan usaha
3. Risiko Pasar	Kenaikan tingkat bunga kredit	Mitigasi	Penerapan pengelolaan tingkat bunga tetap secara konsisten dengan menyesuaikan tingkat bunga kredit terhadap tingkat bunga pinjaman dan beban dana
5. Risiko Hukum	Adanya tuntutan hukum	Mitigasi	Membuat divisi hukum untuk melakukan pengelolaan risiko hukum

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)

JAWAB

Ditengah maraknya wabah virus Covid-19 di seluruh dunia, Indonesia juga terkena dampak yang sangat berarti bagi setiap elemen masyarakat. Wabah yang tak kunjung usai ini mempengaruhi tindakan ekonomi masyarakat baik kalangan kecil, menengah sampai dengan atas. Terbukti dengan adanya kebijakan *social distancing* dan *work from home* atau bekerja dari rumah yang diberlakukan oleh pemerintah, hampir seluruh industri mengalami penurunan omset bahkan harus memutar balik seluruh aktivitas bisnis mereka. Berbagai perusahaan, universitas, sekolah telah meminta karyawan serta muridnya untuk melakukan aktivitas di dalam rumah masing-masing. Dalam budaya bisnis di Indonesia, kegiatan bekerja dari rumah s angat asing untuk dilakukan. Banyak pula yang masih belum mengetahui cara bekerja yang benar bahkan masih sangsi atau ragu apakah kegiatan bekerja dari rumah ini efektif bagi bisnisnya

Aktifitas kerja karyawan secara teknologi terdapat "*Employee Monitoring Software*" yang dapat mengotrol aktivitas karyawan di rumah pada saat WFH

Sofware yang sering dipakai pada saat WFH

1. Zoom

   Software WFH pertama yang sekarang sedang naik daun adalah Zoom. Aplikasi satu ini digunakan untuk melakukan *meeting online.* Zoom sendiri bisa memuat 100 partisipan dalam satu *online meeting.* Aplikasi ini pun sekarang ini tidak hanya digunakan oleh perusahaan saja lho. Bahkan, banyak guru dan dosen di sekolah dan universitas di berbagai kota di Indonesia menggunakan Zoom untuk melakukan pembelajaran daring. Tidak hanya melakukan *online meeting,* kamu pun bisa berbagi layar untuk menampilkan hasil kerjamu, melakukan *chatting* dengan lawan bicara, serta mengirimkan *file* saat melakukan *online meeting.* Walaupun sedang sangat populer dan mudah digunakan, salah satu kekurangan yang dimiliki oleh Zoom adalah adanya batasan 40 menit bagi pengguna aplikasi gratisnya. Jika ingin waktu yang tak terbatas, ada paket yang bisa kamu beli.

2. Absensi online

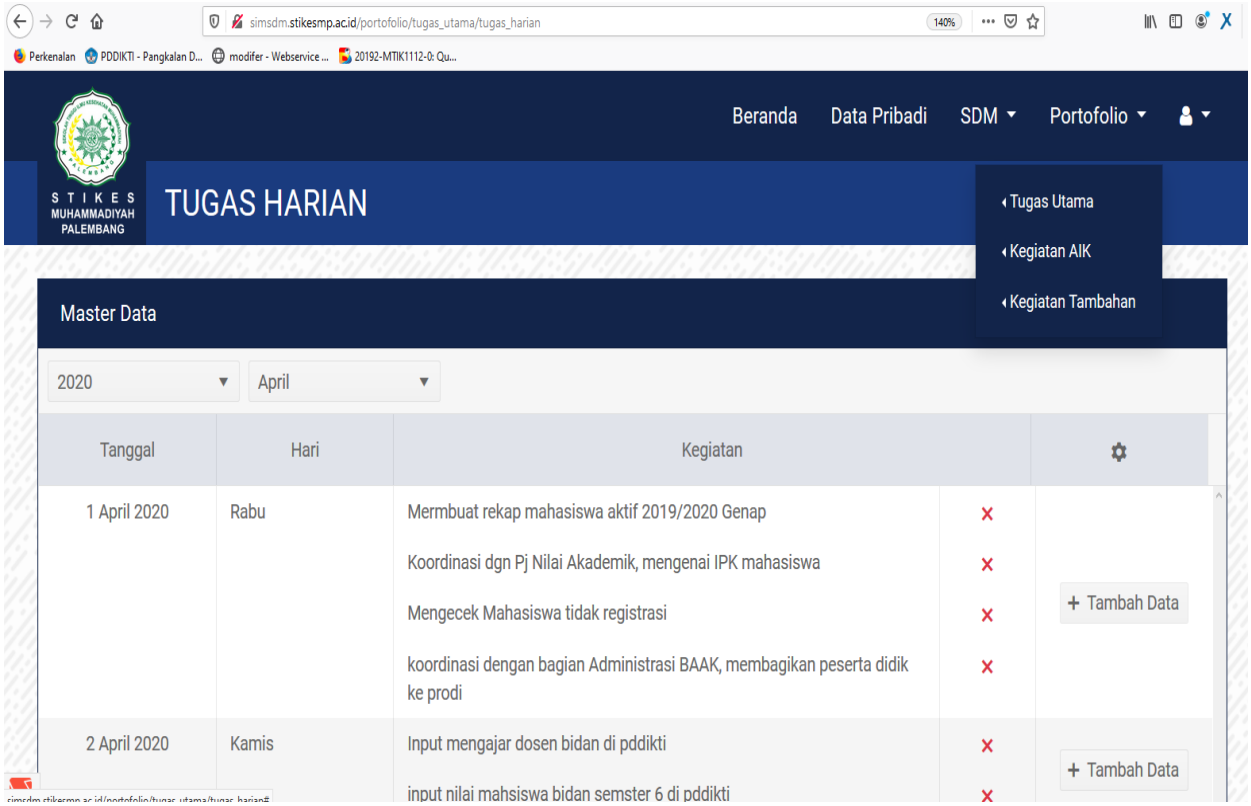
Contoh great data atau

Beberapa permasalah resiko yang akan terjadi

Risk	Event
1. Resiko Operasional	1. Butuh Pelatihan atau penyuluhan tentang sistem dipakai 2. Internet yang tidak stabil atau kouta terbatas pada saat zoom meting 3. Sering terlambatnya pada waktu absensi 4. Kecurangan terhadap absensi
2. Resiko software	1. Hacker 2. Apabila menggunakan software baru biasanya akan butuh pengembangan lebih lanjut 3. Masalah keamanan data pribadi

Contoh SIMTEM KEPEGAWAIAN STIKES MUHAMAMDIYAH PALEMBANG

Alur : Setiap Ka.bagian atau Ka. unit berkoordinasi dengan staft bisa melalui Whasthap, zoom meting. Ka.bagian atau Ka. Unit membuat lembar kerja perbulan mengenai target kerja yang dicapai. Kemudian disampaikan ke staft masing masing untuk dikerjakan sesuai dengan job desk dan jam kerja yang ditentukan. Sistem kepegawaian harus diisi perhari dibagian Tugas harian, sehingga kinerja terpantau dan akan dicek Ka.bagian atau Ka. Unit tiap 2 minggu. Sistem informasi ini juga sebagai portofolio kinerja perhitungan pembagian Insentif SHU (Sisa Hasil Usaha) yang akan dibagian tiap akhir Tahun Akademik.



