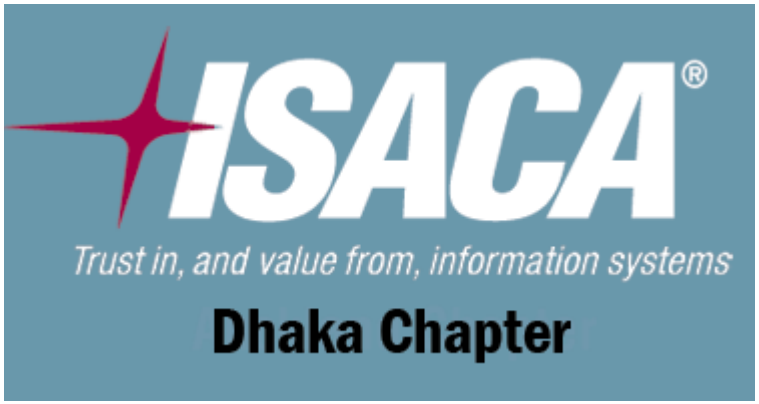
IT Risk and Control Framework

Mohammed Iqbal Hossain
CISA, CGEIT
Deputy Comptroller and Auditor General
Office of the C&AG, Bangladesh,
Board Member, ISACA Dhaka Chapter



Date: 25 February 2012

Session Objectives

ISACA
Trust in, and value from, information systems

- IT opportunities and risks
- Global concern/incidents
- Bangladesh perspective
- Best practices frameworks/standards
- ISACA COBIT framework
- Summary

Information is the key

- Information is the key resources
- We create information
- We use and store information
- We destroy information
- IT plays a key role in these activities
- Our duty is to protect these information asset

*http://www.dailytech.com/Worlds+Data+to+Reach+18+Zettabytes+by+2011/article11055.htm

Technology creates opportunities

- Business online
- Education online
- Government online
- Provide E-health service
- Buy electronic contents(e-books, software, music etc)

We can rich the whole world in a finger move

Opportunity creates Risk

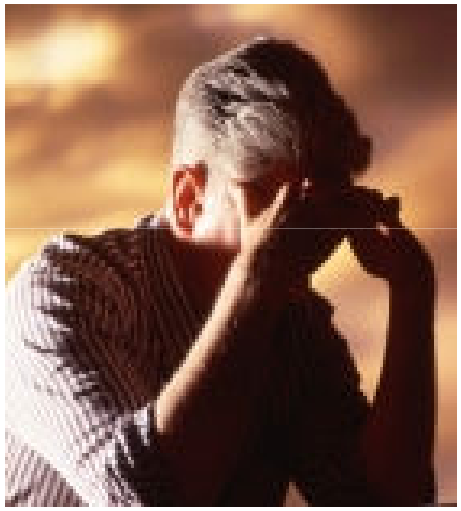
Opportunity and Risk are two sides of the same coin

What are the IT Risks?

- Email password may be disclosed
- Facebook account may be used by someone else
- Credit card information may be disclosed
- Customer information may be stolen
- IT Service delivery to the customers may be poor
- IT systems may be obsolete
- IT projects may be late or fail
- IT systems do not provide any business benefit
- Risk of non-compliance with the regulator
- Own people may harm the systems

IT risk is business risk

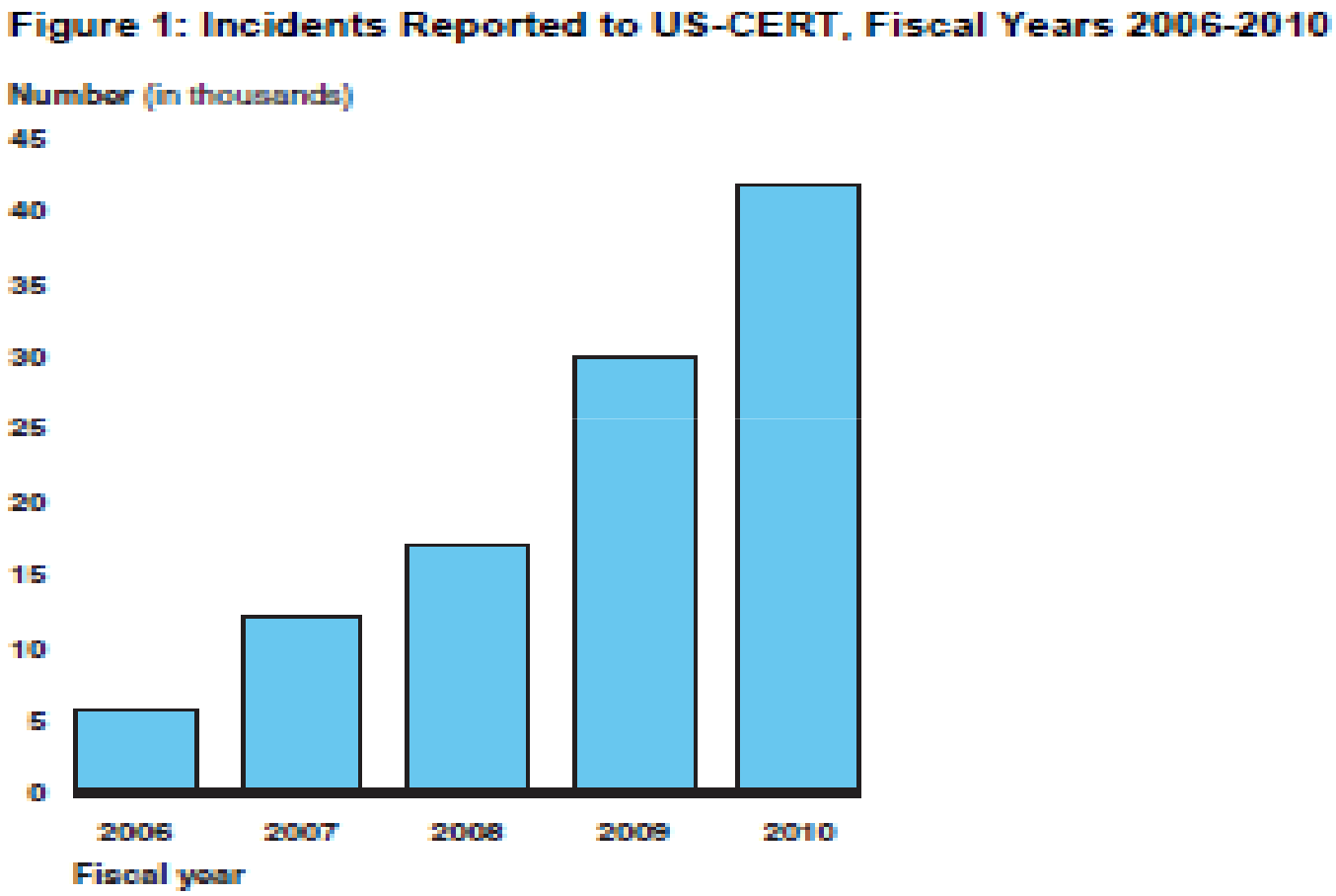
A Study in Project Failure



- Only one in eight IT projects can be considered truly successful (in terms of time, cost and quality)
- The cost of project failure across the European Union was €142 billion in 2004

Source: http://www.bcs.org/content/ConWebDoc/19584

Incidents Reported by US Federal Agencies



http://www.gao.gov/products/GAO-12-137

KPMG e-Crime Survey (2011)

ISACA
Trust in, and value from, information systems

- E-crime is no longer driven by profit alone
- Hackers are now state-sponsored and politically motivated
- Simply defending systems against attack is not a sufficient strategy for today's threat environment.
- A complete approach needs to cover defence, detection, reaction and recovery

"The complexity of security challenges created by technology is only increasing"

http://www.kpmg.com/UK

Recent Cyber crime news

- Department of Homeland Security website hacked
- NASDAQ Site was track down with DDOS Attack
- Cyber attack crashes Irish government website
- Hackers Attack Second Brazilian Bank's Website
- Ukraine Govt retreats after massive cyber-siege
- Zappos.com hacked; 24 million customers affected
- VeriSign Hit by Hackers in 2010
- Saudi hacker publishes Israeli credit card details
- Websites of 2 Palestinian news agencies brought down by cyber attack

Source: http://www.infowar.com/

ISACA Survey (2011)

ISACA
Trust in, and value from, information systems

- Increasing IT costs — 42%
- Insufficient IT skills — 33%
- Problems implementing new IT systems — 30%
- Problems with external IT service providers — 29%
- Serious operational IT incidents — 21%
- Return on investment not as expected — 19%
- IT security or privacy incidents — 18%

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ITGI-Global-Survey-Results.aspx

Bangladesh Scenario

ISACA
Trust in, and value from, information systems

Achievement

- Ranked 134 in UN E-Gov survey in e-gov development category
- Some quick win projects by Government
- Bangladesh is on the list of top 30 destinations for global IT outsourcing for 2010-11(Garter)

Challenges

- Ranked poor in language, infrastructure and data and intellectual property security (Gartner)
- Lack of sustainability of IT Systems
- Lack of ownership of IT systems
- Inadequate Human resources
- Poor IT management
- Increased cyber incidents
- No National BD-CERT

The impact of IT risks

- No organization is unaffected
- Businesses are disrupted
- Privacy is violated
- Organizations' suffer direct financial loss
- Reputation is damaged

What is the solution

- No 100% solution
- We can not solve all the problems
- We can reduce to an acceptable level only
- Use best practices

Advantage of using Best Practices

ISACA
Trust in, and value from, information systems

- Better accountability and responsibility (ownership)
- No blame game
- Better management
- Better benefits from IT investments
- Better Compliance
- Better monitoring
- Compare with others

Some examples of best practice

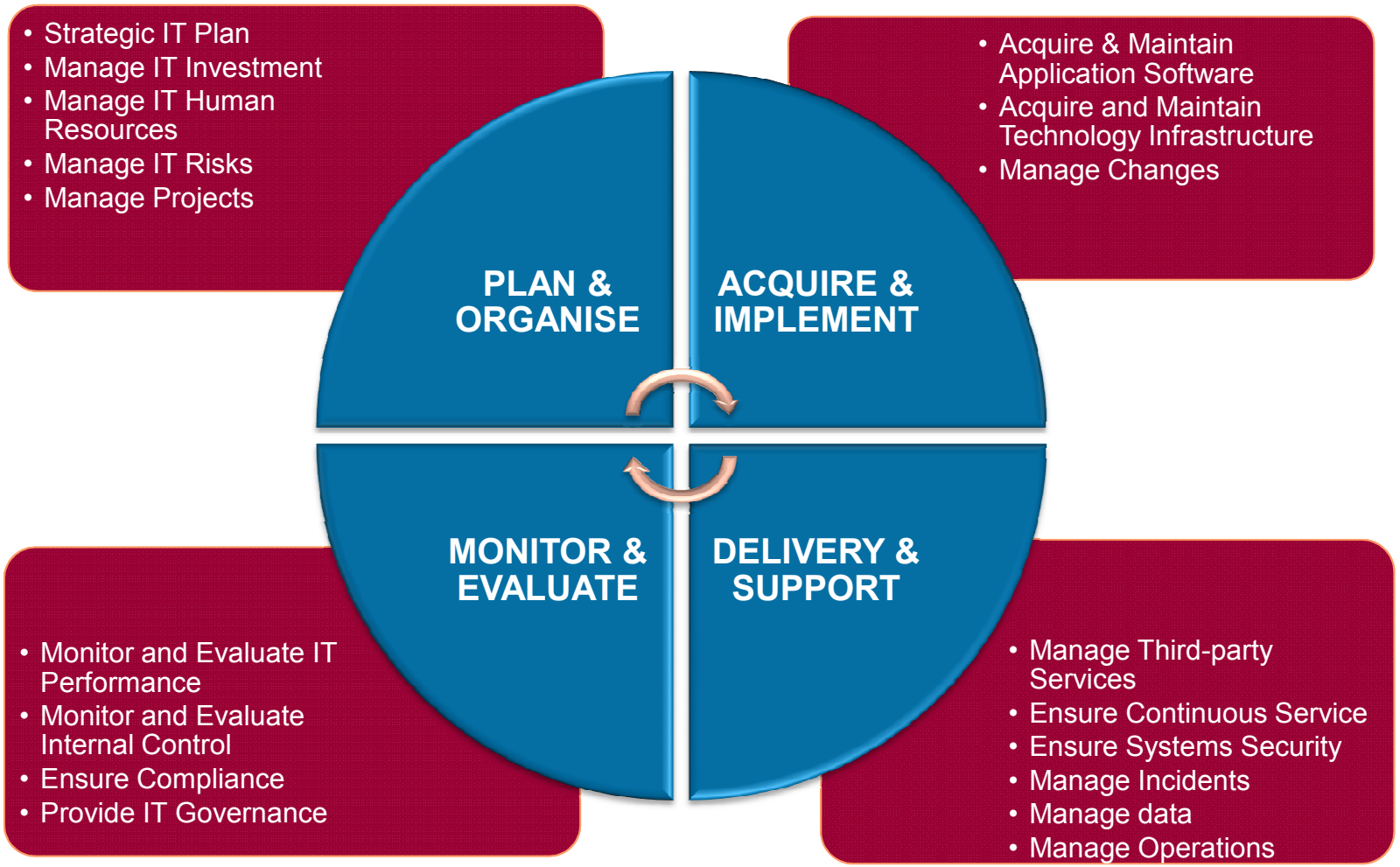
- COBIT
- ITIL
- ISO 27001/2
- COSO ERM
- PRINCE2
- PMBOK
- Six Sigma
- TOGAF

About COBIT

- COBIT is a comprehensive IT governance and management framework.
- Accepted globally as a set of tools that ensures IT is working effectively and efficiently
- Addresses every aspect of IT
- Ensure clear ownership and responsibilities
- A common language for all
- Improves IT efficiency and effectiveness
- Better management of IT investments
- Ensure compliance
- Complementary copy is available (www.isaca.org/cobit)

COBIT Coverage

ISACA
Trust in, and value from, information systems



COBIT Define Responsibility & Accountability

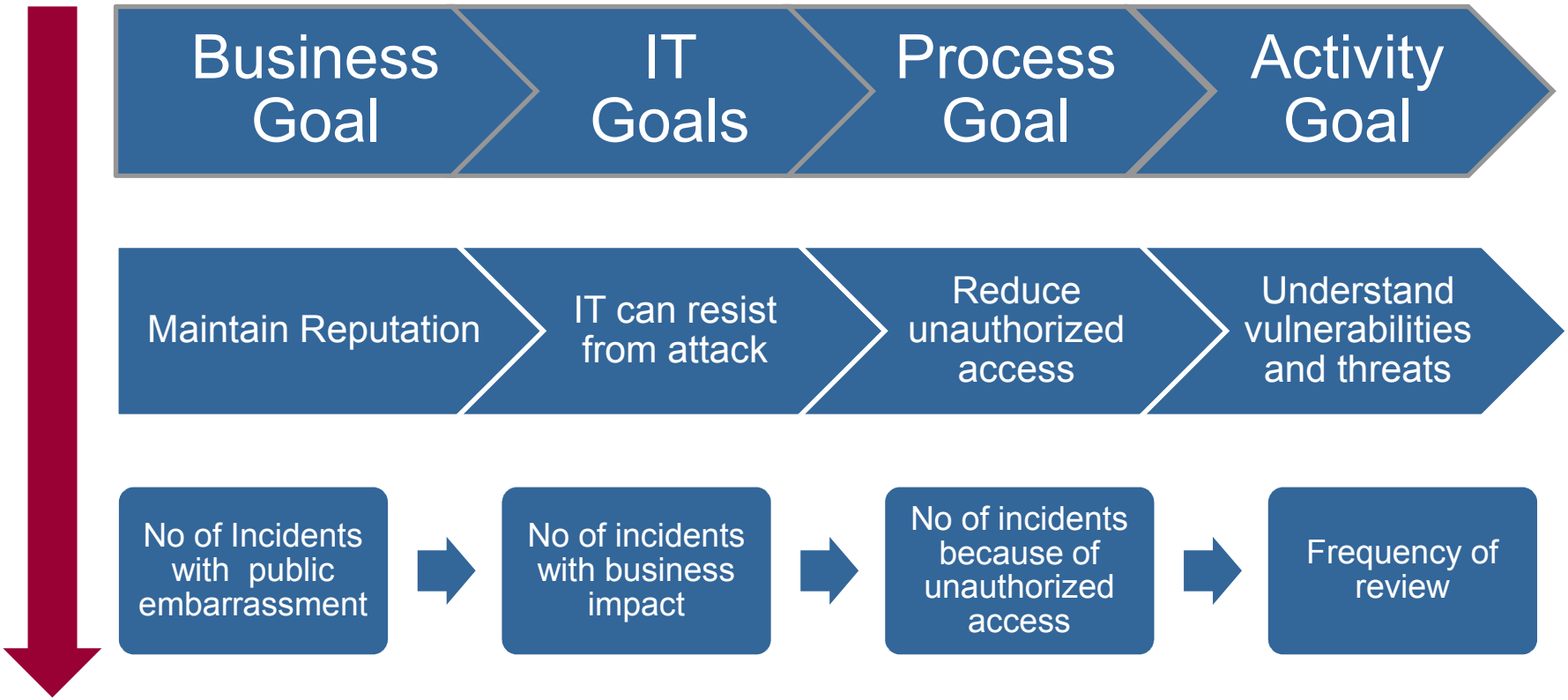
ISACA
Trust in, and value from, information systems

RACI Chart

Activities / Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Link business goals to IT goals.	C	I	A/ R	I	C						
Identify critical dependencies and current performance.	C	C	R	A/ R	C	C	C	C	C		C
Build an IT strategic plan.	A	C	C	R	I	C	C	C	C	I	C
Build IT tactical plans.	C	I		A	C	C	C	C	C	R	I
ENSURE SYSTEM SECURITY (DS5)											
Define and Maintain IT Security Plan.	I	C	C	A	C	C	C	C	I	I	R
Conduct regular vulnerability assessments.		I		A	I	C	C	C			R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Define Goals and Metrics



COBIT links Business goals to IT Process

ISACA
Trust in, and value from, information systems

Business Goals(17) → IT Goals(28) → IT Processes(32)

