DASAR AUDIT

Sistem Informasi

PERAN IT PADA PERUSAHAAN

1. Di dunia yang semakin digital, perusahaan menggunakan TI tidak hanya untuk pemrosesan data tetapilebih untuk keunggulan strategis dan kompetitif juga
2. Penyebaran TI telah berkembang dari datapemrosesan ke MIS ke sistem pendukung keputusan ke transaksi/layanan onlin
3. TI tidak hanya mengotomatisasi proses bisnis tetapi juga mengubah cara proses bisnis dilakukan
4. Setiap perusahaan, terlepas dari ukurannya, perlu memiliki sistem pengendalian internal yang terpasang di dalam struktur perusahaan.
5. Kontrol didefinisikan sebagai ”Kebijakan, prosedur, praktik, dan struktur perusahaan yang dirancang untuk memberikan jaminan yang wajar bahwa tujuan bisnis akan dicapai dan kejadian yang tidak diinginkan dicegah atau dideteksi dan diperbaiki”
6. Organisasi TI harus menentukan strategi dan taktik mereka untuk mendukung organisasi dengan:memastikan bahwa operasi TI sehari-hari disampaikan secara efisien dan tanpa kompromi.

CONTOH RESIKO SISTEM INFORMASI

- 1. Google recovers from outage that took down YouTube, Gmail, and Snapchat (Jun 2019)
- https://www.theverge.com/2019/6/2/18649635/youtube-snapchat-down-outage
- 2. Unsecured Facebook Databases Leak Data Of 419 Million Users (Sep 2019)
- https://www.forbes.com/sites/daveywinder/2019/09/05/facebook-security-snafu-exposes-419-million-user-phone-numbers/#18a045b71ab7
- 3. AWS servers hit by sustained DDoS attack (Oct 2019)
- https://www.cloudpro.co.uk/cloud-essentials/public-cloud/8276/aws-servers-hit-by-sustained-ddos-attack
- 4. Reports says workers are biggest data security threat (Oct 2019)
- http://www.startribune.com/insiders-drive-most-cyber-security-breaches-according-to-study-for-minnesota-s-code42/562174112/

RISIKO

1. Sesuatu yang akan terjadi
2. Risiko adalah kemungkinan terjadinya sesuatu yang merugikan, yang mengakibatkan potensi kerugian/paparan.
3. Risiko dapat didefinisikan sebagai potensi bahaya yang ditimbulkan jika ancaman tertentu mengeksploitasikerentanan tertentu untuk menyebabkan kerusakan pada asset
4. analisis risiko didefinisikan sebagai proses mengidentifikasi risiko keamanan dan menentukan besarnya dan dampaknya terhadap organisasi.