Nama	:	Hermizahadiwidastra
NIM	:	192420035
Jurusan/Kelas	:	MTI 21 / AR2
Mata Kuliah	:	IT RISK MANAGEMENT & DISASTER RECOVERY (MTIK232)
Dosen	:	Dedy Syamsuar, M.I.T.,Ph.D.
UAS	:	Topik 12

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.

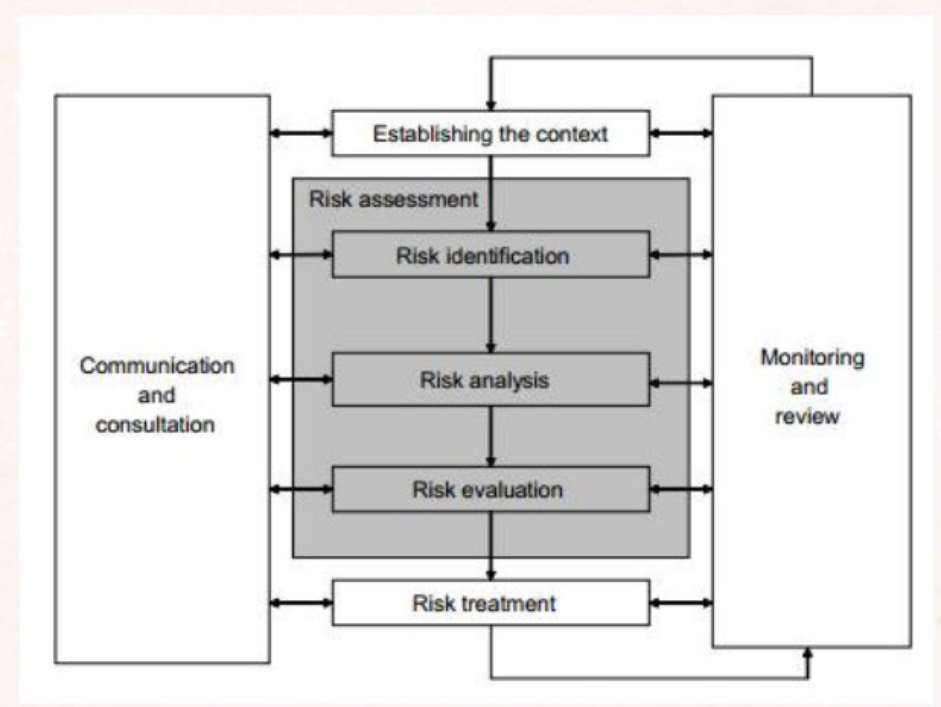
Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information security risk management* untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu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

---- Selamat Bekerja ----

Jawaban:

1. Kita tidak pernah akan tahu apa yang akan terjadi pada perusahaan kita khususnya dalam penggunaan Information Technology. Perlu suatu Analisa yang baik dan matang di dalam menghadapi hal-hal yang tidak diinginkan, dengan antisipasi Analisa yang baik dan akurat. Serta jalur koordinasi dalam tahapan penanganannya. Risk Assessment merupakan proses keseluruhan dari Risk Idnetification, Risk Analsis, Dan Risk Evaluation. Risk Treatment dan Risk Evaluation merupakan bagian analisa Risk dalam Risk Management. Risk evaluation merupakan sebuah pernyataan untuk membandingkan tingkat dari resiko yang diestimasi dengan kriteria resiko yang telah ditetapkan pada saat context ditentukan. Hal ini dilakukan untuk menentukan seberapa pengaruh resiko tersebut terhadap organisasi dan untuk menentukan tipe dari resiko tersebut. Setelah melakukan sebuah Risk Assessment, Risk Treatment merupakan porses untuk memilih dan menyetujui satu atau lebih opsi untuk mengubah probabilitas terjadinya resiko tersebut. Seperti yang telah dijelaskan pada ISO 31000, resiko dibagi menjadi resiko positif dan resiko negatif. Dengan adanya Risk Treatment, diharapkan terdapat langkah-langkah yang tepat yang dapat dilakukan organisasi untuk mengurangi resiko negatif dan mengoptimalkan resiko positif.

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.



Contoh Risk Treatment pada Adira Finance

Berikut ini merupakan contoh sebagian risiko dan pengelolaannya oleh Adira Finance: Risk Event Action Risk Treatment

A. Risiko Kredit Konsumen tidak Reduce.

1) Penerimaan mampu memenuhi Aplikasi Kredit kewajiban dalam yang selektif melunasi kredit.
2) Penerapan Prinsip Mengenal Nasabah pada Lembaga Keuangan Non Bank.
3) Analisis Portofolio dan sistem manajemen informasi.
4) Pendelegasian wewenang persetujuan kredit.

B. Pelaksanaan Risk Operasional berfungsinya control self proses internal assessment.

1) Kegagalan sistem.
2) Pengelolaan kecurangan.
3) Kesalahan manusia.

C. Tinjauan terhadap kebijakan dan SOP secara rutin.

1) Menetapkan Pedoman pengelolaan kelangsungan usaha.
2) Risiko Pasar Kenaikan tingkat Mitigasi Penerapan bunga kredit pengelolaan tingkat bunga tetap secarakonsisten dengan menyesuaikan tingkat bunga kredit terhadap tingkat bunga pinjaman dan beban dana.