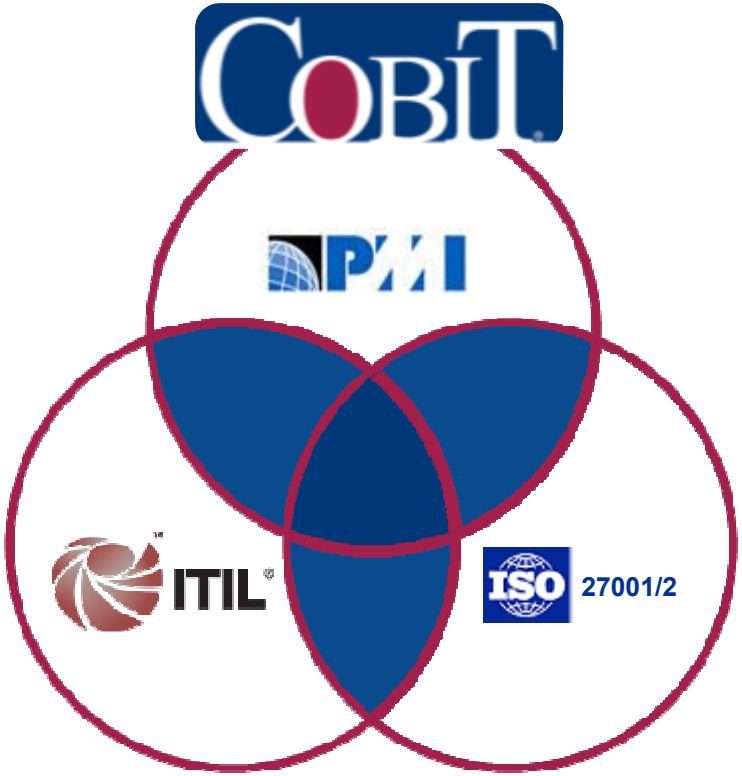
Maintain IT Related Business Risk

- Respond to governance requirements
- Account for and protect all IT assets.
- Protect the achievement of IT objectives.
- Establish clarity of business impact
- Ensure that critical and confidential information is authorized
- Ensure that automated business transactions can be trusted.
- Ensure that IT services and infrastructure can properly resist and recover from failures
- Ensure minimum business impact in the event of an IT service disruption

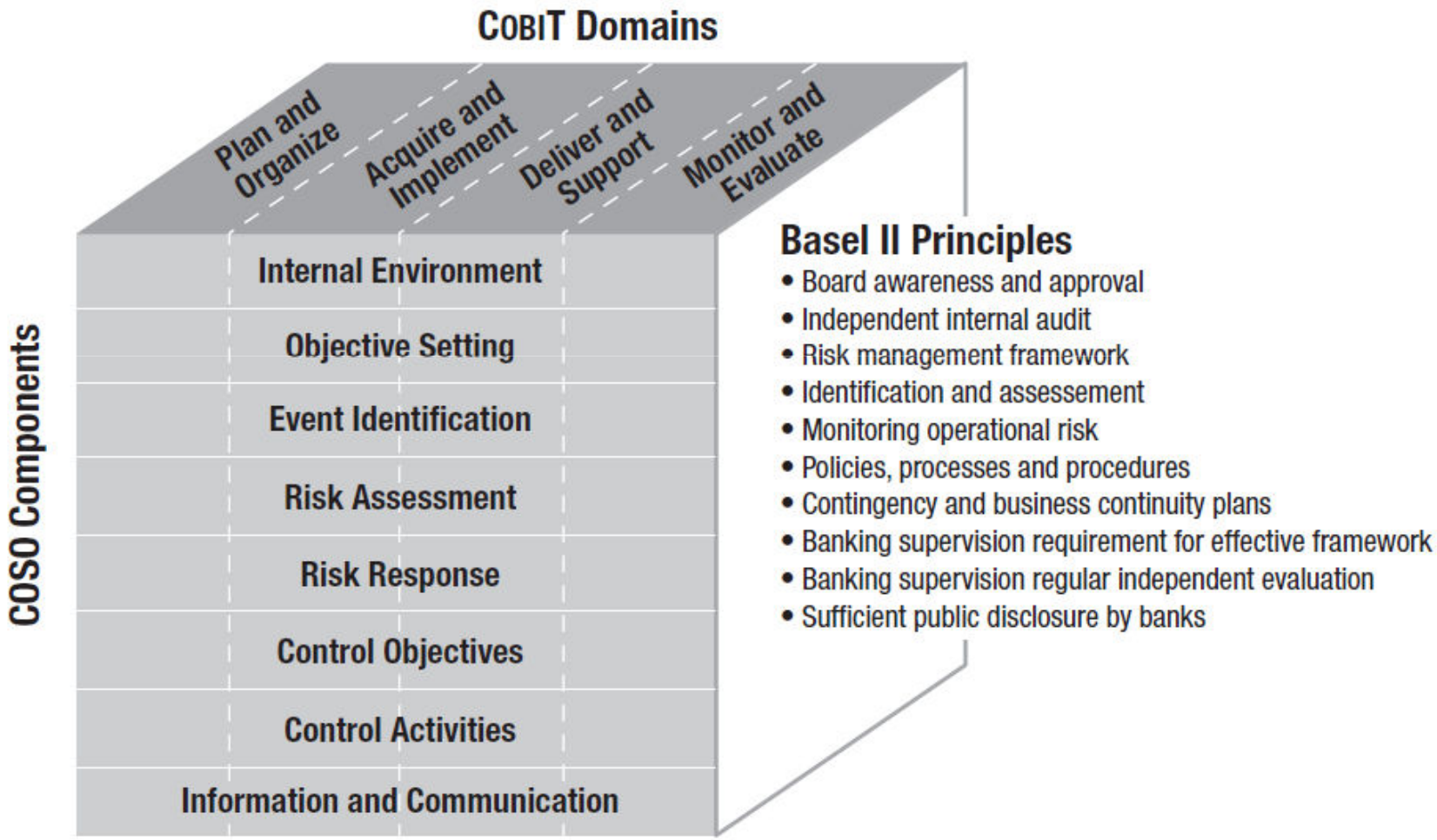
- ❑Assess and manage IT risks(PO9)
- ❑Ensure systems security(DS5)
- ❑Manage the configuration(DS9)
- ❑Manage Facilities(DS12)
- ❑Monitor and evaluate internal control (ME2)

COBIT maps other frameworks

- ITIL
- ISO 27001/2
- ISO 20000
- PMBOK,
- TOGAF
- CMMI
- COSO



COBIT maps with Basel II



Source: IT Control Objectives for Basel II

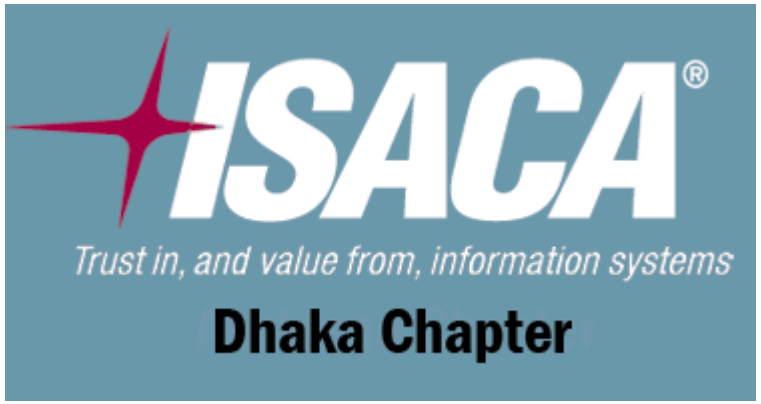
Summary

ISACA
Trust in, and value from, information systems

- Use Best practice such as COBIT to minimize IT Risks
- Start with basic processes
- Form a high level IT Strategy Committee headed by CEO/Head.
- Formulate and implement IT Strategic Plan and IT policies.
- Allocate resources (People, infrastructure,)
- Assign roles and responsibilities, authority and accountability (Use RACI Chart)
- Make IT a regular board agenda.
- Regularly assess, review and monitor IT Risks.
- Establish a national BD-CERT(by gov)

Thank You!

Questions?



Apa Risiko IT-nya?

1. Kata sandi email dapat dicuri

2. Akun Facebook dapat digunakan oleh orang lain

3. Informasi kartu kredit dapat dicuri

4. Informasi pelanggan dapat dicuri

5. IT Layanan pengiriman ke pelanggan mungkin buruk mungkin buruk sistem

6. IT mungkin usang

7. IT proyek mungkin terlambat atau gagal

8. IT sistem lakukan tidak memberikan keuntungan bisnis apa pun

9. Risiko ketidakpatuhan dengan regulator

10. Orang pribadi dapat merusak sistem

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Mata Kuliah : IT Audit
Tugas 3 : Indri Endang Lestari & Sulistiyani

A. Menentukan thread/Ancaman :

1. Access to the network by unauthorized persons
2. Disclosure of passwords
3. Loss of electricity
4. Unauthorized access to the information system
5. Compromising confidential information

B. Menentukan Thread Source

1. Access to the network by unauthorized persons : Employee, Vendor
2. Disclosure of passwords : Employee
3. Loss of electricity : Employee , Contractor
4. Unauthorized access to the information system : Employee , Vendor
5. Compromising confidential information : Employee , Vendor

C. Menentukan Probability/Kemungkinan :

Probability of Occurrence	Score
Access to the network by unauthorized persons	4
Disclosure of passwords	2
Loss of electricity	4
Unauthorized access to the information system	4
Compromising confidential information	3

D. Menentukan Impact

Probability of Occurrence	Score
Access to the network by unauthorized persons	5
Disclosure of passwords	1
Loss of electricity	2
Unauthorized access to the information system	3
Compromising confidential information	5

E. Menentukan *Risk Acceptance*

	Risk Score		Risk Score	Risk Acceptance
	Probability	Impact		
Access to the network by unauthorized persons	4	5	20	High
Disclosure of passwords	2	1	2	Very Low
Loss of electricity	4	2	8	Low
Unauthorized access to the information system	4	3	12	Medium
Compromising confidential information	3	5	15	Medium

tugas sulistiyani

Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

JENIS-JENIS RISIKO AUDIT

Resiko Bawaan atau Risiko Melekat (Inherent Risk)

Kemungkinan adanya kekeliruan atau salah saji dalam segmen audit yang melampaui batas toleransi, sebelum memperhitungkan faktor efektivitas pengendalian intern. Resiko bawaan menunjukkan faktor-faktor kerentanan laporan keuangan terhadap kekeliruan yang material dengan asumsi tidak ada pengendalian intern.
Bila auditor berkesimpulan bahwa akan banyak kemungkinan terjadi kekeliruan tanpa pengendalian intern, berarti risiko bawaannya tinggi. Faktor pengendalian intern tidak diperhitungkan dalam menetapkan inherent risk (risiko bawaan) karena dalam model risiko audit hal itu akan diperhitungkan tersendiri sebagai risiko pengendalian.
Hubungan antara risiko bawaan (inherent risk) dengan risiko penemuan (planned detection risk) serta rencana pengumpulan bukti adalah bahwa inherent risk sifatnya berbanding terbalik dengan planned detection risk rendah, maka planned detection risk tinggi dan bukti yang harus dikumpulkan sedikit.
Contohnya sebagai berikut :

1. Akun kas, memiliki resiko bawaan atau resiko melekat dari pada aktiva tetap
2. Dikarenakan kas tidak mempunyai bukti kepemilikan (sifat : inherent risk)

Risiko Pengendalian (Control Risk)

Penetapan auditor memungkinan adanya kekeliruan (salah saji) dalam segmentas audit yang melampaui batas toleransi yang tidak terdeteksi atau tercegah oleh struktur pengendalian internal klien. Pengendalian manajemen perusahaan klien buruk/kurang baik dalam pengendalian, sehingga tidak bisa dikendalikan auditor.
Risiko pengendalian (control risk) mengandung unsur-unsur sebagai berikut :

1. Apakah struktur pengendalian internal perusahaan klien sudah efektif untuk mendeteksi atau mencegah kekeliruan dalam perusahaan.
2. Auditor dapat membuat penetapan resiko pengendalian dibawah nilai maksimum (100%) dalam rencana audit.

Penemuan Resiko (Detection Risk)

Penemuan resiko menunjukan bahwa bukti yang dikumpulkan auditor dalam perusahaan klien menemukan kekeliruan yang melampaui jumlah yang dapat ditoleransi. Resiko bukti fisik dapat dikendalikan oleh auditor. Karna biasanya disebabkan akuntan perusahaan hanya mengamati bukti fisik, atau akuntan salah dalam memilih sample bukti.
Ada dua hal penting yang harus diperhatikan auditor dalam penemuan resiko :

1. Penemuan risiko yang direncanakan hanya akan berubah jika auditor mengubah salah satu unsur lainnya dalam penemuan resiko.
2. Penemuan resiko menentukan besarnya bukti yang akan dikumpulkan. Hubungan antara penemuan resiko dengan bukti berbanding terbalik. Jika nilai risiko penemuan yang direncanakan diperkecil, berarti jumlah bukti yang harus dikumpulkan auditor dalam audit perusahaan klien lebih banyak.

Jelaskan bagaimana resiko-resiko tersebut dikendalikan?

Resiko merupakan salah satu aspek penting yang mendasari proses audit. Menurut Hendry Simamora (2002;99) ada 2 jenis resiko yang dihadapi oleh auditor yang mengaudit laporan keuangan, yaitu :

1. Resiko audit, adalah resiko yang timbul karena auditor tanpa disadari tidak memodifikasi pendapatnya sebagaimana mestinya, atas suatu laporan keuangan yang mengandung salah saji material.
2. Resiko bisnis auditor, adalah terpaparnya auditor terhadap kerugian atau kerusakan praktik profesinalnya akibat litigasi, publisitas yang buruk, ataupun peristiwa lainnya yang mencuat sehubungan dengan laporan keuangan yang diaudit dan dilaporkannya.

Paparan terhadap resiko bisnis senantiasa muncul baik auditor melakukan auditnya menurut standar auditing yang berlaku umum ataupun tidak. Resiko bisnis auditor berbeda dengan resiko audit, meskipun demikian, auditor bisa saja memutuskan untuk menggali lebih banyak bukti audit disebabkan meningkatnya resiko bisnisnya. Dalam standar auditing yang berlaku umum, auditor tidak boleh memutuskan untuk mengumpulkan lebih sedikit bukti audit hanya karena mengaudit klien dengan resiko bisnis yang minimal. Resiko bisnis auditor tidak dapat dikendalikan secara langsung oleh auditor, meskipun demikian beberapa pengendalian dapat dijalankan melalui penerimaan dan penolakan klien dengan hati – hati. Di lain pihak, resiko audit dapat dikendalikan secara langsung melalui lingkup prosedur tes auditor. Model resiko audit menawarkan kerangka acuan untuk diikuti oleh auditor.

Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

JENIS-JENIS RISIKO AUDIT

Resiko Bawaan atau Risiko Melekat (Inherent Risk)

Kemungkinan adanya kekeliruan atau salah saji dalam segmen audit yang melampaui batas toleransi, sebelum memperhitungkan faktor efektivitas pengendalian intern. Resiko bawaan menunjukkan faktor-faktor kerentanan laporan keuangan terhadap kekeliruan yang material dengan asumsi tidak ada pengendalian intern.
Bila auditor berkesimpulan bahwa akan banyak kemungkinan terjadi kekeliruan tanpa pengendalian intern, berarti risiko bawaannya tinggi. Faktor pengendalian intern tidak diperhitungkan dalam menetapkan inherent risk (risiko bawaan) karena dalam model risiko audit hal itu akan diperhitungkan tersendiri sebagai risiko pengendalian.
Hubungan antara risiko bawaan (inherent risk) dengan risiko penemuan (planned detection risk) serta rencana pengumpulan bukti adalah bahwa inherent risk sifatnya berbanding terbalik dengan planned detection risk rendah, maka planned detection risk tinggi dan bukti yang harus dikumpulkan sedikit.
Contohnya sebagai berikut :

1. Akun kas, memiliki resiko bawaan atau resiko melekat dari pada aktiva tetap
2. Dikarenakan kas tidak mempunyai bukti kepemilikan (sifat : inherent risk)

Risiko Pengendalian (Control Risk)

Penetapan auditor memungkinan adanya kekeliruan (salah saji) dalam segmentas audit yang melampaui batas toleransi yang tidak terdeteksi atau tercegah oleh struktur pengendalian internal klien. Pengendalian manajemen perusahaan klien buruk/kurang baik dalam pengendalian, sehingga tidak bisa dikendalikan auditor.
Risiko pengendalian (control risk) mengandung unsur-unsur sebagai berikut :

1. Apakah struktur pengendalian internal perusahaan klien sudah efektif untuk mendeteksi atau mencegah kekeliruan dalam perusahaan.
2. Auditor dapat membuat penetapan resiko pengendalian dibawah nilai maksimum (100%) dalam rencana audit.

Penemuan Resiko (Detection Risk)

Penemuan resiko menunjukan bahwa bukti yang dikumpulkan auditor dalam perusahaan klien menemukan kekeliruan yang melampaui jumlah yang dapat ditoleransi. Resiko bukti fisik dapat dikendalikan oleh auditor. Karna biasanya disebabkan akuntan perusahaan hanya mengamati bukti fisik, atau akuntan salah dalam memilih sample bukti.
Ada dua hal penting yang harus diperhatikan auditor dalam penemuan resiko :

1. Penemuan risiko yang direncanakan hanya akan berubah jika auditor mengubah salah satu unsur lainnya dalam penemuan resiko.
2. Penemuan resiko menentukan besarnya bukti yang akan dikumpulkan. Hubungan antara penemuan resiko dengan bukti berbanding terbalik. Jika nilai risiko penemuan yang direncanakan diperkecil, berarti jumlah bukti yang harus dikumpulkan auditor dalam audit perusahaan klien lebih banyak.

Jelaskan bagaimana resiko-resiko tersebut dikendalikan?

Resiko merupakan salah satu aspek penting yang mendasari proses audit. Menurut Hendry Simamora (2002;99) ada 2 jenis resiko yang dihadapi oleh auditor yang mengaudit laporan keuangan, yaitu :

1. Resiko audit, adalah resiko yang timbul karena auditor tanpa disadari tidak memodifikasi pendapatnya sebagaimana mestinya, atas suatu laporan keuangan yang mengandung salah saji material.
2. Resiko bisnis auditor, adalah terpaparnya auditor terhadap kerugian atau kerusakan praktik profesinalnya akibat litigasi, publisitas yang buruk, ataupun peristiwa lainnya yang mencuat sehubungan dengan laporan keuangan yang diaudit dan dilaporkannya.