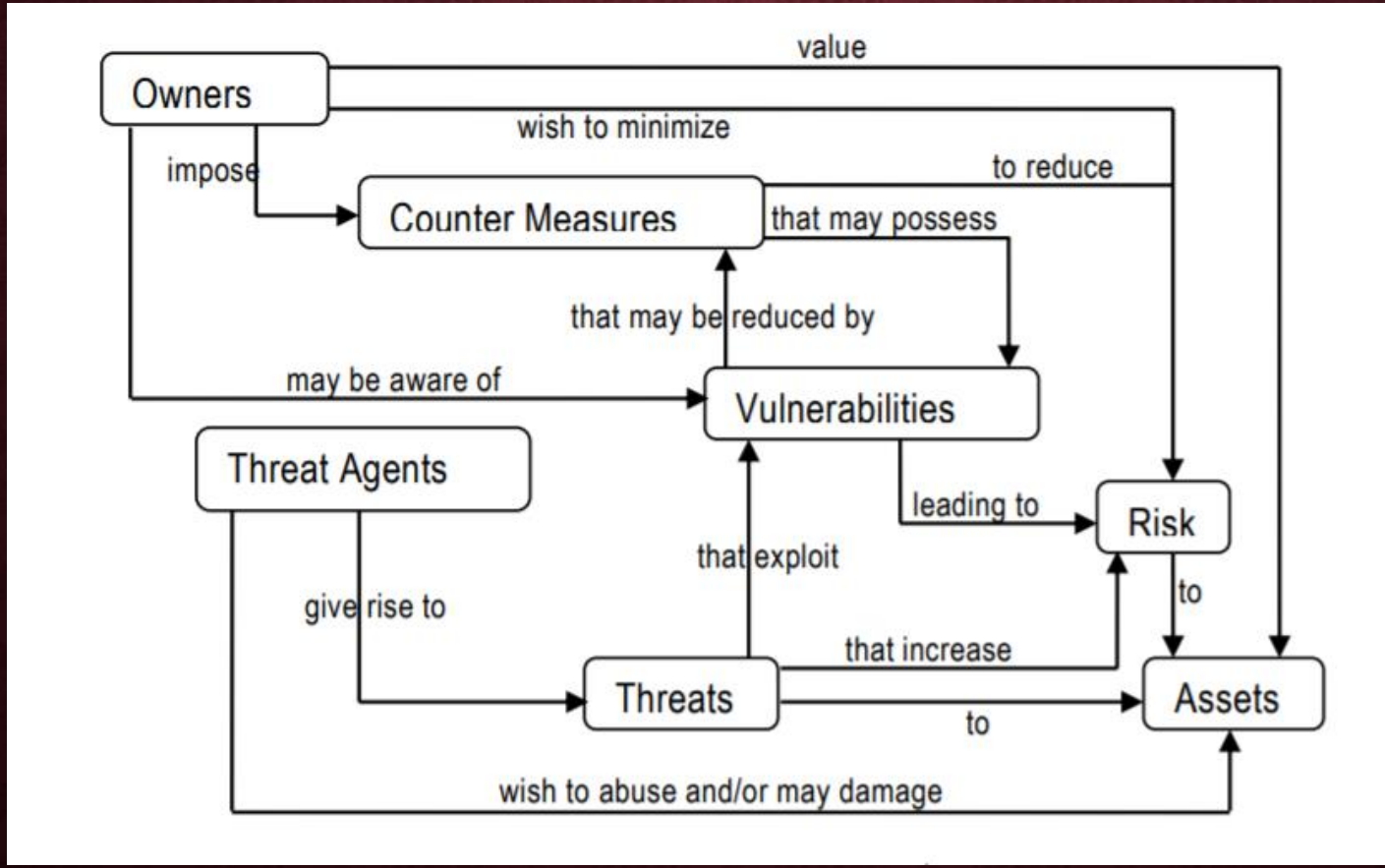
TERMINOLOGI TERKAIT RESIKO

1. Asset, dapat didefinisikan sebagai sesuatu yang bernilai bagi organisasi; misalnya, informasi dalam bentuk elektronik atau fisik, sistem perangkat lunak, karyawan
2. Vulnerability, kelemahan dalam pengamanan sistem yang mengekspossistem terhadap ancaman
3. Threat, Setiap entitas, keadaan, atau peristiwa yang berpotensi membahayakan sistem perangkat lunak ataukomponen melalui akses yang tidak sah, penghancuran, modifikasi, dan/atau penolakan layanan
4. Exposure, tingkat kerugian yang harus dihadapi perusahaan ketika risiko terwujud.

TERMINOLOGI TERKAIT RESIKO

1. Likelihood, Kemungkinan terjadinya ancaman adalah estimasi probabilitas bahwa ancaman tersebutakan berhasil dalam mencapai suatu kejadian yang tidak diinginkan
2. Attack, upaya untuk mendapatkan akses tidak sah ke layanan sistem atau untuk mengkompromikan ketergantungan sistem
3. Counter Measure, Suatu tindakan, alat, prosedur, teknik, atau ukuran lain yang mengurangi kerentanan suatu komponen atau system
4. Residual Risk, Setiap risiko yang masih tersisa setelah tindakan pencegahan dianalisis dan diterapkan

RISIKO


Owners
value
wish to minimize
impose
to reduce
Counter Measures
that may possess
that may be reduced by
may be aware of
Vulnerabilities
Threat Agents
leading to
Risk
that exploit
give rise to
to
that increase
Threats
Assets
to
wish to abuse and/or may damage

RISIKO

1. Threats
    1. Natural Disaster
    2. Man-made threat
    3. Technical
2. Impacts/Exposure
3. Probabilites/Likelihood

AUDIT SI

- Proses **pengumpulan dan evaluasi bukti-bukti** untuk menentukan apakah sistem komputer yang digunakan telah dapat [1]:
  - melindungi aset milik organisasi,
  - mampu menjaga integritas data,
  - membantu pencapaian tujuan organisasi secara efektif,
  - menggunakan sumber daya yang dimiliki secara efisien.
- Audit SI ialah **proses mengumpulkan dan mengevaluasi fakta** untuk memutuskan **apakah sistem komputer** yang merupakan aset bagi perusahaan **terlindungi**, **integritas data terpelihara**, **sesuai dengan tujuan organisasi** untuk **mencapai efektifitas dan efisiensi dalam penggunaan sumber daya** [2]
- Audit SI/TI merupakan **upaya menilai apakah proses IT sudah dilakukan dengan baik** untuk **mendukung tujuan organisasi** dengan **melakukan pengendalian dari outcome yang dihasilkan**. [3]

PENYALAHAGUNAAN KOMPUTER

- Hacking
- Virus
- Illegal Physical Access
- Abouse of Privilages

PENYALAHGUNAAN KOMPUTER

- Destruction of asset (perusakan aset)
- Theft of asset (pencurian aset)
- Modification of asset (modifikasi aset)
- Privacy violaction (pelanggaran privasi)
- Discruption of Operations (pengacauan operasi)
- Unauthorized use of asset (penyalahgunaan otorisasi aset)
- Physical harm to personnel (kejahatan fisik terhadap personal)

TUJUAN AUDIT