3) Risiko Tidak mematuhi atau Mitigasi Membuat divisi Kepatuhan melaksanakan peraturan sekretaris perusahaan untuk perundang-undangan melakukan dan peraturan lain pengawasan yang berlaku.
4) Risiko Hukum Adanya tuntutan Mitigasi Membuat divisi hukum hukum untuk melakukan pengelolaan risiko hukum.
5) Risiko Reputasi Adanya publikasi Mitigasi Membentuk tim dan Risiko negatif khusus untuk strategis mendukung penanganan kasus Risiko yang dikelola adalah berdasarkan pada selera risiko Adira Finance. Pada tahap ini Adira Finance mengelola risiko dengan mempertimbangkan dampak, frekuensi, biaya dan manfaat.

2. Dalam masa wabah pandemi saat ini, pekerjaan lebih banyak dialihkan dari kantor kerumah dengan program yang disebut Work From Home. Hal ini tentunya akan membawa sebuah perubahan dalam sebuah system kerja. Banyak perusahaan telah menggunakan suatu system dibidang information technology didalam membantu proses pemantauan para karyawan yang bekerja WFH. Berbagai software telah dikembangkan, sehingga kita sebagai seorang managerial dibidang IT dituntut untuk menganalisa sebuah aplikasi dalam penggunaannya di perusahaan.

Berdasarkan ISO 27005-2008 terhadap proses information security risk management adalah sebagai berikut:

ISO/IEC 27005 dirancang sebagai panduan untuk Manajemen Risiko Keamanan Informasi dalam sebuah organisasi, khususnya untuk mendukung persyaratan ISMS (information System Managamenet Security) sesuai dengan ISO/IEC 27001 (BS ISO 27005, 2008). ISMS merupakan bagian yang terintegrasi dengan struktur organisasi dan proses manajemen secara keseluruhan, keamanan informasi terdapat pada desain proses, sistem informasi, dan kontrol (BS ISO 27001, 2005). Proses manajemen risiko keamanan informasi terdiri dari Context Establishment, Risk Assessment, Risk Treatment, Risk Acceptance, Risk Communication, Risk Monitoring and Review.

UAS IT Risk Management
Nama : Istiana Ruswita
Nim : 192420032

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!

Jawaban :

Strategi risk treatment/ penanganan risiko dalam bidang IT dapat berdampak pada risiko di bidang lain dalam suatu organisasi/perusahaan. Jadi ketika menyusun strategi risk treatment / penanganan risiko, organisasi harus mempertimbangkan nilai-nilai dan persepsi pemangku kepentingan yang diperoleh dari langkah melakukan identifikasi resiko dan hasil evaluasi resiko yang sebelumnya telah dilakukan. Hal ini mendukung **agar rencana penanganan risiko dapat secara jelas mengidentifikasi urutan prioritas di mana penanganan risiko harus diimplementasikan, agar penanganan risiko itu sendiri tidak menimbulkan risiko pada bidang lainnya.**

Contoh :

Dalam suatu perusahaan yang menggunakan sebuah sistem logistik dan digunakan oleh beberapa user untuk meminta barang dan authorisasi permintaan.

Risiko :

Penyalahgunaan account pada sistem logistik.

Evaluasi Risiko :

Merugikan perusahaan secara administratif dan finansial.
Risiko terbesar pada penyalahgunaan account untuk authorisasi.

Risk Treatment :

Menambah fitur scan sidik jari ketika login.

Beberapa user kerap kali tidak merahasiakan passwordnya sehingga user lain dapat melakukan login menggunakan account tersebut.

Risk treatment yang dapat diusulkan kepada pihak manajemen adalah dengan memberlakukan scan sidik jari pada saat login. **Namun setelah dilakukan evaluasi risiko, perusahaan hanya perlu memberlakukan scan sidik jari tersebut untuk account yang dapat melakukan autorisasi karena dinilai lebih prioritas dan dapat menekan risiko kerugian yang lebih besar.**

Pertanyaan :

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 :
   Proses *information security risk management* untuk teknologi menurut ISO 27005-2008 :

   1. Tahap 1 Penetapan Konteks :
   Penggunaan aplikasi anydesk untuk mengakses sistem informasi logistik.
   Pertimbangan umum : sofware ini mudah untuk diaplikasikan
   Kriteria dasar : free software
   Ruang lingkup dan batasan : hanya untuk input data, tidak untuk autorisasi

   2. Tahap 2 Penilaian Risiko :
   Kemungkinan dari ancaman : Ancaman hampir tidak pernah terjadi
   Dampak terjadinya risiko : Dampak gangguan kecil pada layanan sistem logistik bukan pada program utama. Toleransi penyelesaian masalah 1-2 jam.

UAS

IT RISK MANAGEMENT & DISASTER RECOVERY

Dedy Syamsuar, MIT, PhD

KELAS MTI AR 21

NAMA : ISTIKOMAH

NIM : 192420003

Pertanyaan:

1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengenal, 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 adalah proses menanggulangi risiko dengan:

   1. Menghindari risiko
   2. Menurunkan risiko (mitigation)
   3. Meniadakan sumber risiko
   4. Menurunkan konsekuensi dan atau kemungkinan
   5. Tetap mempertahankan risiko yang ada
   6. Berbagi (sharing) risiko dengan pihak lain

Evaluasi risiko dimaksudkan untuk membantu proses pengambilan keputusan berdasarkan hasil analisis risiko. Evaluasi risiko merupakan proses pembandingan antara level risiko yang ditemukan selama proses analisis dengan kriteria risiko yang ditetapkan sebelumnya.

Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas risiko-risiko tersebut dengan mengacu pada “kriteria risiko”. Dengan kata lain hasil dari evaluasi risiko menunjukkan peringkat risiko yang memerlukan penanganan (mitigasi) lebih lanjut dengan mengacu pada tingkat risiko yang dapat diterima.

2. Risk Management penggunaan aplikasi zoom

a. Zoom merupakan aplikasi komunikasi dengan menggunakan video. Aplikasi tersebut dapat digunakan dalam berbagai perangkat seluler, desktop, hingga telepon dan sistem ruang aplikasi Zoom pada iOS juga diketahui membagikan data-data analitik milik pengguna kepada Facebook, meski sang pengguna tersebut tak memiliki akun Facebook. Zoom memberikan notifikasi kepada Facebook ketika pengguna sedang membuka aplikasi. Selain itu, data-data seperti model perangkat yang digunakan, jam, operator seluler, hingga data-data yang bisa digunakan untuk iklan juga disetorkan kepada Facebook. Zoom juga sempat mendapat protes keras saat diketahui memiliki fitur "attention tracking". Dengan fitur ini, sang "host" video konferensi dapat mengetahui siapa saja anggota yang tidak memperhatikan video konferensi tersebut. Fitur ini dapat memberikan pemberitahuan kepada host tersebut ketika salah seorang anggota membuka windows lain selama lebih dari 30 detik. Zoom juga memiliki kebijakan privasi yang kontroversial. Sebelum kemudian diubah beberapa waktu lalu, kebijakan tersebut memungkinkan Zoom untuk menyimpan segala bentuk informasi yang ada pada saat panggilan video dilakukan.
b. Aplikasi Telemedis memberikan kesempatan kepada dokter dan pasien untuk saling berinteraksi dari jarak jauh. Layanan telemedis antara dokter dan dokter telah lama berkembang dalam bentuk konsul, dan saat ini telesurgery dan teleradiologi merupakan fitur yang potensial untuk dikembangkan.