Paparan terhadap resiko bisnis senantiasa muncul baik auditor melakukan auditnya menurut standar auditing yang berlaku umum ataupun tidak. Resiko bisnis auditor berbeda dengan resiko audit, meskipun demikian, auditor bisa saja memutuskan untuk menggali lebih banyak bukti audit disebabkan meningkatnya resiko bisnisnya. Dalam standar auditing yang berlaku umum, auditor tidak boleh memutuskan untuk mengumpulkan lebih sedikit bukti audit hanya karena mengaudit klien dengan resiko bisnis yang minimal. Resiko bisnis auditor tidak dapat dikendalikan secara langsung oleh auditor, meskipun demikian beberapa pengendalian dapat dijalankan melalui penerimaan dan penolakan klien dengan hati – hati. Di lain pihak, resiko audit dapat dikendalikan secara langsung melalui lingkup prosedur tes auditor. Model resiko audit menawarkan kerangka acuan untuk diikuti oleh auditor.

TUGAS PENGENDALIAN RESIKO

Nama : Uci Suriani

Kelas : MTi Reguler A

NIK : 182420072

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

PASCASARJANA UNIVERSITAS BINA DARMA

PALEMBANG

2019

Resiko adalah suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisa serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko.

Seiring dengan berkembangnya teknologi informasi yang bergerak sangat cepat dewasa ini, pengembangan unit usaha yang berupaya menerapkan sistem informasi dalam organisasinya telah menjadi kebutuhan dasar dan semakin meningkat dari tahun ke tahun. Akan tetapi pola pembangunan sistem informasi yang mengindahkan faktor resiko telah menyebabkan beberapa organisasi mengalami kegagalan menerapkan teknologi informasi tersebut, atau meningkatnya nilai investasi dari *plafon* yang seharusnya, hal ini juga dapat menghambat proses pencapaian misi organisasi.

Jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi :

Pada dasarnya, faktor resiko dalam suatu perencanaan sistem informasi, dapat diklasifikasikan ke dalam 4 kategori resiko, yaitu :

a. *Catastrophic* (Bencana)

b. *Critical* (Kritis)

c. *Marginal* (kecil)

d. *Negligible* (dapat diabaikan)

Adapun pengaruh atau dampak yang ditimbulkan terhadap suatu proyek sistem informasi dapat berpengaruh kepada

a) nilai unjuk kerja dari sistem yang dikembangkan,

b) biaya yang dikeluarkan oleh suatu organisasi yang mengembangkan teknologi informasi,

c) dukungan pihak manajemen terhadap pengembangan teknologi informasi, dan

d) Jadwal waktu penerapan pengembangan teknologi informasi.

Suatu resiko perlu didefinisikan dalam suatu pendekatan yang sistematis, sehingga pengaruh dari resiko yang timbul atas pengembangan teknologi informasi pada suatu organisasi dapat diantisipasi dan di identifikasi sebelumnya. Mendefinisikan suatu resiko dalam pengembangan teknologi informasi pada suatu organisasi terkait dengan Siklus Hidup Pengembangan Sistem (*System Development Life Cycle* [SDLC]), dimana fase-fase penerapan SDLC dalam pengembangan teknologi informasi di spesifikasikan analisa resiko.

Pola Pendekatan

System Development Life Cycle [SDLC] adalah suatu tahapan proses perancangan suatu sistem yang dimulai dari tahap investigasi; pembangunan; implementasi; operasi/perawatan; serta tahap penyelesaian [4]. Dari dasar tersebut di atas, strategi penerapan manajemen resiko perlu mempertimbangkan dampak yang mungkin timbul dengan tingkat probabilitas yang berbeda untuk setiap komponen pengembangan sistem informasi.

Pola pendekatan manajemen resiko juga perlu mempertimbangkan faktor-faktor pada *System Development Life Cycle* (SDLC) yang terintegrasi, yaitu Mengindentifikasikan faktor-faktor resiko yang timbul dan diuraikan disetiap tahap perancangan sistem, yang tersusun sebagai berikut :

1. ***Tahap 1. Investigasi*** : Tahap ini suatu sistem didefinisikan, menyangkut ruang lingkup pengembangan yang akan dibuat, yang semua perencanaan atas pengembangan sistem di dokumentasikan terlebih dahulu. Dukungan yang dibutuhkan dari manajemen resiko pada tahap ini adalah faktor resiko yang mungkin terjadi dari suatu sistem informasi di identifikasikan, termasuk di dalamnya masalah serta konsep pengoperasian keamanan sistem yang semuanya bersifat strategis.
2. ***Pengembangan*** : Tahap ini merupakan tahap dimana suatu sistem informasi dirancang, pembelian komponen pendukung sistem di laksanakan, aplikasi di susun dalam program tertentu, atau masa dimana konstruksi atas sistem di laksanakan. Pada proses ini, faktor resiko diidentifikasikan selama tahap ini dilalui, dapat berupa analisa atas keamanan sistem sampai dengan kemungkinan yang timbul selama masa konstruksi sistem di laksanakan.
3. ***Implementasi*** : Tahap ini kebutuhan atas keamanan sistem dikonfigurasikan, aplikasi sistem di uji coba sampai pada verifikasi atas suatu sistem informasi di lakukan. Pada tahap ini faktor resiko di rancang guna mendukung proses pelaksanaan atas implementasi sistem informasi sehingga kebutuhan riil di lapangan serta pengoperasian yang benar dapat dilaksanakan.
4. ***Pengoperasian dan Perawatan*** : Tahap ini merupakan tahap dimana sistem informasi telah berjalan sebagaimana mestinya, akan tetapi secara secara berkala sistem membutuhkan modifikasi, penambahan peralatan baik perangkat keras maupun perangkat lunak pendukung, perubahan tenaga pendukung operasi, perbaikan kebijakan maupun prosedur dari suatu organisasi. Pada tahap ini manajemen resiko lebih menitik beratkan pada kontrol berkala dari semua faktor yang menentukan berjalannya sistem, seperti perangkat keras, perangkat lunak, analisa sumber daya manusia, analisa basis data, maupun analisa atas jaringan sistem informasi yang ada.
5. **Penyelesaian/penyebaran** : Tahap ini merupakan tahap dimana system informasi yang telah digunakan perlu di lakukan investasi baru karena unjuk kerja atas sistem tersebut telah berkurang, sehingga proses pemusnahan data, penggantian perangkat keras dan perangkat lunak, ataupun berhentinya kegiatan atau kepindahan organisasi ke tempat yang baru. Manajemen resiko yang perlu di perhatikan dalam tahap ini adalah memastikan proses pemusnahan atas komponen-komponen system informasi dapat berjalan dengan baik, terkelola dari segi keamanan.

Setelah pola pendekatan manajemen resiko di definisikan dalam masing-masing tahap SDLC, maka tahap selanjutnya adalah menilai manajemen resiko dalam metodologi tertentu. Upaya memberikan penilaian atas dampak resiko dalam pengembangan sistem informasi,

perlu dilakukan karena dapat memberikan gambaran atas besar atau kecilnya dampak ancaman yang mungkin timbul selama proses pengembangan sistem.

Metodologi Penilaian Resiko

Untuk menentukan kemungkinan resiko yang timbul selama proses pengembangan sistem informasi berlangsung, maka organisasi yang bermaksud mengembangkan sistem informasi perlu menganalisa beberapa kemungkinan yang timbul dari pengembangan sistem informasi tersebut. Adapun metodologi penilaian resiko pengembangan sistem informasi dapat diuraikan dalam 9 langkah, yang tersusun sebagai berikut :

a. Menentukan karakteristik dari suatu sistem

b. Mengidentifikasikan ancaman-ancaman

c. Mengidentifikasikan kelemahan sistem

d. Menganalisa pengawasan

e. Menentukan beberapa kemungkinan pemecahan masalah

f. Menganalisa pengaruh resiko terhadap pengembangan sistem

g. Menentukan resiko

h. Merekomendasikan cara-cara pengendalian resiko

i. Mendokumentasikan hasil keputusan

Tahap ke dua, tiga, empat dan enam dari langkah tersebut di atas dapat dilakukan secara paralel setelah langkah pertama dilaksanakan. Adapun dari setiap langkah tersebut adalah sebagai berikut :

Langkah 1. Menentukan Karakterisasi Sistem

Pada langkah pertama ini batasan suatu sistem yang akan dikembangan di identifikasikan, meliputi perangkat keras, perangkat lunak, sistem interface, data dan informasi, sumber daya manusia yang mendukung sistem IT, tujuan dari sistem, sistem dan data kritis, serta sistem dan data sensitif. Beberapa hal tambahan yang dapat diklasifikasikan pada karakteristik sistem selain hal tersebut di atas seperti bentuk dari arsitektur keamanan sistem, kebijakan yang dibuat dalam penanganan keamanan sistem informasi, bentuk topologi jaringan komputer yang dimiliki oleh organisasi tersebut, Manajemen pengawasan yang dipakai pada sistem TI di organisasi tersebut, dan hal lain yang berhubungan dengan masalah keamanan seputar penerapan Teknologi Informasi di organisasi yang bermaksud mengembangkan sistem informasi.

Adapun teknik pengumpulan informasi yang dapat diterapkan pada langkah ini meliputi :

1. ***Membuat daftar kuesinoner***. Daftar kuesioner ini di susun untuk semua level manajemen yang terlibat dalam sistem dengan tujuan mengumpulkan informasi

seputar keamanan data dan informasi dengan tujuan untuk memperoleh pola resiko yang mungkin dihadapi oleh sistem.

2. ***Interview.*** Bentuk lain dari pengumpulan data dengan cara interview terhadap IT Support atau personil yang terlibat dalam sistem informasi.
3. ***Review atas dokumen.*** Review atas dokumen pengembangan sistem, Dokumen kebijakan, atau dokumen keamanan informasi dapat memberikan gambaran yang bermanfaat tentang bentuk dari kontrol yang saat ini diterapkan oleh SI maupun rencanan pengembangan dari pengawasan di masa depan.
4. ***Penerapan Tool.*** Menggunakan suatu tool aplikasi yang memiliki tujuan untuk mengumpulkan informasi tentang sistem informasi yang digunakan merupakan salah satu cara untuk dapat memetakan sistem secara keseluruhan, seperti penggunakan network monitor, maupun tools lain.

Hasil output dari langkah pertama ini akan menghasilkan Penaksiran atas karakteristik sistem IT, Gambaran tentang lingkungan sistem IT serta gambaran tentang batasan dari sistem yang dikembangkan.

Langkah 2. Mengidentifikasikan ancaman-ancaman

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Timbulnya ancaman dapat dipicu oleh suatu kondisi dari sumber ancaman. Sumber ancaman dapat muncul dari kegiatan pengolahan informasi yang berasal dari 3 hal utama, yaitu (1) Ancaman Alam; (2) Ancaman Manusia, dan (3) Ancaman Lingkungan. Ancaman yang berasal dari manusia memiliki karakteristik tersendiri, serta memiliki alasan tersendiri dalam melakukan gangguan terhadap sistem informasi yang ada. Adapun alasan yang timbul dari ancaman manusia ini dapat di definisikan dalam tabel berikut :

Sumber Ancaman	Alasan	Aksi yang timbul
Hacker, Cracker	• Tantangan • Ego • Memberontak	• Hacking • Social Engineering • Gangguan sistem • Akses terhadap sistem
Kriminal	• Perusakan informasi • Penyingkapan informasi secara ilegal • Keuntungan moneter • Merubah data	• Tindak Kriminal • Perbuatan curang • Penyuapan • Spoofing • Intrusi atas sistem
Teroris	• Surat kaleng • Perusakan • Peledakan • Balas dendam	• Bom/teror • Perang informasi • Penyerangan sistem • Penembusan atas sistem • Tampering sistem
Mata-mata	• Persaingan usaha	• Pencurian informasi • Social engineering

	• Mata-mata ekonomi	• Penembusan atas sistem
Orang dalam Organisasi	• Keingintahuan • Ego • Mata-mata • Balas dendam • Kelalaian kerja	• Surat kaleng • Sabotase atas sistem • Bug sistem • Pencurian/penipuan • Perubahan data • Virus, trojan, dll • Penyalahgunaan komputer

Organisasi yang membutuhkan daftar dari sumber ancaman, perlu melakukan hubungan dengan badan-badan atau sumber-sumber yang berhubungan dengan keamanan, seperti misalnya sumber ancaman dari alam diharapkan hubungan dengan BMG yang menangani masalah alam, atau pihak intelijen atau media massa yang dapat mendeteksi sumber ancaman dari manusia. Hasil output dari ancaman ini merupakan pernyataan atau daftar yang berisikan sumber ancaman yang mungkin dapat mengganggu sistem secara keseluruhan.

Langkah 3. Identifikasi kelemahan

Cacat atau kelemahan dari suatu sistem adalah suatu kesalahan yang tidak terdeteksi yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh sumber ancaman yang mencoba menyusup terhadap sistem tersebut.

Pada beberapa vendor besar, informasi atas kelemahan sistem yang dibuat oleh vendor tersebut ditutup atau dihilangkan dengan penyediaan layanan purna jual dengan menyediakan hot fixes, service pack, pathces ataupun bentuk layanan lain.

Penerapan metode proaktif atau tersedianya karyawan yang bertugas untuk melakukan sistem test dapat di pakai untuk mencek kelemahan sistem secara efisien, dimana hal tersebut tergantung kepada keberadaan sumber daya atau kondisi IT yang bersifat kritis. Metode tes yang diterapkan dapat berbentuk :

- Penggunaan tool yang menscan kelemahan sistem secara automatis
- Adanya Evaluasi dan sekuriti tes (ST&E), atau
- Melakukan penetrasi tes

Penggunaan tools untuk mencek kelemahan sistem diterapkan pada grup perusahaan dengan kelengkapan jaringan komputer yang memadai, yang digunakan untuk memindai beberapa servis sistem yang disinyalir lemah (seperti : Diperbolehkannya anonymous FTP, sendmail automatis, dll). Strategi ST&E merupakan metode tes yang di terapkan pada saat proses penilaian atas resiko dilakukan. Metode ini diterapkan saat pengembangan dan eksekusi atas Sistem Informasi berjalan yaitu pada bagian *test plan*. Kegunaan dari metode ini adalah untuk melihat efektifitas dari kontrol atas sekuriti dari sistem IT terimplementasikan dalam kondisi sistem beroperasi. Penetrasi tes merupakan metode yang digunakan sebagai pelengkap dalam memeriksa kontrol atas sekuriti dan menjamin tidak adanya masalah sekuriti yang mungkin timbul pada sistem IT.

Bentuk keluaran yang timbul pada langkah ketiga ini memungkinkan pihak penilai resiko mendapatkan daftar dari kelemahan sistem yang dapat dianggap sebagai potensi dari sumber ancaman di kemudian hari.

Langkah 4. Analisa pengawasan

Tujuan yang diharapkan pada langkah ini adalah untuk menganalisa penerapan kontrol yang telah diimplementasikan atau yang direncanakan. Bagi organisasi langkah ini perlu untuk meminimalisasi atau bahkan mengeliminasi probabilitas kemungkinan yang timbul dari sumber ancaman atau potensi kelemahan atas sistem.

Metode pengawasan

Metode pengawasan terdiri atas metode yang bersifat teknis maupun non teknis. Metode pengawasan secara teknis merupakan salah satu upaya perlindungan kepada organisasi dalam hal perlindungan terhadap perangkat keras komputer, perangkat lunak maupun mekanisme akses kontrol yang digunakan, sedangkan metode nonteknis lebih ditekankan kepada pengawasan atas manajemen dan operasional penggunaan sistem IT di organisasi tersebut, seperti penerapan policy keamanan, prosedur operasional, maupun manajemen personel yang ada.

Kategori pengawasan

Kategori pengawasan baik secara teknis maupun non teknis dapat diklasifikasikan dalam 2 pendekatan yaitu pendekatan preventif atau detektif.

Pendekatan preventif adalah upaya untuk mencegah upaya pelanggaran atas policy keamanan seperti pengaksesan atas sistem IT atau tindakan lain misalnya dengan cara mengenkripsi informasi atau menerapkan otentifikasi atas informasi.

Pendekatan detektif adalah cara untuk memperingati pengguna atas terjadinya pelanggaran atau percobaan pelanggaran atas policy keamanan yang ada, metode ini contoh pada Microsoft Windows dengan menggunakan teknik audit trails, metode deteksi penyusupan atau teknik checksum.

Teknis analisa pengawasan

Analisa pengawasan atas policy keamanan dapat menggunakan teknik checklist pengguna yang mengakses sistem IT atau dengan penggunaan checklist yang tersedia untuk memvalidasi keamanan, hal paling penting pada tahap ini adalah mengupdate terus menerus atas checklist pengguna sistem untuk mengontrol pemakai.

Hasil yang diharapkan muncul pada tahap ini adalah tersedianya daftar kontrol yang digunakan dan yang sedang direncanakan oleh sistem IT untuk memitigasi kemungkinan adanya kelemahan atas sistem dan memperkecil dampak yang mungkin timbul atas penerapan policy keamanan.

Langkah 5. Menerapkan beberapa kemungkinan

Pada langkah ini, semua skalabilitas kemungkinan yang mungkin timbul dari kelemahan sistem didefinisikan. Terdapat beberapa faktor yang perlu dipertimbangkan dalam upaya mendefinisikan skalabilitas seperti :

- Motif dan kapabilitas dari sumber ancaman
- Kelemahan bawaan dari sistem
- Eksistensi dan efektifitas kontrol yang di terapkan

TIGA JENIS RISIKO AUDIT IT

KELOMPOK 4 :
Yuniarti Denita Sari
Raju Septa Wijaya
Hendri

JENIS RISIKO AUDIT

1. Inherent Risk (IR) / Risiko Bawaan

Adalah risiko yang mungkin timbul akibat karakter bawaan dari suatu transaksi, entah karena:

(a) kompleksitas transaksi dan klas transaksi; atau

(b) kompleksitas perhitungan; atau

(c) aset yg mudah tercuri/digelapkan; atau

(d) ketiadaan informasi yang sifatnya obyektif.

Sudah menjadi pemahaman publik bahwa inherent risk adalah diluar jangkauan auditor dalam melakuk an pencegahan. Bahkan, juga diluar kendali pihak auditee sendiri. Dengan kata lain, auditor hanya bisa menemukan tetapi tidak bisa melakukan apa-apa.

JENIS RISIKO AUDIT

2. Control Risk (CR) / Risiko Pengendalian

Adalah risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, entah karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain—thus tidak mampu mencegah potensi salahsaji bersifat material dan/atau penggelapan (fraud). CR tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee jika mereka mau.

3. Detection Risk (DR) / Risiko Deteksi

Adalah risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud). DR ada dalam kendali auditor. Karena DR sepenuhnya ada pada kendali auditor, maka sudah pasti mereka harus berupaya untuk menekan risiko ini hingga ke tingkatakan yang paling minimal (tidak mungkin menghilangkan risiko ini sepenuhnya).