   Layanan telemedis mengundang berbagai topik yang berpotensi menjadi masalah etik, yang relevan dengan pelaksanaannya di Indonesia antara lain masalah privasi dan konfidensialitas pasien, serta berubahnya interaksi tatap muka dokter-pasien

   Peretasan keamanan konfidensialitas data pasien termasuk data teks, audio, dan visual/video adalah salah satu risiko utama sistem telemedis. Hal ini sangat perlu untuk diperhatikan, lebih-lebih bila ada data-data sensitif pasien yang akan sangat merugikan jika terpublikasi, seperti riwayat penyakit menular seksual dan gangguan jiwa. Hendaknya keamanan data yang bersifat konfidensial ini dijaga semaksimal mungkin, misalnya

dengan memastikan dokter yang dikonsulkan berada di tempat yang dapat menjaga kerahasiaan (seperti dalam ruangan pribadi) bila menggunakan telepon, untuk mencegah orang yang mencuri dengar. Atau bila dilakukan dengan aplikasi chatting melalui ponsel pintar, hendaknya menggunakan aplikasi yang bereputasi baik dalam hal konfidensialitas, Sementara itu, layanan telemedis juga menyebabkan perubahan interaksi tatap muka klasik dokter dan pasien. Secara positif, interaksi ini berarti pasien dapat menjangkau dokternya dengan lebih mudah, cepat, murah, dan sering. Pasien dapat terus mengkonsultasikan keadaan kesehataannya dengan dokter.

Nama : Istiqomah Febrianty
NIM : 192420042
Kelas : MTI R2

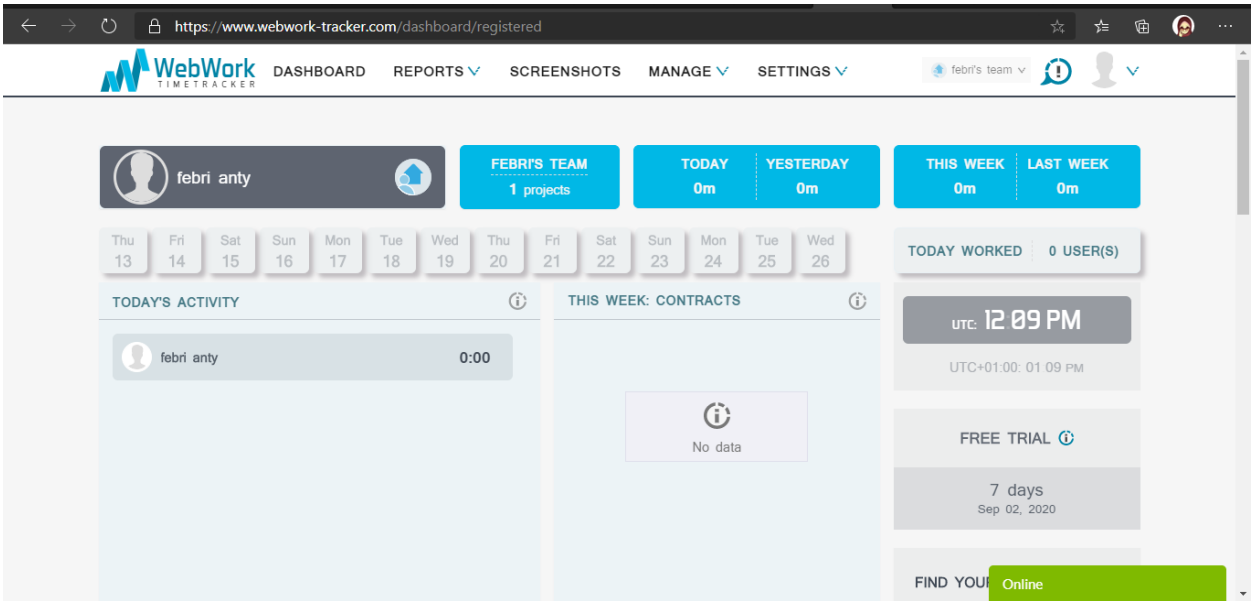
1. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!
   Jawaban:
   Manajemen risiko pada dasarnya dilakukan melalui proses-proses:
   1. Identifikasi risiko. Banyak risiko yang dihadapi oleh suatu organisasi, mulai dari risiko penyelewengan oleh karyawan, risiko kejatuhan meteor atau komet, dan lainnya. Ada beberapa teknik untuk mengidentifikasi risiko, misal dengan menelusuri sumber risiko sampai terjadinya peristiwa yang tidak diinginkan. Sebagai contoh, bank menghadapi risiko terutama adalah risiko kredit (kemungkinan debitur tidak melunasi hutangnya). Untuk bank yang juga aktif melakukan perdagangan sekuritas, maka bank tersebut akan menghadapi risiko pasar. Setiap bisnis akan menghadapi risiko yang berbeda-beda karakteristiknya.
   2. Evaluasi dan Pengukuran Risiko. Tujuan evaluasi risiko adalah untuk memahami karakteristik risiko dengan lebih baik. Jika kita memperoleh pemahaman yang lebih baik, maka risiko akan lebih mudah dikendalikan. Evaluasi yang lebih sistematis dilakukan untuk 'mengukur' risiko tersebut. Sebagai contoh, risiko perubahan tingkat bunga bisa diukur dengan teknik duration (durasi). Modul identifikasi dan pengukuran risiko spekulatif akan banyak membicarakan pengukuran risiko perubahan tingkat bunga. Teknik lain untuk mengukur risiko adalah dengan mengevaluasi dampak risiko tersebut terhadap kinerja perusahaan.
   3. Pengelolaan risiko. Risiko harus dikelola. Jika organisasi gagal mengelola risiko, maka konsekuensi yang diterima bisa cukup serius, misal kerugian yang besar. Risiko bisa dikelola dengan berbagai cara, seperti penghindaran, ditahan (retention), diversifikasi, atau ditransfer ke pihak lainnya. Erat kaitannya dengan manajemen risiko adalah pengendalian risiko (risk control), dan pendanaan risiko (risk financing).
   Manajemen risiko bertujuan untuk mengelola risiko. Kegagalan mengelola risiko bisa mengakibatkan konsekuensi yang serius terhadap organisasi. Proses manajemen risiko mencakup identifikasi risiko, evaluasi dan pengukuran risiko, dan pengelolaan risiko. Kegiatan tersebut pada dasarnya bertujuan mempelajari karakteristik risiko dengan baik sehingga kita bisa mengelola risiko dengan baik. Di samping itu, manajemen risiko juga memerlukan infrastruktur pendukungnya, baik keras maupun lunak.