CONTOH Control Risk (CR) / Risiko Pengendalian

PT Bank Mandiri (Persero) Tbk yang mengalami sistem error yang menyebabkan saldo nasabahnya berubah pada saat proses backup data rutin. Dimana Manajemen Bank Mandiri memastikan bahwa perubahan drastis saldo rekening yang dialami nasabahnya bukan karena penipuan atau fraud. Perubahan saldo terjadi karena sistem error saat proses backup data rutin.

Bila yang terjadi adalah fraud, seharusnya saldo nasabah berkurang. Namun, yang terjadi adalah saldo nasabah ada yang bertambah dan berkurang secara acak (random). Manajemen Bank Mandiri pun menjelaskan kronologi sistem eror yang menyebabkan 10% nasabahnya atau sekitar 1,5 juta nasabah mengalami perubahan saldo. Insiden Bank Mandiri ini dinilai terjadi karena human error, bukan karena kerusakan pada piranti keras atau hardware. Sebab bila terjadi kegagalan pada hardware, proses pemindahan data dari satu perangkat ke perangkat lain semestinya gagal dilakukan.Dengan demikian , perubahan nominal tabungan pada nasabah seharusnya tidak terjadi jika terdapat kerus akan pada hardware.

Perubahan saldo nasabah ini sendiri terjadi pada Sabtu dini hari dibulan Juli. Bermula dari bank yang melakukan proses tutup buku rutin di akhir hari. Saat proses itu berlangsung, data nasabah dipindahkan dalam sebuah backup server. Kemudian, core server memproses transaksi yang terjadi di hari sebelumnya. Namun gangguan itu tidak berpengaruh terhadap transaksi di luar rekening tabungan nasabah, misalnya e-money, pembayaran surat izin mengemudi (SIM), dan sebagainya. Sebab, menurutnya transaksi itu terlepas dari sistem backup data nasabahnya.

PENGENDALIAN DARI CONTOH AUDIT SEBELUMNYA :

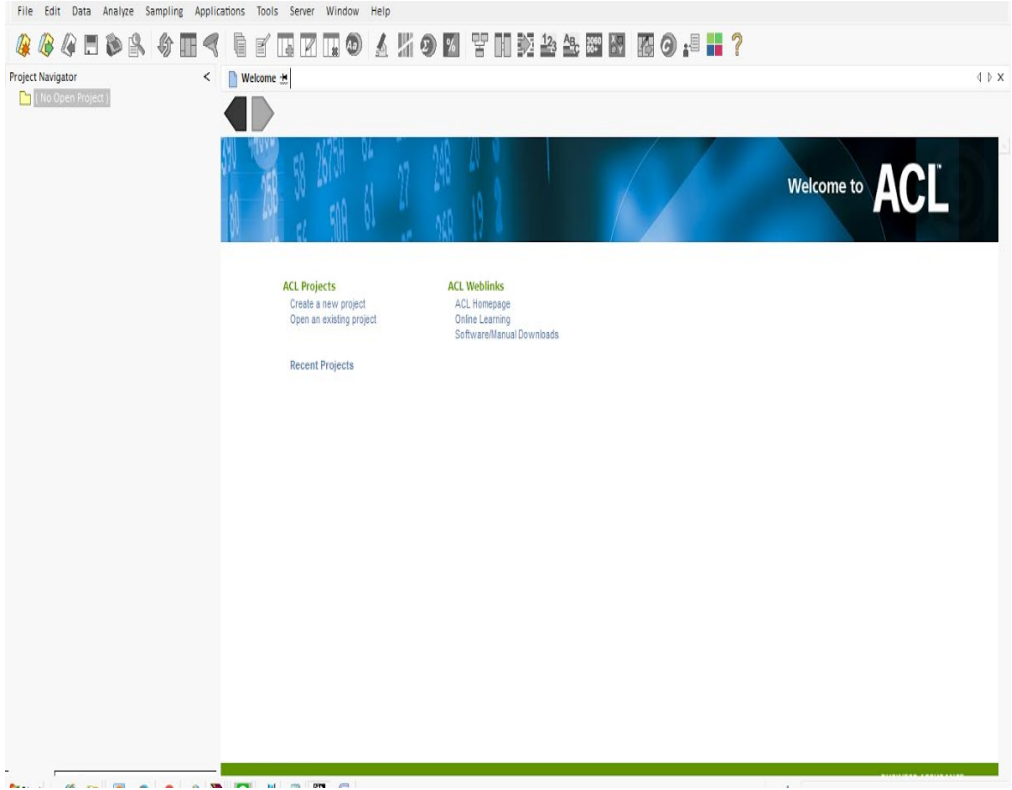
- Perlunya pengecekan secara berlapis (double checking). Dimana sebelum eksekusi perpindahan data, ada orang lain yang melakukan pengecekan ulang lagi (investigasi lebih lanjut, yang diperiksa kembali, apakah memang permasalahan tersebut dari hardware, software, atau human eror).
- Perlunya proses perekrutan pegawai TI sesuai dengan prosedur yang ada.

Tools yang digunakan :

ACL

ACL (Audit Command Language) merupakan sebuah software CAAT (Computer Assisted Audit Techniques) yang sudah sangat populer untuk melakukan analisa terhadap data dari berbagai macam sumber.

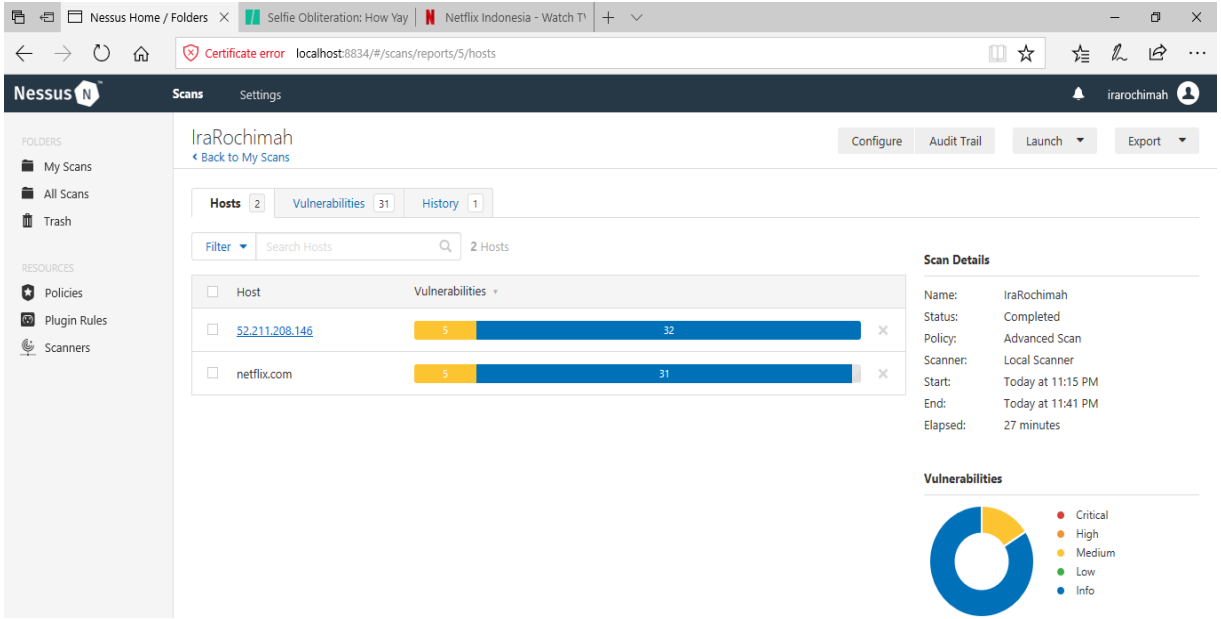
ACL for Windows (sering disebut ACL) adalah sebuah software TABK(TEKNIK AUDIT BERBASIS KOMPUTER) untuk membantu auditor dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik.



Tools yang digunakan :

NESSUS

Nessus adalah termasuk kelompok scanner gratis baru. Nessus bekerja dengan memeri ksa target yang anda telah anda tentukan, seperti Sekumpulan host / bisa juga host dalam fokus tersendiri. Begitu aktivitas scan selesai, anda dapat melihat informasi hasilnya, baik dalam bentuk grafikal atau baris. Interface (tampilan) grafikal Nessus dibangun dengan menggunakan Gimp Toolkit (gtk). Gtk adalah sebuah library gratis yang banyak digunakan untuk membangun interface grafikal dibawah X. Alasan kenapa kebanyakan Administrator Security Computer memilih Nessus adalah karena distribusi aplikasi ini selalu up to date (selalu diperbaharui), berbasis web interface, mudah dioperasikan dan gratis.



Fungsi Nessus yaitu digunakan untuk mencari kelemahan pada sebuah sistem komputer. Nessus juga dapat melakukan pengecekan terhadap kerentanan system komputer, dan meningkatkan keamanan sistem yang kita miliki.

TERIMA KASIH

AUDIT IT

KELOMPOK 5

1. ZENA LUSI
2. TRI AKHYARI ROMADHON
3. ABI DAUD

RESIKO AUDIT IT

- Menurut Peltier dalam Gondodiyoto (2007 : 110), risiko adalah sesuatu yang dapat menciptakan atau menimbulkan bahaya.

- Menurut Peltier (2005: 325), “Risiko adalah kemungkinan adanya kelemehan infrastruktur yang kemudian dimanfaatkan oleh ancaman tertentu yang dipengaruhi eksploitasi tersebut.”

JENIS-JENIS RESIKO

1. Risiko Bawaan (*Inherent Risk*)

Risiko bawaan ialah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan jika tidak ada pengendalian internal.

2. Risiko Pengendalian (*Control Risk*)

Dalam suatu organisasi yang baik seharusnya sudah ada *risk assessment*, dan dirancang pengendalian internal secara optimal terhadap setiap potensi risiko. Risiko pengendalian ialah masih adanya risiko meskipun sudah ada pengendalian

3. Risiko Deteksi (*Detection Risk*)

Risiko deteksi adalah risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya *error* yang cukup matrealitas atau adanya kemungkinan *fraud*.

CONTOH RESIKO AUDIT IT

PENCURIAN DANA DENGAN KARTU ATM PALSU

1. Pembobolan dana rekening tersebut kemungkinan besar dilakukan oleh orang dalam perusahaan atau orang dalam perbankan dan dilakukan lebih dari satu orang.
2. Karena tidak semua pemilik rekening memiliki hubungan dengan perusahaan tersebut, ada kemungkinan pembocoran informasi itu tidak dilakukan oleh satu perusahaan saja, mengingat jumlah dana yang dibobol sangat besar.
3. Modusnya mungkin penipuan berkedok program yang menawarkan keanggotaan. Korban, yang tergoda mendaftar menjadi anggota, secara tidak sadar mungkin telah mencantumkan informasi-informasi yang seharusnya bersifat rahasia.

4. Pelaku kemungkinan memanfaatkan kelemahan sistem keamanan kartu ATM yang hanya dilindungi oleh PIN.

5. Pelaku juga kemungkinan besar menguasai pengetahuan tentang sistem jaringan perbankan. Hal ini ditunjukkan dengan penggunaan teknik yang masih belum diketahui dan hampir bisa dapat dipastikan belum pernah digunakan sebelumnya.

6. Dari rangkuman berita diatas, disebutkan bahwa para pemilik yang uangnya hilang telah melakukan keluhan sebelumnya terhadap pihak bank. Hal ini dapat diartikan bahwa lamanya bank dalam merespon keluhan-keluhan tersebut juga dapat menjadi salah satu sebab mengapa kasus ini menjadi begitu besar.

PENGENDALIAN NYA

- Melakukan perbaikan atau perubahan sistem keamanan untuk kartu ATM. Dengan penggunaan kartu ATM berbasis chip misalnya, yang dirasa lebih aman dari skimming. Atau dengan penggunaan sistem keamanan lainnya yang tidak bersifat PIN, seperti pengamanan dengan sidik jari, scan retina, atau dengan penerapan tanda tangan digital misalnya.

- Karena pembobolan ini sebagiannya juga disebabkan oleh kelengahan pemilik rekening, ada baiknya jika setiap bank yang mengeluarkan kartu ATM memberikan edukasi kepada para nasabahnya tentang tata cara penggunaan kartu ATM dan bagaimana cara untuk menjaga keamanannya.

TOOLS

Metasploit merupakan sofware security yang sering digunakan untuk menguji coba ketahanan suatu sistem dengan cara mengeksploitasi kelemahan software suatu sistem. Metasploit biasanya digunakan untuk menyerang application layer dengan 1day attack yang merupakan metode penyerangan pada software yang belum di patch. Metasploit biasa dikaitkan dengan istilah remote exploitation! maksudnya penyerang berada pada jarak jangkauan yang jauh dapat mengendalikan komputer korban.Metasploit menyerang dengan cara mengirimkan extasploit pada komputer korban. Exploit ini berisi payload yang sudah ditentukan oleh penyerang.

exploit adalah software yang berfungsi untuk memanfaatkan kelemahan pada software korban(misal web browser)! setelah berhasil mengeksploitasinya exploit tersebut memasukkan payload ke dalam memori korban.payload merupakan sebuah executable milik penyerang yang akan di run pada komputer korban dengan tujuan dapat mengendalikan komputer tersebut secara remote atau memasang backdoor! trojan! "irus! worm! dan lain-lain. Terlepas dari penggunaan metasploit yang disalah gunakan untuk kejahatan! software ini juga membantu System Security untuk memperkuat pertahanan jaringannya dari ulah penyerang dari luar.

INHERENT YANG DAPAT TERJADI

1. Kejahatan yang dilakukan dengan menyusup kedalam sistem jaringan komputer tanpa sepengetahuan dari pemilik sistem jaringan komputer. Contohnya : seorang pelaku kejahatan atau hacker melakukan sabotase terhadap informasi yang sangat penting atau mencuri informasi yang sangat penting dan rahasia.
2. Kejahatan dengan memasukkan data atau berupa informasi ke jaringan internet tentang sesuatu yang tidak benar dan melanggar ketentuan hukum. Contohnya pemuatan berita atau informasi yang tidak benar seperti memuat video pornografi, memuat informasi yang sangat rahasia seperti rahasi negara, dll
3. Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan pada dokumen melalu internet.
4. Kejahatan dengan memanfaatkan jaringan internet untuk melakukan mata-mata terhadap pihak yang menjadi sasaran, dengan memasuki sistem jaringan komputer pihak yang menjadi sasarannya.
5. Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau pengahncuran terhadap data atau sistem jaringan komputer. Misalnya menyusupkan virus komputer dimana data yang terkena virus tidak dapat digunakan lagi.

CARA PENGENDALIAN NYA

1. Pengendalian secara umum (General control) yang merupakan pengendalian sistem tekonologi informasi yang paling luar dan harus dihadapi terlebih dahulu oleh pemakai sistem informasi. Beberapa pengendaliannya yaitu : Organisasi, dokumentasi, kontrol pencegah kerusakan perangkat, parameter keamanan data, dll.
2. Pengendalian aplikasi merupakan pengendalian yang dipasang pada pengelolaan aplikasinya yaitu berupa : pengendalian masukan, pengendalian pengolahan, dan pengendalian keluaran.

Threats

1. Boms
2. Thief
3. User Error
4. Breach of contractual relations
5. Social Engginers

Vurnability

Threat	Threat Source	Vulnerability	Impact VS LikeliHood	Risk
Bomb Threats	**Ekternal, Rival**	**Inadequate control of physical access, Inadequate security awareness**	**5 x 1**	**Very Low (5)**
Thieft	**Internal, Ekternal**	**Inadequate control of physical access, Inadequate security awareness**	**5 x 5**	**Very High (25)**
User Error	**Pegawai**	**Inadequate training of employees**	**2 x 5**	**Medium (10)**
Breach Of Contractual Relations	**Organisasi**	**Incomplete specification for software development**	**5 x 2**	**Medium (10)**
Social Enggineering	**Cracker, Hacker**	**Unprotected public network connections**	**5 x 5**	**Very High (25)**

Risiko Audit adalah istilah yang umum digunakan dalam kaitannya dengan audit atas laporan keuangan suatu entitas.
Risiko audit diartikan sebagai tingkat ketidakpastian tertentu yang dapat diterima auditor dalam pelaksanaan auditnya, seperti :

- Ketidakpastian validitas dan reliabilitas bukti audit.
- Ketidakpastian mengenai efektivitas pengendalian internal.

Resiko Audit (*Audit Risk*) adalah resiko bahwa auditor mungkin tanpa sengaja telah gagal untuk memodifikasi pendapat secara tepat mengenai laporan keuangan yang mengandung salah saji material.

Of less concern is the situation where the auditor states that the financial statements do not meet the standard of fair presentation, when in fact they do.. Perhatian kurang adalah situasi di mana auditor menyatakan bahwa laporan keuangan tidak memenuhi standar penyajian secara wajar, padahal sebenarnya mereka lakukan.

Resiko Audit (*Audit Risk*) antara lain :

- **Resiko Inheren (*Inheren Risk*)**

merupakan suatu ukuran yang dipergunakan oleh auditor dalam menilai adanya kemungkinan bahwa terdapat sejumlah salah saji yang material (kekeliruan atau kecurangan) dalam suatu segmen sebelum ia mempertimbangkan keefektifan dan pengendalian intern yang ada. Dengan mengasumsikan tiadanya pengendalian intern, maka risiko inheren ini dapat dinyatakan sebagai kerentanan laporan keuangan terhadap timbulnya salah saji yang material. Jika auditor, dengan mengabaikan pengendalian intern, menyimpulkan bahwa terdapat suatu kecenderungan yang tinggi atas keberadaan sejumlah salah saji, maka auditor akan menyimpulkan bahwa tingkat

risiko inherennya tinggi. pengendalian intern diabaikan dalam menetapkan dalam menetapkan nilai risiko inheren karena pengendalian intern ini dipertimbangkan secara terpisah dalam model risiko audit sebagai risiko pengendalian. Penilaian ini cenderung didasarkan atas sejumlah diskusi yang telah dilakukan dengan pihak manajemen, pemahaman yang dimiliki akan perusahaan, serta hasil-hasil yang diperoleh dari tahun-tahun sebelumnya.

Hubungan antara risiko dengan risiko deteksi terencana serta dengan bukti audit yang direncanakan adalah sebagai berikut : risiko inheren saling berlawanan dengan risiko deteksi terencana serta memiliki hubungan yang searah dengan bukti audit.