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.

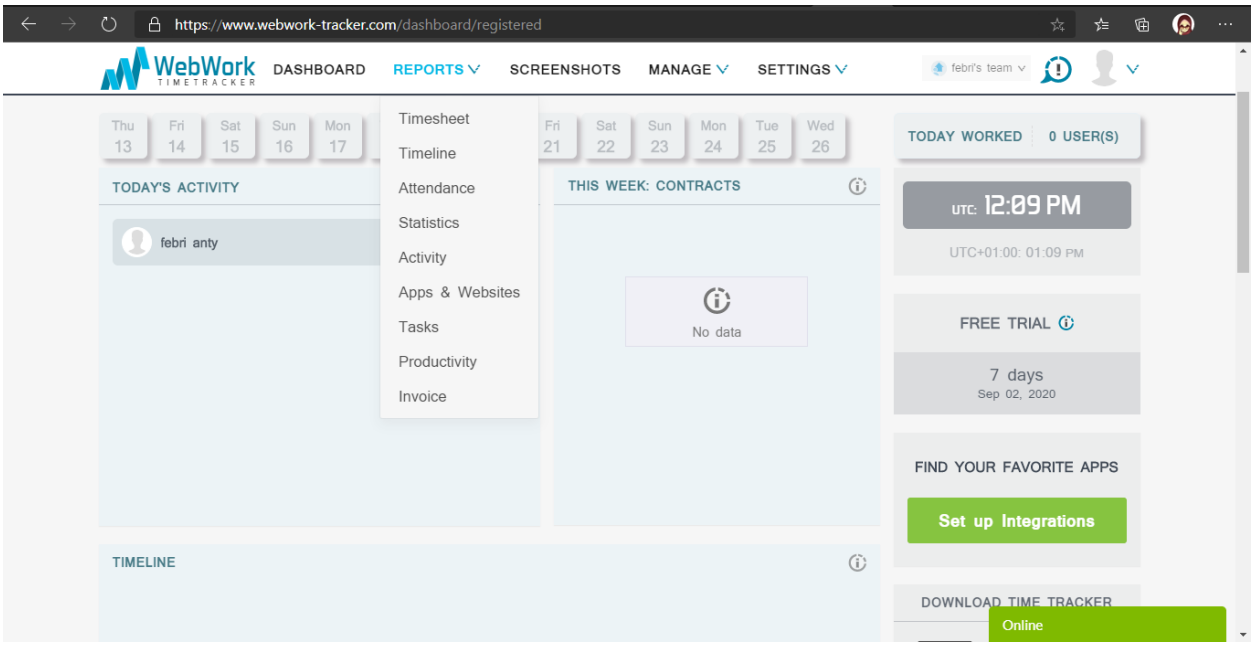
   Sebagai seorang manager IT anda diminta pertimbangan berupa *risk management* dari penggunaan Software ini. Silahkan lakukan dua tahapan awal saja dalam proses *information*

security risk management untuk teknologi ini menurut ISO 27005-2008! (Anda dapat menggunakan contoh software/teknologi untuk membantu menjelaskan jawaban anda)

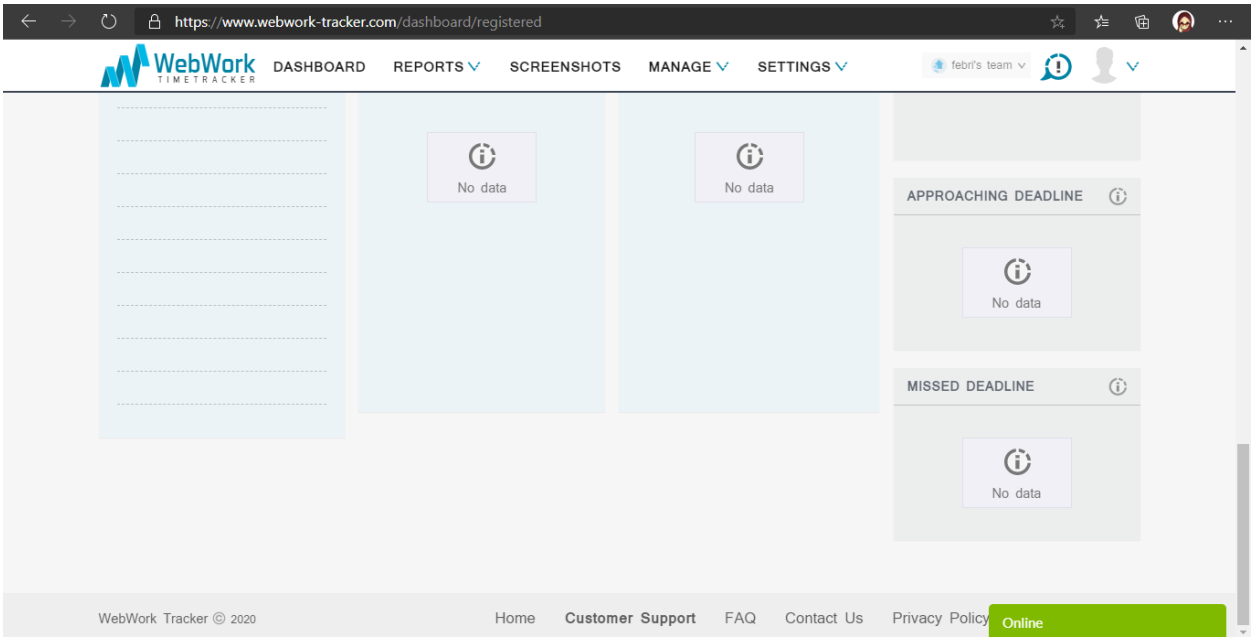
Jawaban:



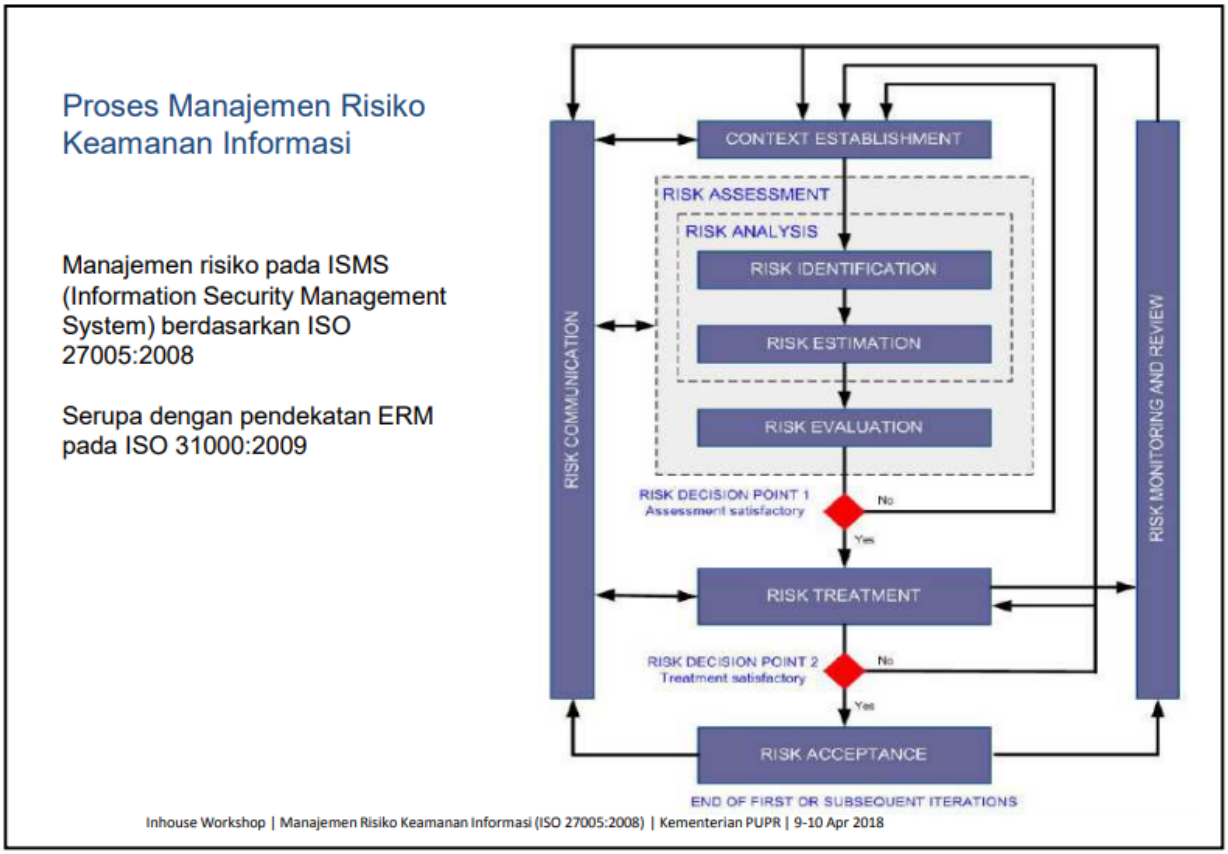
Berikut adalah contoh software aplikasi GRATIS uji coba dari https://www.webwork-tracker.com/dashboard/registered



Pada menu report terdapat banyak hasil laporan dari setiap jobdesk yang telah dikerjakan oleh pegawai pada suatu perusahaan.



Sidebar disebelah kanan memberikan peringatan pekerjaan mana yang harus didahulukan untuk disetujui maupun pekerjaan apa saja yang telah terlewatkan.



1) Penetapan konteks manajemen risiko keamanan informasi: pada tahap ini dilakukan penggambaran konteks manajemen risiko keamanan informasi untuk *Employee Monitoring Software* yang meliputi: pertimbangan umum, kriteria dasar, ruang lingkup dan batasan, organisasi manajemen keamanan informasi.

2) Penilaian risiko keamanan informasi: Secara umum proses ini meliputi: identifikasi risiko, analisis risiko dan evaluasi risiko. Identifikasi risiko diuraikan lagi menjadi beberapa proses yaitu identifikasi aset, ancaman, identifikasi kerentanan, identifikasi dampak terjadinya ancaman atau ancaman. Proses analisis risiko meliputi penentuan kategori dampak risiko yang mungkin terjadi berdasar pada ancaman yang ada, penentuan kemungkinan terjadinya ancaman (likelyhood), serta menentukan level risiko yang mungkin terjadi dari setiap ancaman terhadap aset yang ada. Untuk membuat kategori dampak risiko dan kemungkinan terjadinya ancaman dapat dilakukan berdasar dari keputusan pihak pengelola sesuai dengan hasil analisis. Jadi pengkategorian ini tidak bersifat baku untuk setiap organisasi atau instansi.

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. Tujuan dari manajemen risiko adalah minimalisasi kerugian dan meningkatkan kesempatan ataupun peluang. Bila dilihat terjadinya kerugian dengan teori accident model dari ILCI, maka manajemen risiko dapat memotong mata rantai kejadian kerugian tersebut, sehingga efek dominonya tidak akan terjadi. Pada dasarnya manajemen risiko bersifat pencegahan terhadap terjadinya kerugian maupun 'accident'

Kebijakan Manajemen Risiko Kebijakan manjemen risiko harus relevan dengan konteks strategi dan tujuan organisasi, objektif dan sesuai dengan sifat dasar bisnis (organisasi) tersebut. Manejemen akan memastikan bahwa kebijakan tersebut dapat dimengerti, dapat diimplementasikan di setiap tingkatan organisasi.