Selain semakin meningkatnya bukti audit yang diperlukan untuk suatu tingkat risiko inheren yang lebih tinggi dalam suatu area audit tertentu, merupakan hal yang umum dilakukan pula untuk menugaskan staf yang telah memiliki lebih banyak pengalaman untuk melakukan audit pada area tersebut serta melakukan riview yang lebih mendalam pada kertas kerja yang telah selesai dibuat.

Contoh :

jika risiko inheren atas keusangan persediaan sangat tinggi, maka sangatlah masuk akal bila kantor akuntan publik memilih staf yang berpengalaman untuk melakukan sejumlah tes yang lebih mendalam atas keusangan persediaan ini dan melakukan review yang lebih cermat atas hasil-hasil yang diperoleh dari audit ini.

- **Resiko Pengendalian (*Control Risk*)**

merupakan ukuran yang digunakan oleh auditor untuk menilai adanya kemungkina bahwa terdapat sejumlah salah saji material yang melebihi nilai salah saji yang masi dapat ditoleransi atas segmen tertentu akan tidak terhadang atau tidak terdeteksi oleh

pengendalian intern yang dimiliki klien. Resiko pengendalian ini memperhatikan 2 hal berikut:

1. penilaian tentang apakah pengendalian intern yang dimiliki klien efektif untuk mencegah atau mendeteksi terjadinya salah saji.
2. kehendak auditor membuat penilaian tersebut senantiasa berada di bawah nilai maksimum (100 persen) sebagai bagian dari rencana audit yang dibuatnya.

Model resiko audit menunjukan hubungan yang erat antara resiko inheren dan resiko pengendalian.

Sama dengan yang terjadi pada resiko inheren, hubungan antara resiko pengendalian dan resiko deteksi terencana adalah saling berlawanan, sementara hubungan antara resiko pengendalian dan bukti substantif merupakan hubungan yang searah.

Contoh :

jika auditor menyimpulkan bahwa pengendalian intern bersifat efektif, maka nilai resiko deteksi terencana dapat meningkat sehingga jumlah bukti audit yang direncanakan akan dikumpulkan akan turun. Auditor dapat meningkatkan resiko deteksi terencana pada saat pengendalian intern bersifat efektif karena pengendalian intern yang efektif akan mengurangi kemungkinan hadirnya salah saji dalam laporan keuangan.

Sebelum auditor dapat menetapkan nilai resiko pengendalian kurang dari 100 persen, auditor harus memahami pengendalian intern yang ada, dan berdasarkan pemahaman itu, auditor melakukan evaluasi tentang bagaimana seharusnya fungsi pengendalian intern tersebut, serta melakukan uji atas efektifitas pengendalian intern tersebut. Hal

pertama dari semua ini adalah keharusan untuk memahami semua jenis audit. Dua hal terakhir adalah langkah-langkah penilaian resiko pengendalian yang diperlukan jika auditor memilih untuk memberikan nilai atas resiko pengendalian supaya berada di bawah nilai maksimum

- **Risiko Deteksi Terencana (Planned Detection Risk)**

  merupakan ukuran risiko bahwa bukti audit atas segmen tertentu akan gagal mendeteksi keberadaan salah saji yang melebihi suatu nilai salah saji yang masih dapat ditoleransi, andaikan salah saji semacam itu ada. Terdapat dua poin utama tentang risiko deteksi terencana ini yaitu sebagai berikut :

1. Risiko ini tergantung pada ketiga faktor lainnya yang terdapat dalam model. Risiko deteksi terencana hanya akan berubah jika auditor melakukan perubahan pada salah satu dari ketiga faktor lainnya tersebut.

2. Risiko ini menentukan nilai substantif yang direncanakan oleh auditor untuk dikumpulkan, yang merupakan kebalikan dari ukuran risiko deteksi terencana itu sendiri.

   Jika nilai risiko deteksi terencana berkurang, maka auditor harus mengumpulkan lebih banyak bukti audit untuk mencapai nilai risiko deteksi yang berkurang ini.

RESIKO AUDIT

OLEH
AHKMAD IPANDY
ANGGARI AYU P
ARVIAN AGUSAPUTRA
DEDI ZULKARNAIN

RESIKO AUDIT

risiko salah saji bersifat material dan/atau penggelapan (fraud) yang bisa lolos dari proses audit jika auditor tidak melakukan tugasnya secara cermat. Auditor menyadari bahwa risiko tersebut ada karena adanya hal-hal sebagai berikut, misalnya ketidakpastian mengenai kompetensi bukti, efektivitas struktur pengendalian intern klien, serta ketidakpastian apakah laporan memang telah disajikan secara wajar setelah audit selesai.

Jenis Resiko Audit

RESIKO BAWAAN

Risiko bawaan (Inherent risk) merupakan kerentanan asersi terhadap salah saji (misstatement) yang material, dengan mengasumsikan bahwa tidak ada pengendalian yang berhubungan

RESIKO PENGENDALIAN

risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, entah karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain

RESIKO DITEKSI

risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud)

AUDITOR SALAH MENETAPKAN LANGKAH PENGUJIANNYA (PROSEDUR AUDIT)

prosedur pengeluaran barang menetapkan bahwa setiap pengeluaran barang harus didasarkan pada permintaan dari pihak yang akan menggunakan. Jadi dalam pelaksanaan pengeluaran barang akan terdapat dua populasi bukti yang saling terkait, bukti permintaan barang dan bukti pengeluaran barang.

prosedur audit “periksa apakah atas setiap bukti permintaan barang terdapat bukti pengeluaran barangnya!” Prosedur ini dipastikan tidak akan menemukan kesalahan seperti kecurangan pihak gudang yang mengeluarkan barang walaupun tidak ada permintaan dari pihak yang membutuhkan barang, karena jika ada permintaan barang dapat dipastikan bagian gudang akan menerbitkan bukti pengeluaran barang

prosedur audit yang ditetapkan adalah: “periksa apakah atas setiap bukti pengeluaran barang terdapat bukti permintaan barangnya!” maka prosedur ini mungkin akan dapat menemukan kecurangan bagian gudang atas pengeluaran barang yang tidak didasarkan pada permintaan barang. Dengan prosedur tersebut, jika seandainya bagian gudang melakukan kecurangan mengeluarkan barang tetapi bukan untuk kepentingan perusahaan, maka akan dapat ditemukan dari sampel pengeluaran barang yang tidak ditemukan bukti permintaan barangnya

CONTOH RESIKO DITEKSI

PENGENDALIAN

Aditor memahami prosedur dan dukumen yang akan di audit.

Menggunakan semua dokumen prosedur sebagai bukti untuk dilakukan audit

control

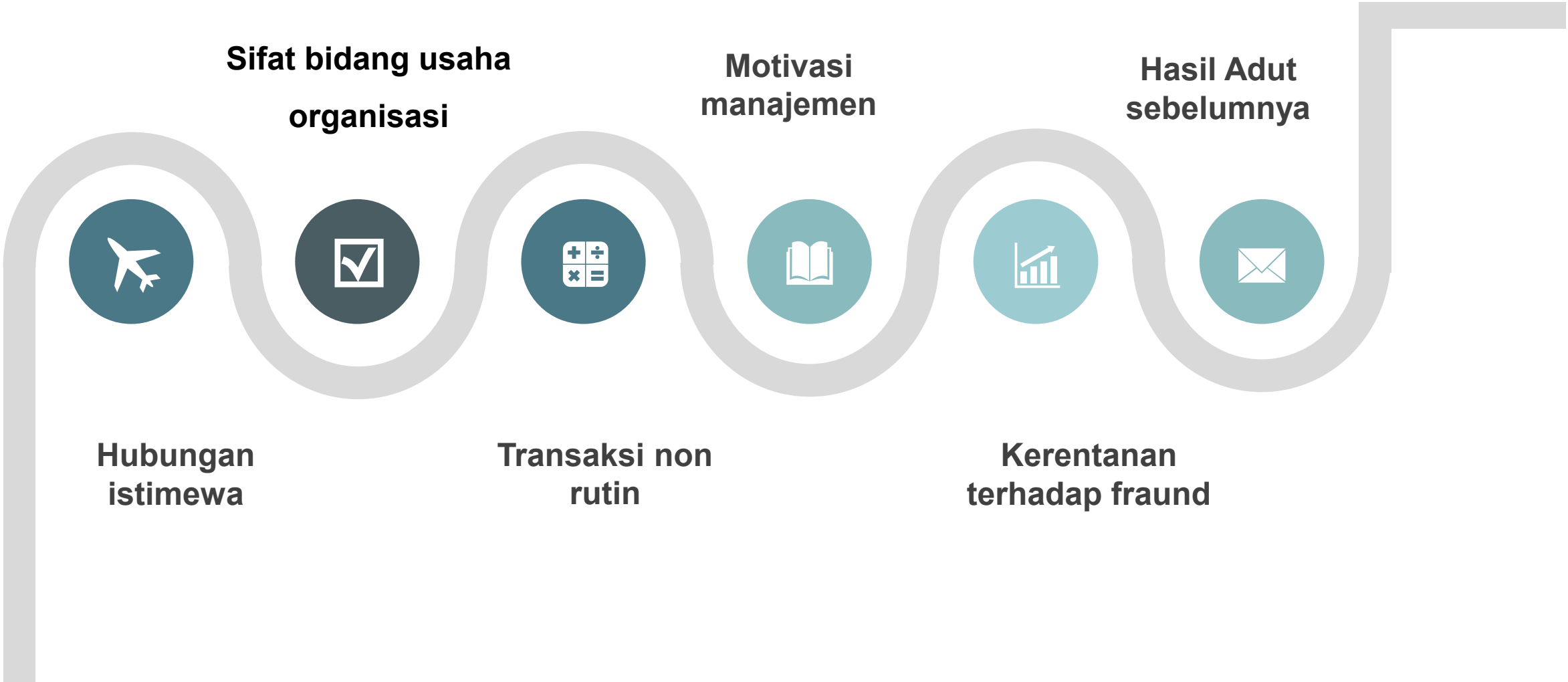
Dilakukan pelatihan bagi auditor, sehingga auditor paham mengenai model risiko audit

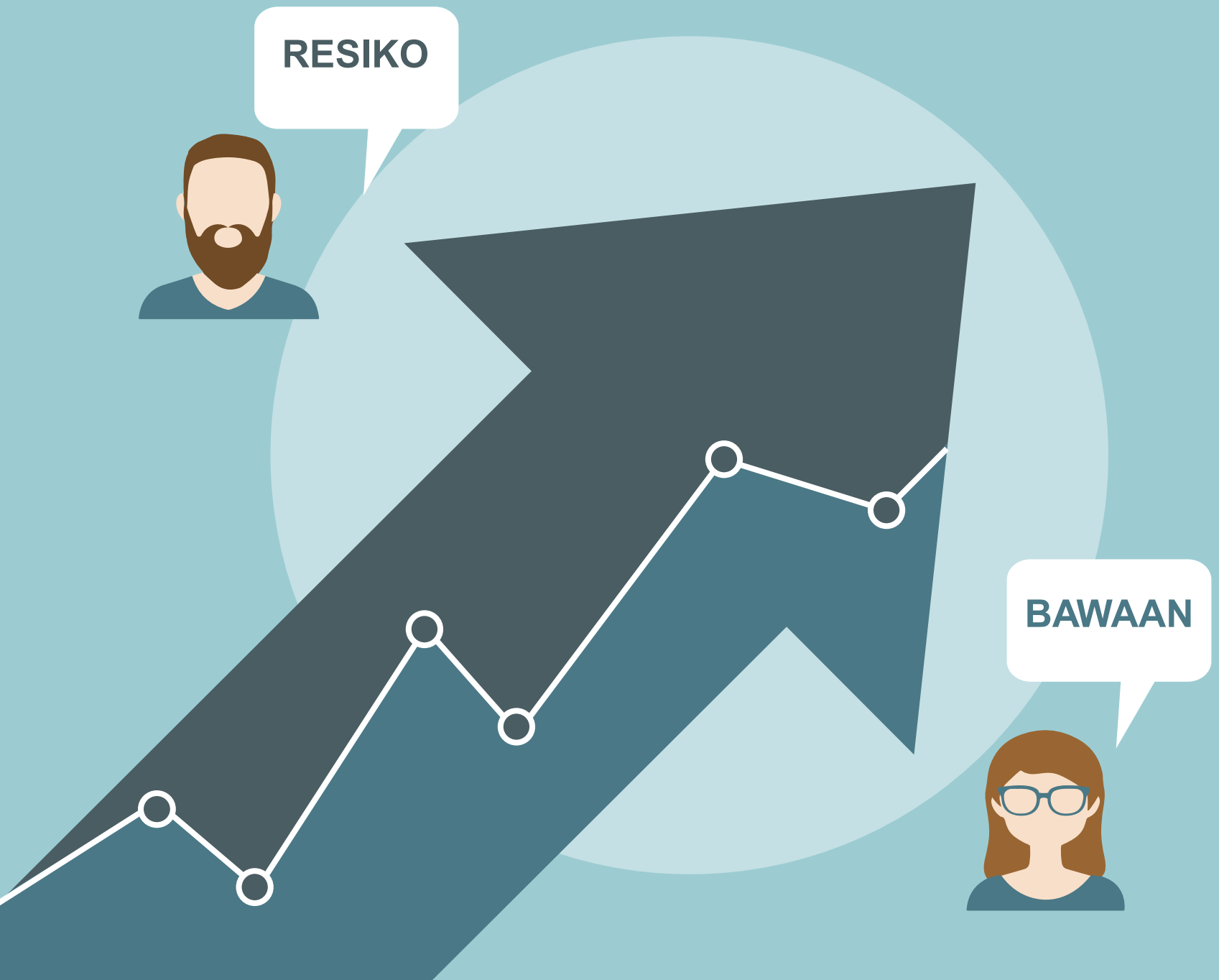
Merancang luasnya pengujian dan menggunakan metode audit yang baik sehingga agar auditor tidak mengalami risiko audit (dalam arti audit menjadi tidak efektif), serta agar audit dapat dilaksanakan secara efisien (dalam arti audit dapat menghindarkan diri, melakukan perluasan pengujian yang tidak perlu).

CONTOH RESIKO BAWAAN

Perhitungan yang rumit lebih mungkin disajikan salah jika dibandingkan dengan perhitungan yang sederhana. Akun yang terdiri dari jumlah yang berasal estimasi akuntansi cenderung mengandung risiko lebih besar dibandingkan dengan akun yang sifatnya rutin dan berisi data berupa fakta.

Faktor-faktor yang perlu ditelaah auditor dalam menetapkan risiko bawaan





Risiko bawaan selalu ada dan tidak pernah mencapai angka nol. Risiko bawaan tidak dapat diubah oleh penerapan prosedur audit yang paling baik sekalipun.

Contoh resiko pengendalian

Audit pada bagian Persediaan.
memeriksa apakah ada 2 pekerjaan terkait atau lebih dirangkap oleh satu orang petugas

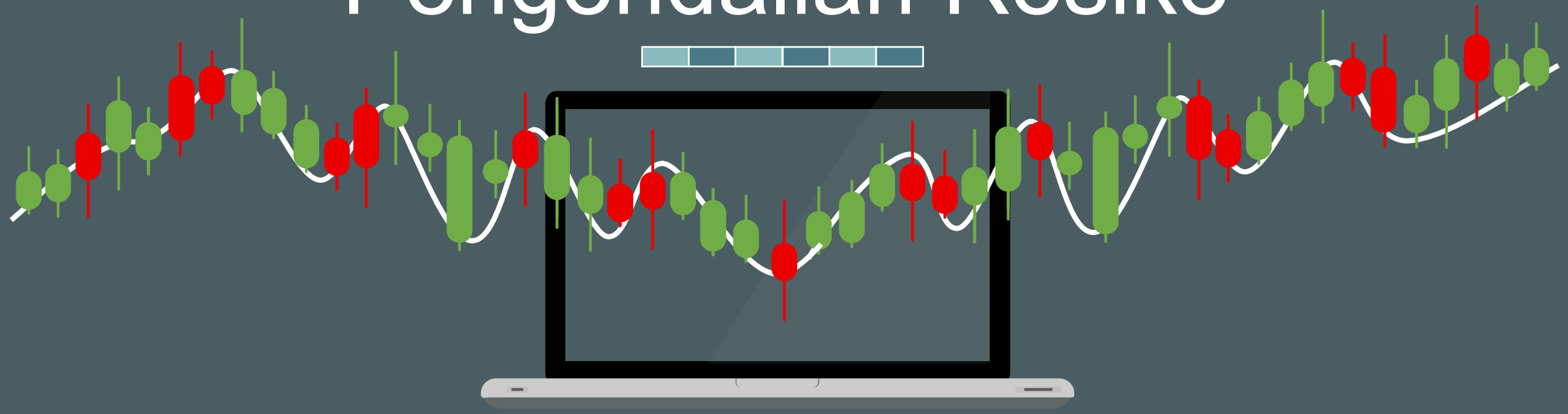
Pegawai Purchasing merangkap sebagai petugas yang penerima barang atau pekerjaan gudang persediaan lainnya (ini buruk); atau Pegawai Shipping merangkap sebagai petugas gudang yang mengurus persediaan barang jadi (ini juga buruk).

Foreman di bagian produksi (yang biasa request persediaan untuk keperluan produksi) diijinkan bebas keluar-masuk gudang persediaan bahan baku atau bahan penolong (ini buruk).

Pegawai admin yang input Receipt of Goods (ROG) memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Payable (Utang)

Pegawai admin yang input picking sheet di Shipping memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Receivable (Piutang).

Pengendalian Resiko



Resiko pengendalian ini tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee

Cara pengedalain resiko :

1. melakukan pembagian tugas yang jelas

2. Melakukan audit internal dan bila diperlukan memiliki bagian audit tersendiri

3. Memperkuat pengawasan manajemen terhadap pegawai

Thank You

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya “scope creep” (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Bagaimana cara mengendaliannya :

Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (*Control Objectives for Information and Related Technology*) adalah standar internasional untuk tata kelola TI

RESIKO AUDIT

OLEH
AHKMAD IPANDY
ANGGARI AYU P
ARVIAN AGUSAPUTRA
DEDI ZULKARNAIN

RESIKO AUDIT

risiko salah saji bersifat material dan/atau penggelapan (fraud) yang bisa lolos dari proses audit jika auditor tidak melakukan tugasnya secara cermat. Auditor menyadari bahwa risiko tersebut ada karena adanya hal-hal sebagai berikut, misalnya ketidakpastian mengenai kompetensi bukti, efektivitas struktur pengendalian intern klien, serta ketidakpastian apakah laporan memang telah disajikan secara wajar setelah audit selesai.