A. Perencanaan Dan Pengelolaan Hasil

1. Komitmen Manajemen. Organisasi harus dapat memastikan bahwa:
   a. Sistem manejemen risiko telah dapat dilaksanakan, dan telah sesuai dengan standar
   b. Hasil/ performa dari sistem manajemen risiko dilaporkan ke manajemen organisasi, agar dapat digunakan dalam meninjau (review) dan sebagai dasar (acuan) dalam pengambilan keputusan.
2. Tanggung jawab dan kewenangan Tanggung jawab, kekuasaan dan hubungan antar anggota yang dapat menunjukkan dan membedakan fungsi kerja didalam manajemen risiko harus terdokumentasikan khususnya untuk hal-hal sebagai berikut:
   a. Tindakan pencegahan atau pengurangan efek dari risiko.
   b. Pengendalian yang akan dilakukan agar faktor risiko tetap pada batas yang masih dapat diterima.
   c. Pencatatan faktor-faktor yang berhubungan dengan kegiatan manajemen risiko.
   d. Rekomendasi solusi sesuai cara yang telah ditentukan.
   e. Memeriksa validitas implementasi solusi yang ada.
   f. Komunikasi dan konsultasi secara internal dan eksternal.

3. Sumber Organisasi harus dapat mengidentifikasikan persyaratan kompetensi sumber daya manusia (SDM) yang diperlukan. Oleh karena itu untuk meningkatkan kualifikasi SDM perlu untuk mengikuti pelatihan-pelatihan yang relevan dengan pekerjaannya seperti pelatihan manajerial, dan lain sebagainya.

B. Elemen Utama Manjemen Riseko Elemen utama dari proses manajemen risiko, meliputi:

a. Penetapan tujuan Menetapkan strategi, kebijakan organisasi dan ruang lingkup manajemen risiko yang akan dilakukan.
b. Identifkasi risiko Mengidentifikasi apa, mengapa dan bagaimana faktor-faktor yang mempengaruhi terjadinya risiko untuk analisis lebih lanjut.

c. Analisis risiko Dilakukan dengan menentukan tingkatan probabilitas dan konsekuensi yang akan terjadi. Kemudian ditentukan tingkatan risiko yang ada dengan mengalikan kedua variabel tersebut (probabilitas X konsekuensi).
d. Evaluasi risiko Membandingkan tingkat risiko yang ada dengan kriteria standar. Setelah itu tingkatan risiko yang ada untuk beberapa hazards dibuat tingkatan prioritas manajemennya. Jika tingkat risiko ditetapkan rendah, maka risiko tersebut masuk ke dalam kategori yang dapat diterima dan mungkin hanya memerlukan pemantauan saja tanpa harus melakukan pengendalian.
e. Pengendalian risiko Melakukan penurunan derajat probabilitas dan konsekuensi yang ada dengan menggunakan berbagai alternatif metode, bisa dengan transfer risiko, dan lain-lain.
f. Monitor dan Review Monitor dan review terhadap hasil sistem manajemen risiko yang dilakukan serta mengidentifikasi perubahan-perubahan yang perlu dilakukan.
g. Komunikasi dan konsultasi Komunikasi dan konsultasi dengan pengambil keputusan internal dan eksternal untuk tindak lanjut dari hasil manajemen risiko yang dilakukan.

2. Di tengah meluasnya penyebaran virus *Corona* (Covid-19) mengakibatkan banyak perusahaan besar maupun kecil di seluruh dunia memulai skema kerja dari rumah (*Work from Home*/WFH) untuk para karyawannya.

Skema *Work from Home* ini mungkin merupakan hal yang baru dan di luar dari kebiasaan perusahaan sebelumnya, terutama bagaimana perusahaan dapat menerima hasil yang maksimal.

GreatDay HR sebagai pionir *mobile HR application* siap menanggapi kebutuhan darurat perusahaan yang harus mengubah pola kerja karyawannya ke skema WFH. Yakni mulai dari pengaturan kehadiran, jadwal kerja, hingga pengajuan klaim dan *reimbursement*, semuanya bisa dilakukan langsung melalui aplikasi ponsel GreatDay HR.

Berikut beberapa hal yang perlu diperhatikan dalam menjalankan *Work from Home* untuk memastikan karyawan yang bekerja dari rumah tetap produktif.

Sistem Komunikasi

Komunikasi merupakan kunci utama dalam melakukan kerja jarak jauh. Bagaimana komunikasi antara atasan dan bawahan bisa dilakukan dengan mudah dan jelas. Ketika salah satu pihak tidak dapat dijangkau hal ini menjadi tantangan tersendiri. Oleh sebab itu, perusahaan memerlukan suatu media yang jelas untuk menjamin komunikasi antarkaryawan tetap dapat dilakukan secara teratur.

GreatDay HR memiliki fitur percakapan atau *chatting* internal yang terdapat di aplikasi. Fitur obrolan ini sangat berguna untuk memaksimalkan komunikasi antarkaryawan tanpa tatap

muka. Selain mempermudah jalur komunikasi, antarkaryawan juga bisa berbagi dokumen dengan format yang beragam.

GreatDay HR berdedikasi untuk selalu memaksimalkan keterkaitan karyawan, salah satunya adalah dengan media sosial internal milik setiap karyawan pengguna. Tampilan lini masa atau *timeline* GreatDay HR juga dibuat secara kronologis, semua pengguna dapat dengan mudah melihat siapa saja yang sudah melakukan absensi, *update* atau kabar terbaru yang bisa diunggah oleh masing-masing karyawan.

Tentu saja dalam masa *social distancing* ini, fitur sosial media internal GreatDay akan sangat membantu untuk tetap membangun komunikasi dan mengetahui kabar terbaru yang dibagikan perusahaan khusus untuk para karyawannya.

Rekam Kehadiran

Salah satu kekhawatiran memulai sistem kerja dari rumah adalah, sulitnya memastikan karyawan benar-benar bekerja dan mengatur sistem absensi. Tidak sedikit perusahaan yang masih mengandalkan sistem manual *fingerprint* untuk merekam kehadiran, berujung mengharuskan karyawannya untuk tetap masuk kerja karena tidak punya pilihan lain untuk mengatasi hal ini.

Dengan teknologi GreatDay HR, semua pengguna aplikasi dapat merekam data kehadiran mereka dengan mudah melalui aplikasi seluler. GreatDay HR dilengkapi dengan teknologi pemindai wajah dan penanda lokasi, kedua hal ini sangat penting untuk memastikan keaslian data karyawan yang bisa langsung diintegrasikan dengan sistem penggajian.

Tidak berakhir di pencatatan kehadiran, setiap karyawan juga bisa langsung mengkoreksi data kehadiran mereka langsung dari aplikasi GreatDay HR, hal ini termasuk dengan pengajuan cuti dan lembur.