Jenis Resiko Audit

RESIKO BAWAAN

Risiko bawaan (Inherent risk) merupakan kerentanan asersi terhadap salah saji (misstatement) yang material, dengan mengasumsikan bahwa tidak ada pengendalian yang berhubungan

RESIKO PENGENDALIAN

risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, entah karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain

RESIKO DITEKSI

risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud)

AUDITOR SALAH MENETAPKAN LANGKAH PENGUJIANNYA (PROSEDUR AUDIT)

prosedur pengeluaran barang menetapkan bahwa setiap pengeluaran barang harus didasarkan pada permintaan dari pihak yang akan menggunakan. Jadi dalam pelaksanaan pengeluaran barang akan terdapat dua populasi bukti yang saling terkait, bukti permintaan barang dan bukti pengeluaran barang.

prosedur audit “periksa apakah atas setiap bukti permintaan barang terdapat bukti pengeluaran barangnya!” Prosedur ini dipastikan tidak akan menemukan kesalahan seperti kecurangan pihak gudang yang mengeluarkan barang walaupun tidak ada permintaan dari pihak yang membutuhkan barang, karena jika ada permintaan barang dapat dipastikan bagian gudang akan menerbitkan bukti pengeluaran barang

prosedur audit yang ditetapkan adalah: “periksa apakah atas setiap bukti pengeluaran barang terdapat bukti permintaan barangnya!” maka prosedur ini mungkin akan dapat menemukan kecurangan bagian gudang atas pengeluaran barang yang tidak didasarkan pada permintaan barang. Dengan prosedur tersebut, jika seandainya bagian gudang melakukan kecurangan mengeluarkan barang tetapi bukan untuk kepentingan perusahaan, maka akan dapat ditemukan dari sampel pengeluaran barang yang tidak ditemukan bukti permintaan barangnya

CONTOH RESIKO DITEKSI

PENGENDALIAN

Aditor memahami prosedur dan dukumen yang akan di audit.

Menggunakan semua dokumen prosedur sebagai bukti untuk dilakukan audit

control

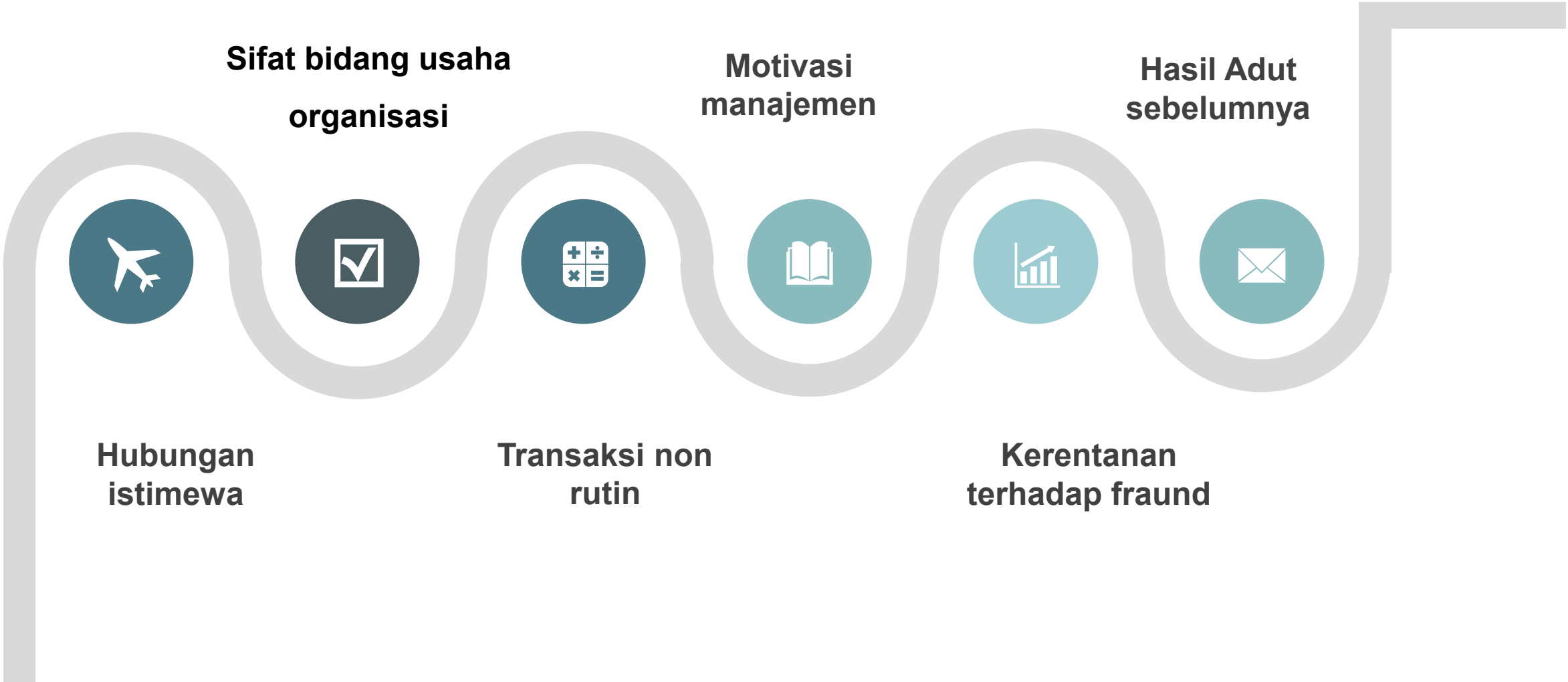
Dilakukan pelatihan bagi auditor, sehingga auditor paham mengenai model risiko audit

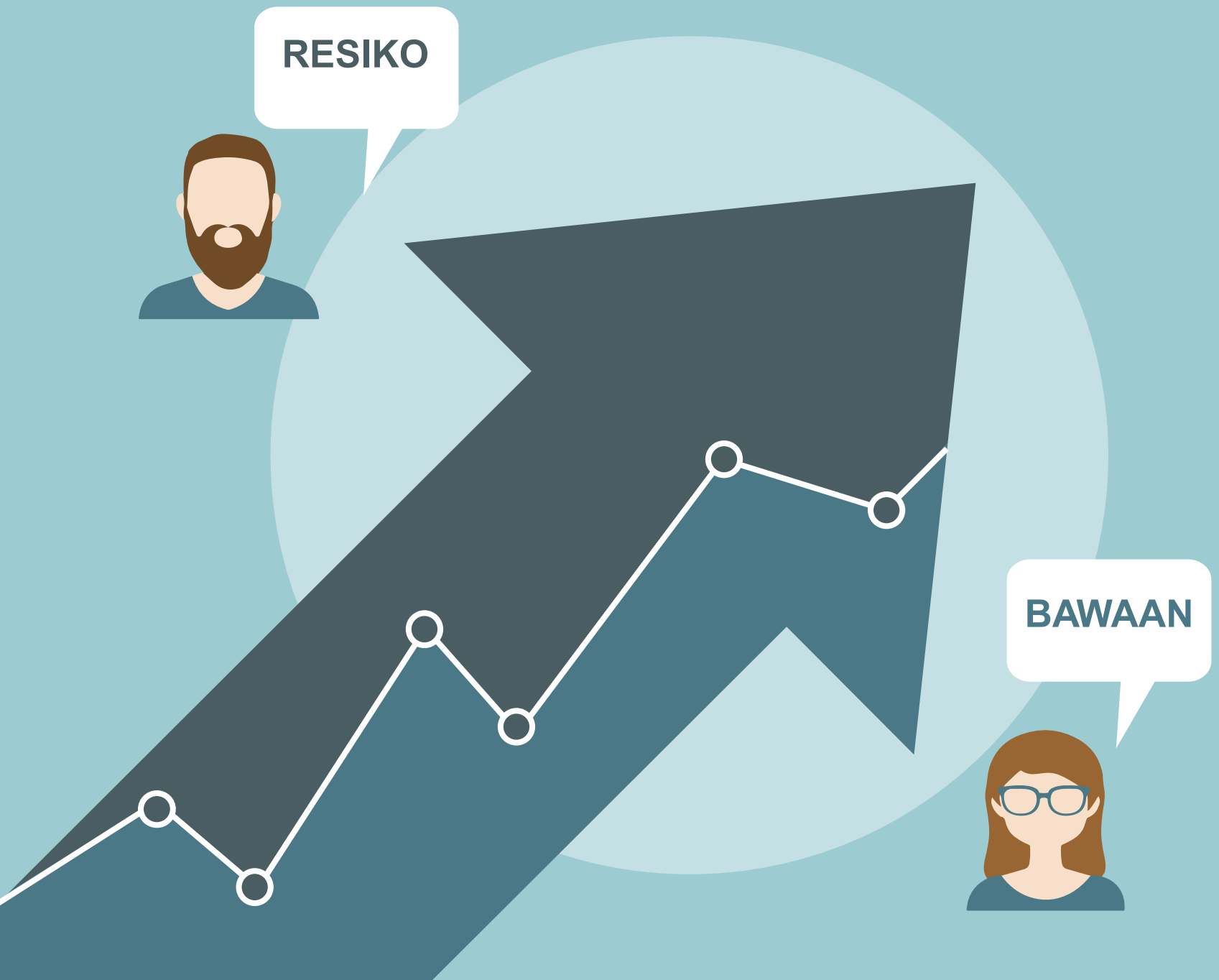
Merancang luasnya pengujian dan menggunakan metode audit yang baik sehingga agar auditor tidak mengalami risiko audit (dalam arti audit menjadi tidak efektif), serta agar audit dapat dilaksanakan secara efisien (dalam arti audit dapat menghindarkan diri, melakukan perluasan pengujian yang tidak perlu).

CONTOH RESIKO BAWAAN

Perhitungan yang rumit lebih mungkin disajikan salah jika dibandingkan dengan perhitungan yang sederhana. Akun yang terdiri dari jumlah yang berasal estimasi akuntansi cenderung mengandung risiko lebih besar dibandingkan dengan akun yang sifatnya rutin dan berisi data berupa fakta.

Faktor-faktor yang perlu ditelaah auditor dalam menetapkan risiko bawaan





Risiko bawaan selalu ada dan tidak pernah mencapai angka nol. Risiko bawaan tidak dapat diubah oleh penerapan prosedur audit yang paling baik sekalipun.

Contoh resiko pengendalian

Audit pada bagian Persediaan.
memeriksa apakah ada 2 pekerjaan terkait atau lebih dirangkap oleh satu orang petugas

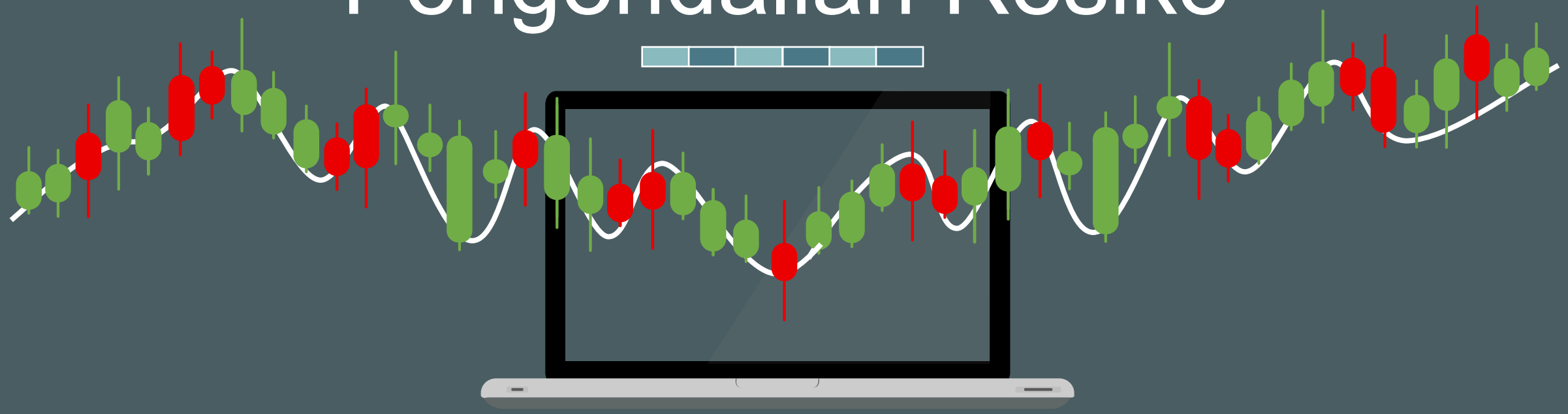
Pegawai Purchasing merangkap sebagai petugas yang penerima barang atau pekerjaan gudang persediaan lainnya (ini buruk); atau Pegawai Shipping merangkap sebagai petugas gudang yang mengurus persediaan barang jadi (ini juga buruk).

Foreman di bagian produksi (yang biasa request persediaan untuk keperluan produksi) diijinkan bebas keluar-masuk gudang persediaan bahan baku atau bahan penolong (ini buruk).

Pegawai admin yang input Receipt of Goods (ROG) memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Payable (Utang)

Pegawai admin yang input picking sheet di Shipping memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Receivable (Piutang).

Pengendalian Resiko



Resiko pengendalian ini tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee

Cara pengedalain resiko :

1. melakukan pembagian tugas yang jelas

2. Melakukan audit internal dan bila diperlukan memiliki bagian audit tersendiri

3. Memperkuat pengawasan manajemen terhadap pegawai

Thank You

PROFESIONAL INDEPENDEN

OLEH

AHKMAD IPANDY
ANGGARI AYU P
ARVIAN AGUSAPUTRA
DEDI ZULKARNAIN

ITAF

01 Standar umum

02 Standar kerja

03 Standar pelaporan

Standsart Umum

Bahwa seoarang auditor dan penjamin SI harus harus independen dan obyektif dalam sikap dan penampilan dalam semua hal yang berkaitan dengan audit dan pemeriksaan

SIKAP AUDITOR DAN PEJAMIN MUTU

1. Melakukan audit atau pemeriksaan dengan kerangka pikir yang adil dan tidak memihak dalam menyikapi masalah jaminan dan mencapai kesimpulan.
2. Harus Independen sebenarnya, walapun terkadang tidak selalu harus independen setiap saat.
3. Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat
4. Menilai independensi secara teratur dengan manajemen dan komite audit, jika ada.
5. Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen karenanya peran tersebut dapat merusak independensi di masa depan.

PEDOMAN AUDIT

TUJUAN

1. Mengetahui kapan seorang audit dan penjamin merasa dalam kondisi ke-indipenenannya terancam atapun terganggu.
2. Melakukan suatu pendekatan alternative ketika proses audit berjalan dan ke-indipenenannya sedang dan atau mungkin terganggu.
3. Mengurangi atau menghilangkan dampak akibat ke-indipenenan audit SI dan kinerja professional seorang penjamin, peran, fungsi dan layanan non audit
4. Menentukan persyaratan untuk penilaian ketika ke-indipenenan merasa terganggu

JENIS ANCAMAN

1. Kerangka kerja konseptual
2. Ancaman dan perlindungan
3. Mengelola ancaman
4. Layanan atau peran non-audit
5. Layanan atau peran non-audit yang tidak mengganggu independensi
6. Layanan atau peran non-audit yang merusak independensi
7. Relevans
8. i independensi ketika memberikan layanan atau peran non-auditTata kelola penerimaan layanan atau peran non-audit
9. Pelaporan

KERANGKA KERJA KONSEPTUAL

Pedoman ini menetapkan kerangka kerja konseptual yang membutuhkan profesional untuk mengidentifikasi, mengevaluasi, dan menangani ancaman terhadap independensi. Kerangka kerja konseptual pendekatan membantu dalam mematuhi standar independensi, dan mengakomodasi banyak variasi dalamkeadaan yang menciptakan ancaman bagi kemerdekaan

JENIS ANCAMAN

1. Kepentingan pribadi
2. Tinjauan diri sendiri
3. Advokasi
4. Keakraban
5. Intimidasi
6. Bias
7. Partisipasi manajemen

ANCAMAN DAN PERLINDUNGAN

ANCAMAN

Ancaman dapat diciptakan oleh berbagai hubungan dan keadaan. Ketika suatu hubungan atau keadaan menciptakan ancaman, ancaman seperti itu dapat merusak, atau bisa dianggap merusak, keprofessionalan independen.

PERLINDUNGAN

kontrol yang dirancang untuk menghilangkan ancaman terhadap independensi atau menguranginnya.

PERLINDUNGAN

Sruktur tata kelola di perusahaan dan fungsi audit yang menyediakan pengawasan dan komunikasi mengenai audit SI dan layanan jaminan yang akan dilakukan

Memastikan bahwa profesional (dan manajemen audit IS) melapor ke tingkat hierarki yang memadai dalam perusahaan, terutama yang bertanggung jawab atas tata kelola

Prosedur internal di perusahaan dan fungsi audit yang memastikan pilihan obyektif dalam penugasan keterlibatan, misalnya, persyaratan pendidikan, pelatihan dan

Menugaskan manajemen dan staf dari luar fungsi audit, seperti meminjam staf dari yang lain fungsi, divisi, organisasi eksternal, untuk melengkapi para professional

Infographic Style

01

DOKUMENTASI

02

Your
Contents Here

03

Your
Contents Here

04

Your
Contents Here

05

Your
Contents Here

Columns Layout

ALLPPT Layout
Clean Text Slide for your Presentation

01

Easy to change colors, photos and Text.

Easy to change colors, photos and Text. Get a modern PowerPoint Presentation that is beautifully designed. I hope and I believe that this Template will your Time, Money and Reputation. Easy to change colors, photos and Text. You can simply impress your audience and add a unique zing and appeal to your Presentations.

Get a modern PowerPoint Presentation that is beautifully designed.

02

Easy to change colors, photos and Text.

Easy to change colors, photos and Text. Get a modern PowerPoint Presentation that is beautifully designed. I hope and I believe that this Template will your Time, Money and Reputation. Easy to change colors, photos and Text. You can simply impress your audience and add a unique zing and appeal to your Presentations.

Get a modern PowerPoint Presentation that is beautifully designed.

Columns Layout

This PowerPoint Template has clean and neutral design that can be adapted to any content and meets various market segments.

Your Text Here

Easy to change colors, photos and Text. Get a modern PowerPoint Presentation that is beautifully designed. I hope and I believe that this Template will your Time, Money and Reputation. You can simply impress your audience and add a unique zing and appeal to your Presentations.

Get a modern PowerPoint Presentation that is beautifully designed. You can simply impress your audience and add a unique zing and appeal to your Presentations.

Your Text Here

Easy to change colors, photos and Text. Get a modern PowerPoint Presentation that is beautifully designed. I hope and I believe that this Template will your Time, Money and Reputation. You can simply impress your audience and add a unique zing and appeal to your Presentations.

Get a modern PowerPoint Presentation that is beautifully designed. You can simply impress your audience and add a unique zing and appeal to your Presentations.

Thank You

Insert the Sub Title of Your Presentation

Fully Editable Shapes

Fully Editable Icon Sets: A

You can Resize without losing quality

You can Change Fill Color &
Line Color

FREE PPT TEMPLATES

www.allppt.com

Fully Editable Icon Sets: B

You can Resize without losing quality

You can Change Fill Color &
Line Color

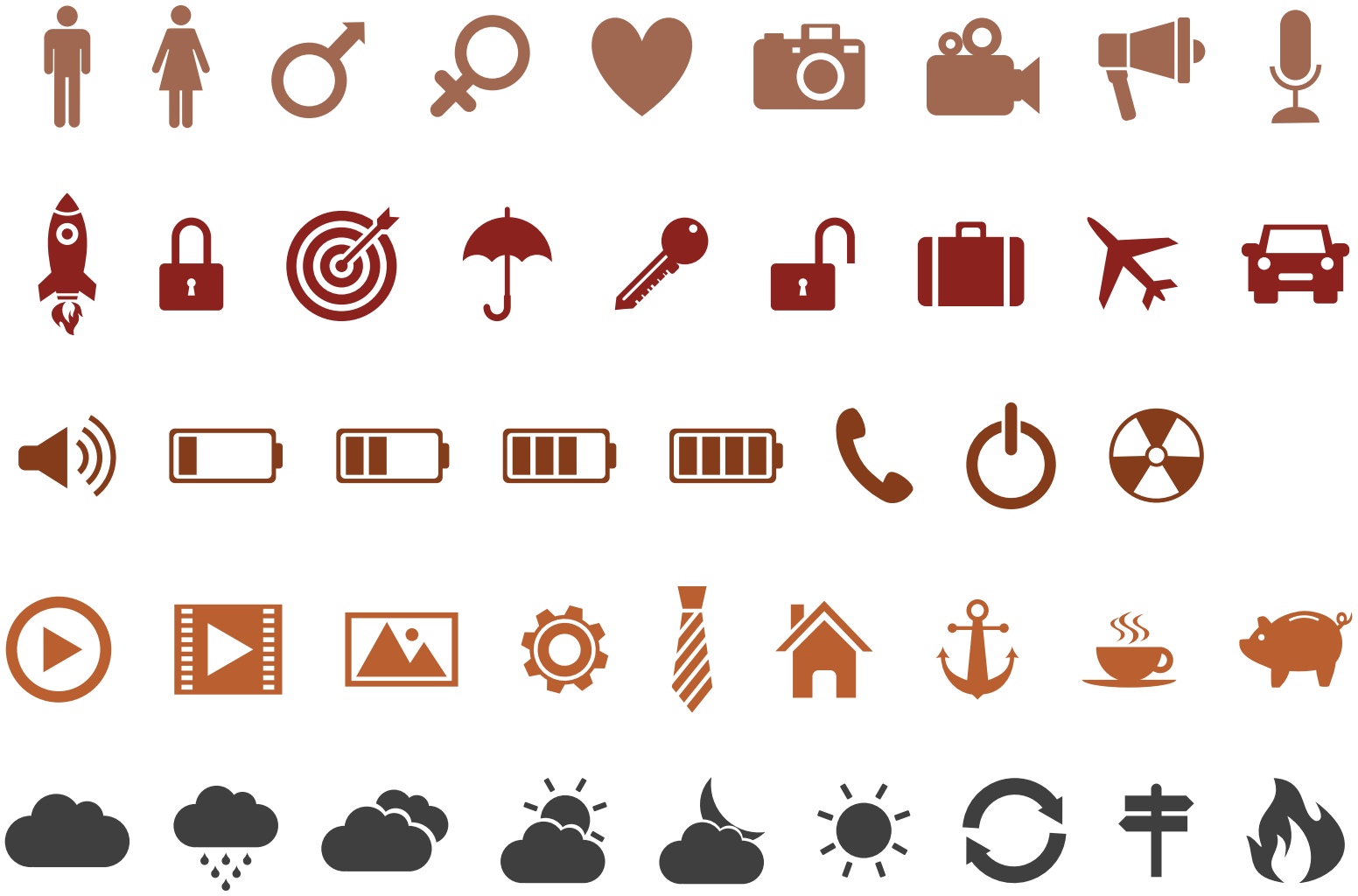
FREE PPT TEMPLATES

www.allppt.com

Fully Editable Icon Sets: C

You can Resize without losing quality

You can Change Fill Color &
Line Color



FREE PPT TEMPLATES

www.allppt.com

Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

1. Email password may be disclosed
2. Facebook account may be used by someone else
3. Credit card information may be disclosed
4. Customer information may be stolen
5. IT Service delivery to the customers may be poor may be poor
6. IT systems may be obsolete
7. IT projects may be late or fail
8. IT systems do not provide any business benefit
9. Risk of non-compliance with the regulator
10. Own people may harm the systems

Jelaskan bagaimana resiko-resiko tersebut dikendalikan (lihat contoh Risk Management Framework yang terlampir?

Dengan menggunakan COBIT pengendalian risiko meliputi :

1. **PLAN & ORGANISE**
   - Strategic IT Plan
   - Manage IT Investment
   - Manage IT Human Resources
   - Manage IT Risks
   - Manage Project
2. **ACQUIRE & IMPLEMENT**
   - Acquire & Maintain Application Software
   - Acquire and Maintain Technology Infrastructure
   - Manage Changes
3. **DELIVERY & SUPPORT**
   - Manage Third-party Services
   - Ensure Continuous Service
   - Ensure Systems Security
   - Manage Incidents
   - Manage data
   - Manage Operations
4. **MONITOR & EVALUATE**
   - Monitor and Evaluate IT Performance
   - Monitor and Evaluate Internal Control
   - Ensure Compliance
   - Provide IT Governance

Kemudian membuat RACI chart mengidentifikasi siapa yang **Responsible, Accountable, Consulted and/or Informed.**

Resiko Audit IT

By : Dedy Zulkarnain
182420080

Penilaian risiko

Penilaian risiko untuk tujuan pelaporan keuangan adalah identifikasi analisis dan pengelolaan risiko suatu entitas yang relevan dengan penyusunan laporan keuangan yang disajikan secara wajar sesuai dengan prinsip-prinsip akuntansi yang berlaku umum. Penilaian risiko oleh manajemen juga harus mencakup pertimbangan khusus atas risiko yang dapat muncul dari perubahan kondisi seperti yang diuraikan dalam AU 319.29:

- Perubahan dalam lingkungan operasi
- Personel baru
- Sistem informasi yang baru atau dimodifikasi
- Pertumbuhan yang cepat
- Teknologi baru
- Lini, produk, atau aktivitas baru
- Restrukturisasi perusahaan
- Operasi di luar negeri
- Pernyataan tentang pengertian akuntansi

Aktivitas pengendalian

Aktivitas pengendalian adalah kebijakan dan prosedur yang membantu meyakinkan bahwa perintah manajemen telah dilaksanakan. Mereka membantu memastikan bahwa tindakan yang diperlukan telah diambil untuk mengatasi risiko terhadap pencapaian tujuan entitas.

Aktivitas pengendalian yang relevan dengan pengertian dan jenis-jenis audit laporan keuangan dapat dikategorikan dalam berbagai cara. Salah satu cara adalah sebagai berikut :

- Pengendalian otorisasi
- Pemisahan tugas
- Pengendalian pemrosesan informasi meliputi pengendalian umum, pengendalian aplikasi, pengendalian atas proses pelaporan keuangan, pengendalian fisik, review kinerja dan pengendalian atas manajemen kebijaksanaan dalam pelaporan keuangan.

- **Tujuan Audit Teknologi Informasi adalah:**
- Memahami Peran Auditor TI dan Lingkungannya
  - Departemen Internal Audit
  - Organisasi
  - Finansial, Operasional dan Teknologi
  - Tujuan Audit Teknologi Informasi (TI)
- Menguasai Framework COBIT
  - Ruang Lingkup COBIT
  - Menggunakan Control Objectives COBIT
  - Memahami Control Maturity Model
- Memahami dan Menguasai Manajemen TI
  - Tata Kelola dan Dukungan Manajemen Serta Eksekutif Perusahaan
  - Manajemen TI, Struktur dan Budaya Departement TI
  - Memahami Manajemen Resiko
- Menguasai Manajemen Konfigurasi Perangkat Keras dan Pengembangan Sistem
  - Konfigurasi Server
  - Konfigurasi Workstation
  - Framework Pengembangan Sistem
  - Menggunakan SDLC dalam Manajemen Proyek
  - Memahami Fungsi Project Management Office (PMO)

- Menguasai Manajemen Data dan Perubahan
  - Memahami Konsep Basis Data Relasional
  - Memahami Media Penyimpanan, Jenis dan Tipe Akses
  - Menguasai Klasifikasi dan Perlindungan Data
  - Memahami Pengendalian Library Perangkat Lunak
  - Menguasai Penyelarasan Antara Library Kode Sumber dan Executable
  - Menguasai manajemen patch
- Menguasai Manajemen Jaringan dan Keamanan Informasi
  - Memahami Konsep Jaringan dan Firewall
  - Menguasai Manajemen Konfigurasi Jaringan
  - Menguasai Teknik Mengawasi Intrusion Detection dan Penetration Testing
  - Memahami dan Menguasai Kebijakan Keamanan Informasi
  - Mengawasi Implementasi Keamanan Informasi
  - Memahami Standar ISO27002
- Menguasai Manajemen IT Contingency
  - Memahami Business Continuity dan Disaster Recovery
  - Menjalankan Rencana Business Continuity dan Disaster Recovery
  - Mengawasi Implementasi Business Continuity dan Disaster Recovery
- Memahami IT Outsourcing
- Memilih dan Menggunakan Jasa Outsourcing
- Mengawasi, Memeriksa Aktivitas Outsourcing
- Melakukan Review Atas Jasa Outsourcing

Metode Audit Teknologi Informasi adalah:

- Data Pengujian
- Pendekatan Fasilitas Uji Terintegrasi (ITF)
- Simulasi Paralel
- Perangkat Lunak Audit
- Generalized Audit Software (GAS)
- PC Software (ACL Software)
- Embedded Audit Routine
- Extended Record
- Snapshot
- Tracing
- Dokumentasi Tinjauan Sistem
- Flowchart Pengendalian
- Mapping (pemetaan)

- **Studi Kasus: Pencurian Dana dengan Kartu ATM Palsu**
  Jakarta (ANTARA News) – Sekitar 400 juta yen (Rp.44 miliar) deposito di enam bank di Jepang telah ditarik oleh kartu-kartu ATM palsu setelah informasi pribadi nasabah dibocorkan oleh sebuah perusahaan sejak Desember 2006, demikian harian Yomiuri Shimbun dalam edisi onlinenya, Rabu.
- Bank-bank yang kini sedang disidik polisi adalah Bank Chugoku yang berbasis di Okayama, North Pasific Bank, Bank Chiba Kogyo, Bank Yachiyo, Bank Oita, dan Bank Kiyo. Polisi menduga para tersangka kriminal itu menggunakan teknik pemalsuan baru untuk membuat kartu ATM tiruan yang dipakai dalam tindak kriminal itu. Pihak Kepolisian Metropolitan Tokyo meyakini kasus pemalsuan ATM ini sebagai ulah komplotan pemalsu ATM yang besar sehingga pihaknya berencana membentuk gugus tugas penyelidikan bersama dengan satuan polisi lainnya.

  Berdasarkan sumber kepolisian dan bank-bank yang dibobol, sekitar 141 juta yen tabungan para nasabah telah ditarik dari 186 nomor rekening di North Pasific Bank antara 17–23 Oktober 2007. Para nasabah bank-bank itu sempat mengeluhkan adanya penarikan-penarikan dana dari rekening mereka tanpa sepengetahuan mereka. Kejadian serupa ditemukan di bank Chugoku dan Bank Chiba. Dalam semua perkara itu, dana tunai telah ditarik dari gerai-gerai ATM di Tokyo dan Daerah Administratif Khusus Osaka, yang letaknya jauh dari tempat para pemilik rekening yang dibobol. Polisi yakin peristiwa serupa menimpa bank-bank lainnya.

PENYELESAIAN MASALAH

yaitu :

- Skills Kemampuan yang diberikan harus sesuai dengan bidang kerja yang ia lakukan.Kemudian kemampuan tersebut dikembangkan lebih lanjut untuk meningkatkankontribusi karyawan pada perusahaan.Perusahaan melakukan pelatihan pendidikan secara periodik kepada karyawan sesuaidengan perkembangan teknologi yang berkembang.
- Pembinaan ini sangatlah penting karena setiap karyawan memiliki kepribadian yangberbeda jadi attitude ini harus ditekankan kepada karyawan. Dalam hal ini karyawandiharapkan dapat memiliki kepribadian yang baik sehingga dapat memperkecil resikoterjadinya penyimpangan dari karyawan itu sendiri.

2 Prosedur Otoritas Yang Wajar

a) Harus ada batas transaksi untuk masing-masing teller dan head teller.

b) Penyimpanan uang dalam khasanah harus menggunakan pengawasan ganda.

c) Teller secara pribadi tidak diperkenankan menerima kuasa dalam bentuk apapundari nasabah untuk melaksanakan transaksi atas nasabah tersebut.

d) Teller secara pribadi dilarang menerima titipan barang atau dokumen pentingmilik nasabah.

- Uniknya, tidak satu pun dari para pemilik rekening itu kehilangan kartu ATM-nya. Dalam kasus Bank Oita misalnya, salah satu kartu ATM telah digunakan untuk menarik dana meskipun pemilik rekening tidak memiliki kartu ATM. Para pemilik rekening juga diketahui tinggal di tempat yang berbeda-beda dan tidak menggunakan kartu-kartu ATM yang sama. Hal ini menunjukkan bahwa teknik "skimming" atau "pembacaan sepintas" tidak digunakan untuk mengakses informasi dalam ATM.
- Sampai berita ini diturunkan, polisi masih menyelidiki teknik dan metode yang pelaku gunakan dalam melakukan serangkaian pembobolan ATM tersebut. Namun, polisi telah berhasil menemukan satu benang merah, yaitu dimana sebagian besar pemilik rekening yang dibobol itu adalah anggota satu program yang dijalankan olah sebuah perusahaan penjual produk makanan kesehatan yang berbasis di Tokyo.

- **Analisa Kasus:**
- Dari rangkuman berita diatas, dapat ditarik beberapa kesimpulan, antara lain :
- · Pembobolan dana rekening tersebut kemungkinan besar dilakukan oleh orang dalam perusahaan atau orang dalam perbankan dan dilakukan lebih dari satu orang.
- · Karena tidak semua pemilik rekening memiliki hubungan dengan perusahaan tersebut, ada kemungkinan pembocoran informasi itu tidak dilakukan oleh satu perusahaan saja, mengingat jumlah dana yang dibobol sangat besar.
- · Modusnya mungkin penipuan berkedok program yang menawarkan keanggotaan. Korban, yang tergoda mendaftar menjadi anggota, secara tidak sadar mungkin telah mencantumkan informasi-informasi yang seharusnya bersifat rahasia.
- · Pelaku kemungkinan memanfaatkan kelemahan sistem keamanan kartu ATM yang hanya dilindungi oleh PIN.
- · Pelaku juga kemungkinan besar menguasai pengetahuan tentang sistem jaringan perbankan. Hal ini ditunjukkan dengan penggunaan teknik yang masih belum diketahui dan hampir bisa dapat dipastikan belum pernah digunakan sebelumnya.
- · Dari rangkuman berita diatas, disebutkan bahwa para pemilik yang uangnya hilang telah melakukan keluhan sebelumnya terhadap pihak bank. Hal ini dapat diartikan bahwa lamanya bank dalam merespon keluhan-keluhan tersebut juga dapat menjadi salah satu sebab mengapa kasus ini menjadi begitu besar.