Menetapkan Target

Bekerja dari rumah tentunya akan terasa lebih santai dan dinamis sehingga akan cenderung sulit untuk memonitor apa yang sedang dilakukan karyawan. Memastikan apa yang perlu dikerjakan dan diselesaikan oleh karyawan dalam jangka waktu tertentu menjadi satu cara untuk mengukur produktivitas karyawan. Masing-masing karyawan dapat menetapkan target mereka masing-masing dan membagikannya melalui media yang disiapkan perusahaan.

Media sosial internal dari GreatDay HR juga menyediakan ruang untuk para atasan memberi tugas kepada karyawan, para karyawan yang mendapatkan tugas otomatis akan menerima notifikasi di ponsel mereka masing-masing.

Manajemen juga dapat dengan mudah melacak kinerja karyawannya dengan fitur rekam aktivitas. Fitur rekam aktivitas bisa dilakukan oleh karyawan yang didelegasikan tugas, dan seterusnya bisa diberikan umpan balik oleh penyelenggara tugas.

Suasana Kerja

Membuat suasana kerja yang nyaman di tengah banyaknya isu negatif mengenai penyebaran virus *Corona* menjadi tantangan tersendiri. Saling berbagi bagaimana kondisi kerja masing-masing bisa membuat karyawan tetap fokus untuk menyelesaikan pekerjaannya. Mengetahui kegiatan rekan tim yang sedang berjauhan menjadi salah satu alternatif dalam berkomunikasi, GreatDay HR paham betul urgensi untuk mengandalkan teknologi dalam memaksimalkan skema *Working from Home.*

Media sosial yang dibangun oleh GreatDay HR bisa menjadi pilihan tepat perusahaan untuk bisa tetap menghidupkan semangat kerja secara virtual, semua karyawan bisa dengan mudah mengunggah kabar terbaru, pencapaian, dan *update* lainnya untuk mendapatkan “likes” dari sesama karyawan pengguna GreatDay HR.

Nama : M. Danial Sentosa

Nim : 192420040

Magister Teknik Informatika Kelas A R2

Universitas Binadarma

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 sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya karna Risk treatment bertujuan untuk menentukan tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara keseluruhan. Terdapat beberapa risk treatment yang umumnya digunakan, yaitu; risk prevention (pencegahan risiko) dengan tujuan untuk mengurangi secara substansial kemungkinan terjadinya risiko, risk mitigation (mitigasi risiko) dengan tujuan untuk meminimalkan konsekuansi dari risiko, risk sharing (berbagi risiko) dengan tujuan untuk memindahkan risiko tidak hanya ke organisasi lain namun juga ke entitas bisnis ataupin individu, dan risk retention (retensi risiko) atau dikenal juga sebagai penyerapan, toleransi, atau penerimaan risiko.

Contoh sederhananya, data penting perusahaan sangat rentan di retas oleh seseorang. Dari hasil evaluasi resiko yang telah dilakukan terdapat terdapat banyak celah keamanan yang akan memudahkan seseorang meretasnya. Oleh karna itu dilakukan risk treatment untuk

mencegah resiko tersebut terjadi seperti meletakkan server data yang tidak mudah dilihat orang. Menggunakan password yang tidak mudah ditebak. Memberdayakan SDM yang terpecaya.

2. Penggunaan teknologi *Employee Monitoring Software* dapat membantu perusahaan dalam memonitor, mentracking atau bahkan merekam aktifitas kerja karyawannya. Penggunaan teknologi tersebut juga mempunyai beberapa resiko.

Seperti penggunaan aplikasi zoom. Untuk risk identification yaitu apakah data pribadi pengguna aman, apakah orang lain tanpa izin dapat mengintip komunikasi pengguna zoom.

Dan ternyata setelah dilakukan risk analys, ditemukan bahwa data pribadi pengguna zoom mengalami kebocoran, selain itu juga karna system keamanan zoom hanya mengandalkan protocol transport layer security, orang lain tanpa izin dapat mengintip komunikasi para pengguna zoom.

Oleh karna itu menurut saya, Aplikasi zoom boleh digunakan hanya untuk pekerjaan yang tidak memiliki data yang penting. Selain itu para pengguna zoom seharusnya tidak menggunakan email pribadi, dan hanya menggunakan email perusahaan saja.

UAS IT Risk Management

Nama : M.Afdhaluddin

Nim :1912420012

Dosen : Dedy Syamsuar, MIT, PhD

Pertanyaan dan Jawaban

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!

   Risk treatment adalah proses menanggulangi segala resiko yang akan terjadi dengan cara menghindari, menurunkan resiko, dan menghadapi resiko yang akan terjadi untujk melindungi asset, hal ini sangat berhubungan erat dengan hasil evalusi resiko yang telah ditetapkan dengan cara dilakukan penilaian apakah efektif atau tidaknya pencegahan yang dilakukan atau resiko mana yang paling tinggi akan terjadi

   Contoh : risk treatment pada ruang server, salah satu resiko yang akan terjadi adalah bencana alam seperti banjir gempa bumi, atau terjadinya pencurian, dan kebakaran. Dengan ancaman yang mungkin akan terjadi kita dapat mengevaluasi resiko tersebut dengan cara back up data, ruangan dengan suhu yang dingin, menyediakan pemadam api, kamera CCTV dan akses masuk ke ruang server yang ketat. lalu kita dapat hasil dari evaluasi tersebut seperti keamanan hardware yang pertama kita gunakan gembok, lalu dievaluasi dikarenakan resiko yang lain lalu ditambah jeruji pelindung lalu dievaluasi lagi, penambahan akses dengan kartu pegawai atau scan sidik jari dan kamera cctv.

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)

   Risk management Google hangouts meet.

   Rencana yang dilakukan dengan memberikan layanan akses kepada karyawan ke google hangouts, Menggunakan password saat memasuki konfrensi video, dan menggunakan data pribadi yang benar dan diketahui oleh perusahaan. Dan tidak men share file yang penting secara sembarang.

Resiko yang akan dihadapi berupa penambahan biaya yang akan digunakan , dikarenakan untuk mendapatkan akses berupa paket 100 pengguna atau pun fitur yang lain pada google hangouts meet harus melakukan pembayaran , di karenakan jumlah karyawan yang banyak.

Membutuhkan jaringan internet yang stabil.

Resiko yang lainya, pihak yang tidak bertanggung jawab mengakses atau mengawasi konfrensi yang dilakukan oleh perusahaan kita. Walaupun google hangouts meet telah memberikan layanan enkripsi video tetapi masih tetap harus waspada.