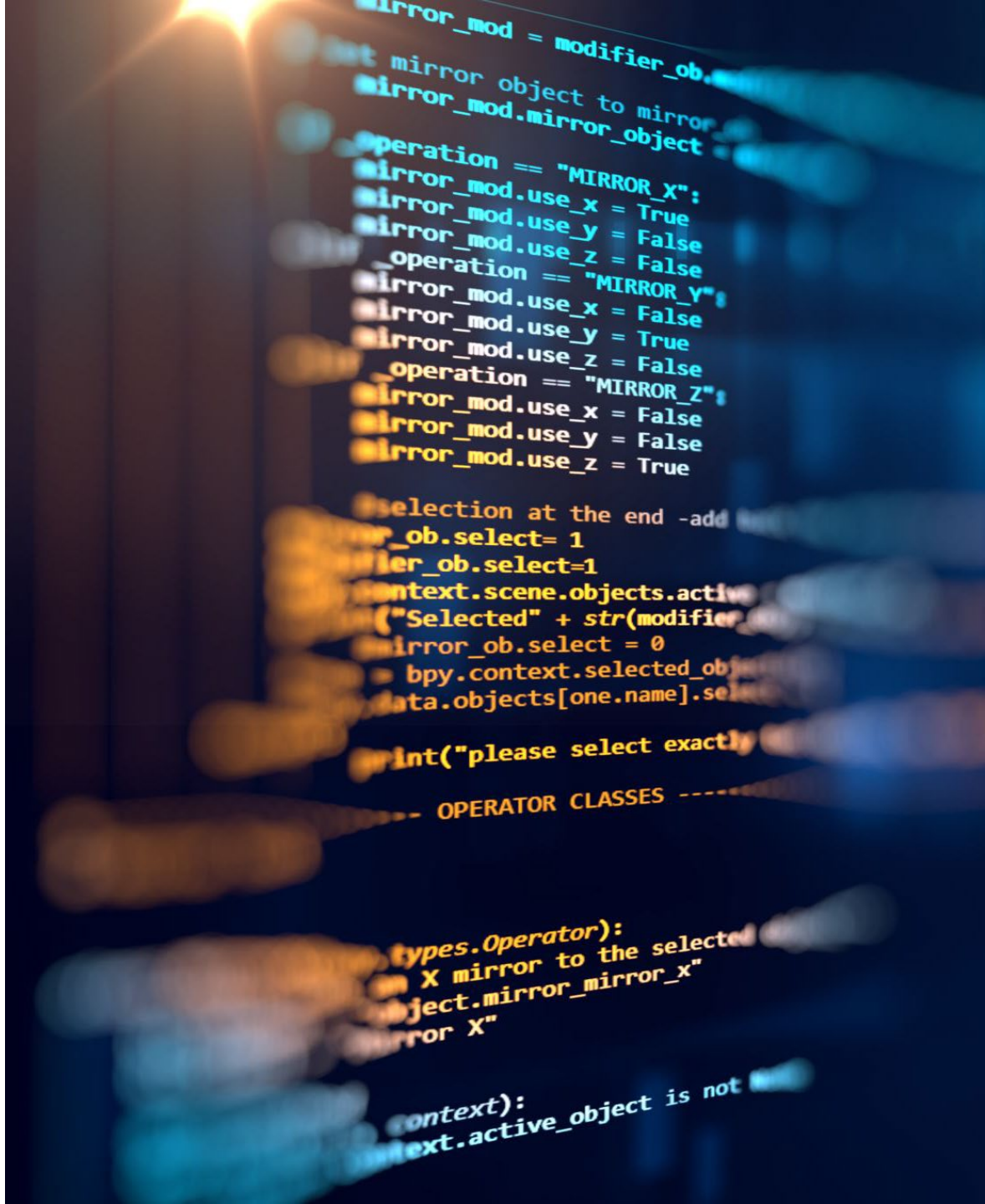
Dari segi sistem keamanan kartu ATM itu sendiri, terdapat 2 kelemahan, yaitu:

- 1. Kelemahan pada mekanisme pengamanan fisik kartu ATM.
  Kartu ATM yang banyak digunakan selama ini adalah model kartu ATM berbasis pita magnet. Kelemahan utama kartu jenis ini terdapat pada pita magnetnya. Kartu jenis ini sangat mudah terbaca pada perangkat pembaca pita magnet (skimmer).
- 2. Kelemahan pada mekanisme pengamanan data di dalam sistem.
  Sistem pengamanan pada kartu ATM yang banyak digunakan saat ini adalah dengan penggunaan PIN (Personal Identification Number) dan telah dilengkapi dengan prosedur yang membatasi kesalahan dalam memasukkan PIN sebanyak 3 kali yang dimaksudkan untuk menghindari brute force. Meskipun dapat dikatakan cukup aman dari brute force, mekanisme pengaman ini akan tidak berfungsi jika pelaku telah mengetahui PIN korbannya.
-
- **Saran:**
- · Melakukan perbaikan atau perubahan sistem keamanan untuk kartu ATM. Dengan penggunaan kartu ATM berbasis chip misalnya, yang dirasa lebih aman dari skimming. Atau dengan penggunaan sistem keamanan lainnya yang tidak bersifat PIN, seperti pengamanan dengan sidik jari, scan retina, atau dengan penerapan tanda tangan digital misalnya.
- · Karena pembobolan ini sebagiannya juga disebabkan oleh kelengahan pemilik rekening, ada baiknya jika setiap bank yang mengeluarkan kartu ATM memberikan edukasi kepada para nasabahnya tentang tata cara penggunaan kartu ATM dan bagaimana cara untuk menjaga keamanannya.

TERIMA KASIH

SOFTWARE IT AUDIT

Manage Engine AD Audit Plus



JENIS RESIKO AUDIT

Control Risk (Risiko Pengendalian)
Adalah ukuran penetapan auditor akan kemungkinan adanya kekeliruan (salah saji) dalam segmen audit yang melampaui batas toleransi yang tidak terdeteksi atau tercegah oleh struktur pengendalian intern klien.

SALAH SATU RESIKO YANG MUNGKIN MUNCUL DI BIDANG IT

Data Breach

merupakan salah satu jenis serangan cyber yang dapat mengancam bisnis Anda. Data breach atau pelanggaran data merupakan suatu kondisi di mana hacker mampu menyusup masuk ke dalam sistem dan mengekstraksi data-data penting di dalamnya.

Hal ini mampu membawa berbagai dampak negatif untuk bisnis, mulai dari tercurinya data-data sensitif sampai hilangnya kepercayaan pelanggan. Untuk menghindarinya,

APA SAJA YANG DAPAT MENYEBABKAN DATA BREACH DAPAT TERJADI.

1. **Kredensial yang lemah**

Kredensial atau kata sandi yang lemah menjadi salah satu penyebab data breach dapat terjadi. Kata sandi dibuat dengan tujuan untuk mengamankan sistem. Namun sayangnya masih banyak yang menggunakan kata sandi dengan frasa sederhana seperti Password1 atau 123456. Jika hacker dapat menemukan kata sandi yang Anda gunakan, mereka dapat dengan mudah masuk ke dalam sistem dan mengakses data-data sensitif di dalamnya. Oleh karena itu, penting bagi perusahaan untuk selalu menggunakan kata sandi yang kuat dan secara regular memperbaruinya.

2. **Adanya kerentanan di dalam aplikasi**

Sebagian besar hacker akan melakukan sejumlah serangan ketika mereka menemukan kerentanan dalam sebuah sistem. Itulah sebabnya, penting bagi perusahaan untuk melakukan penetration testing secara rutin. Penetration testing dapat membantu perusahaan untuk menemukan celah keamanan agar bisa segera ditambal atau diperbaiki.

3. Malware

Malware (malicious software) merupakan suatu program atau file berbahaya yang dibuat dengan tujuan jahat. Peretas dapat menyebarluaskan malware ketika sistem memiliki kerentanan keamanan. Mereka juga dapat menanamkan malware ketika karyawan Anda secara tidak sadar mengklik tautan berbahaya yang dikirim melalui email. Berbagai serangan malware ini biasanya digunakan oleh peretas untuk menghilangkan langkah otentikasi yang digunakan untuk melindungi sistem.

4. **Orang dalam yang berbahaya**
Selain karena faktor kesalahan teknis, data breach juga dapat terjadi karena faktor kesengajaan. Beberapa karyawan Anda mungkin memiliki akses untuk melihat data sensitif perusahaan. Terkadang karena iming-iming imbalan berupa uang, karyawan dapat menyalahgunakannya dan memberikan akses tersebut kepada peretas. Jika peretas berhasil membujuk karyawan Anda, mereka dapat mengakses data dengan mudah tanpa harus mengekploitasi sistem untuk menemukan celah keamanan.

Sumber Infografis : https://hostingtribunal.com/blog/biggest-data-breach-statistics/

SOFTWARE IT AUDIT

Penggunaan software IT audit untuk melakukan pemantauan dan pengujian terhadap aktivitas yang dilakukan user terhadap devices di organisasi

Melakukan pengujian untuk mengetahui apakah sistem yang digunakan memiliki celah keamanan yang dapat diretas oleh pihak yang tidak bertanggung jawab

Mengontrol setiap perubahan yang terjadi pada sistem.

ManageEngine
ADAudit Plus

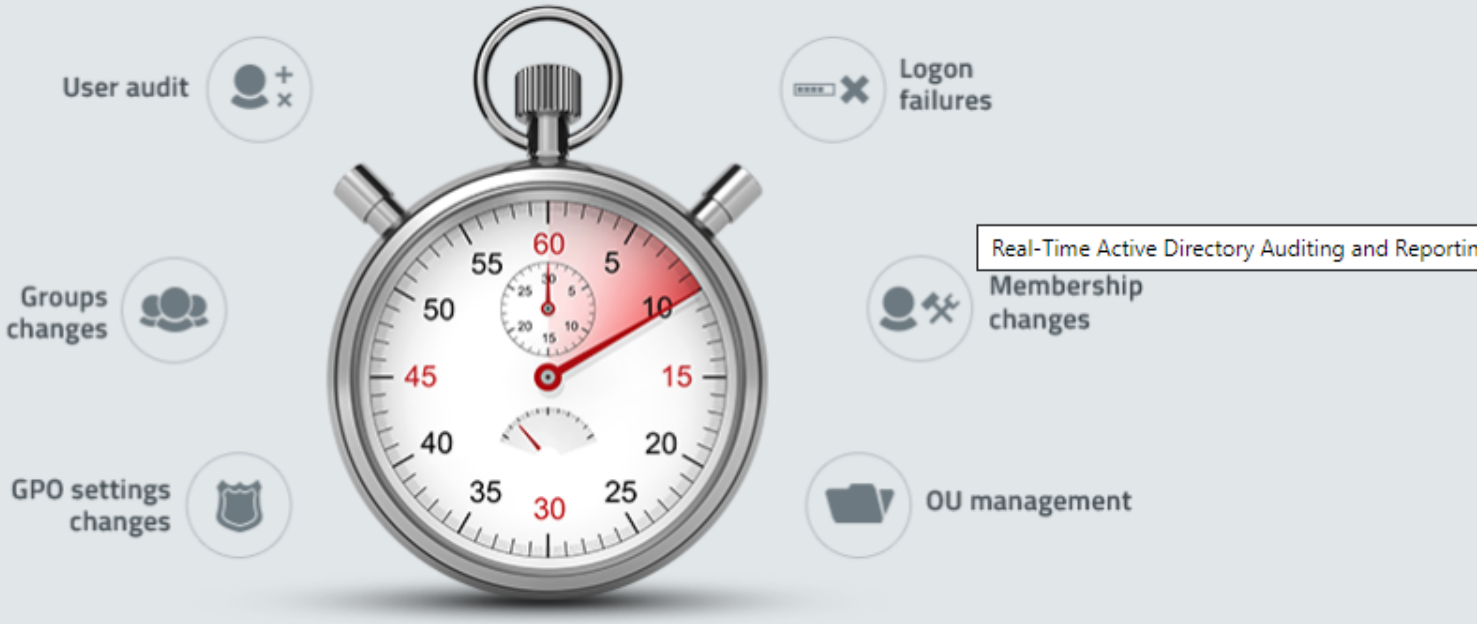
Products Store Partners Support |

Overview Features Demo Resources Get Quote Support Download

Real-Time Auditing for Active Directory

with 200+ audit reports & e-mail alerts

Download



Real-Time Active Directory Auditing and Reportin

ACTIVE DIRECTORY AUDITING

LOGON/LOGOFF AUDITING

FILE SERVER AUDITING

WINDOWS SERVERS AUDITING

REAL-TIME WINDOWS ACTIVE DIRECTORY AUDITING

In real-time, ensure critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes with 200+ detailed event specific GUI reports and email alerts.

Insider Threats

User Logon

Compliance

Reports & Alerts

Data Archiving

GPO Settings

WINDOWS LOGON/LOGOFF AUDITING

Audit the critical user workstation logon & logoff time to monitor the logon duration, logon failures, logon history and terminal services activity. View & Schedule graphical reports with Email alerts for periodic analysis & quick response during security threats.

Logon / Logoff

Compliance

Data Archiving

Reports & Alerts

All Workstation Reports

WINDOWS FILE SERVER AUDITING

Securely track the file creation, modification & deletion from an authorized / unauthorized access, with detailed forensics of security and permission changes to the documents in their files / folder structure and shares.

File Servers

Access Permissions

Failover Clusters

NetApp Filers

EMC Servers

All File Server Reports

WINDOWS SERVERS AUDITING

Track the Logon/Logoff, Schedule to track events like RADIUS Logon, Terminal Services Activity, Logon Duration and Logon History. Audit related processes can be kept tab by Tracking Windows Schedule jobs.

Windows Servers

Printer Auditing

File integrity Monitoring

Compliance

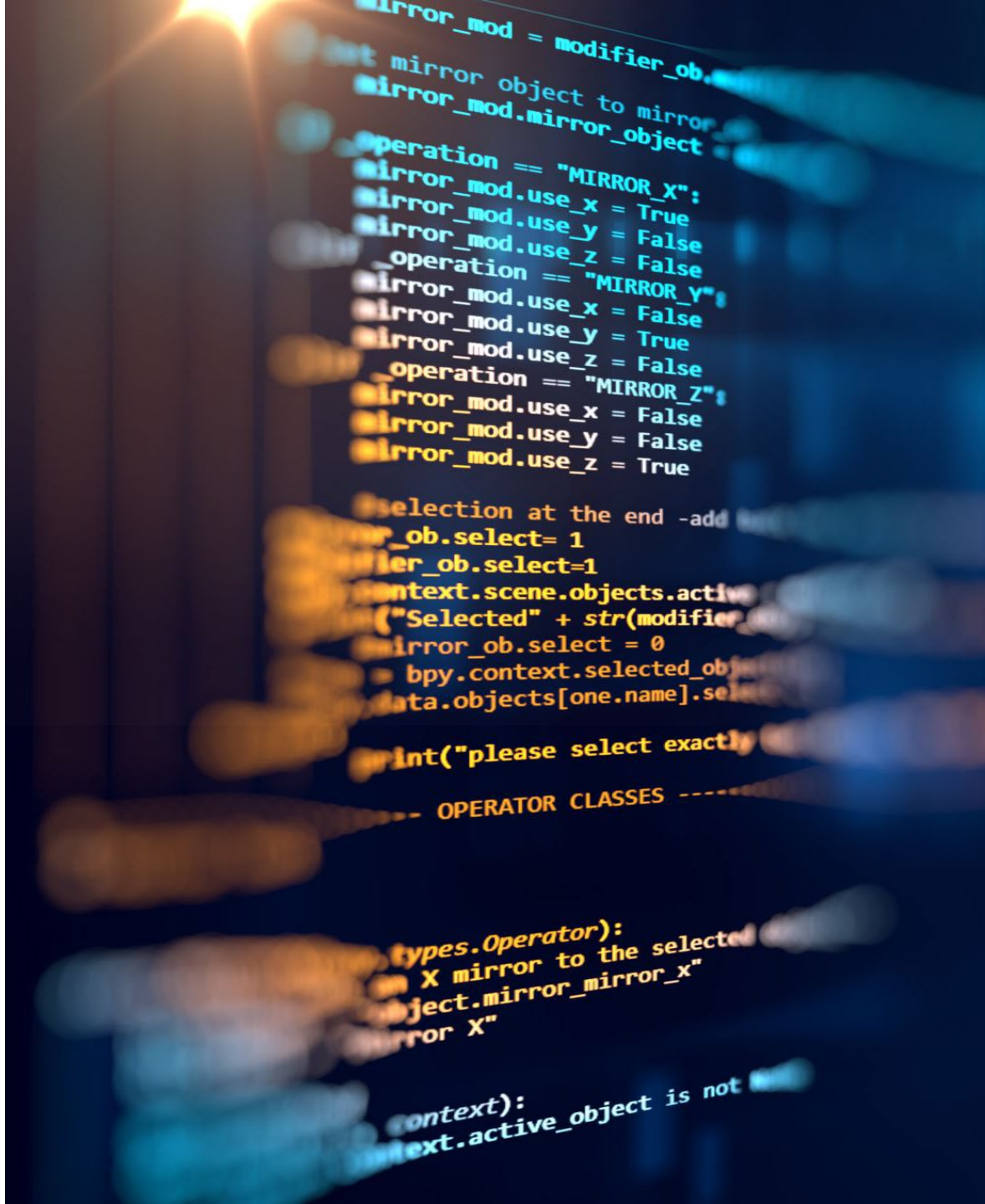
Reports & Alerts

All Windows Servers Reports

DEMO : HTTPS://WWW.YOUTUBE.COM/WATCH?V=X6SJRLSDQQU

SOFTWARE IT AUDIT

Manage Engine AD Audit Plus



SALAH SATU RESIKO YANG MUNCUL DI BIDANG IT

Data Breach

merupakan salah satu jenis serangan cyber yang dapat mengancam organisasi. Data breach atau pelanggaran data merupakan suatu kondisi di mana hacker mampu menyusup masuk ke dalam sistem dan mengekstraksi data-data penting di dalamnya.

Hal ini mampu membawa berbagai dampak negatif untuk bisnis, mulai dari tercurinya data-data sensitif sampai hilangnya kepercayaan pelanggan.

APA SAJA YANG DAPAT MENYEBABKAN DATA BREACH DAPAT TERJADI.

1. **Kredensial yang lemah**

Kredensial atau kata sandi yang lemah menjadi salah satu penyebab data breach dapat terjadi. Kata sandi dibuat dengan tujuan untuk mengamankan sistem. Namun sayangnya masih banyak yang menggunakan kata sandi dengan frasa sederhana seperti Password1 atau 123456. Jika hacker dapat menemukan kata sandi yang Anda gunakan, mereka dapat dengan mudah masuk ke dalam sistem dan mengakses data-data sensitif di dalamnya. Oleh karena itu, penting bagi perusahaan untuk selalu menggunakan kata sandi yang kuat dan secara regular memperbaruinya.

2. **Adanya kerentanan di dalam aplikasi**

Sebagian besar hacker akan melakukan sejumlah serangan ketika mereka menemukan kerentanan dalam sebuah sistem. Itulah sebabnya, penting bagi perusahaan untuk melakukan penetration testing secara rutin. Penetration testing dapat membantu perusahaan untuk menemukan celah keamanan agar bisa segera ditambal atau diperbaiki.

3. Malware

Malware (malicious software) merupakan suatu program atau file berbahaya yang dibuat dengan tujuan jahat. Peretas dapat menyebarluaskan malware ketika sistem memiliki kerentanan keamanan. Mereka juga dapat menanamkan malware ketika karyawan Anda secara tidak sadar mengklik tautan berbahaya yang dikirim melalui email. Berbagai serangan malware ini biasanya digunakan oleh peretas untuk menghilangkan langkah otentikasi yang digunakan untuk melindungi sistem.

4. **Orang dalam yang berbahaya**
Selain karena faktor kesalahan teknis, data breach juga dapat terjadi karena faktor kesengajaan. Beberapa karyawan Anda mungkin memiliki akses untuk melihat data sensitif perusahaan. Terkadang karena iming-iming imbalan berupa uang, karyawan dapat menyalahgunakannya dan memberikan akses tersebut kepada peretas. Jika peretas berhasil membujuk karyawan Anda, mereka dapat mengakses data dengan mudah tanpa harus mengekploitasi sistem untuk menemukan celah keamanan.

Sumber Infografis : https://hostingtribunal.com/blog/biggest-data-breach-statistics/

SOFTWARE IT AUDIT

Penggunaan software IT audit untuk melakukan pemantauan dan pengujian terhadap aktivitas yang dilakukan user terhadap devices di organisasi

Melakukan pengujian untuk mengetahui apakah sistem yang digunakan memiliki celah keamanan yang dapat diretas oleh pihak yang tidak bertanggung jawab

Mengontrol setiap perubahan yang terjadi pada sistem.

ManageEngine
ADAudit Plus

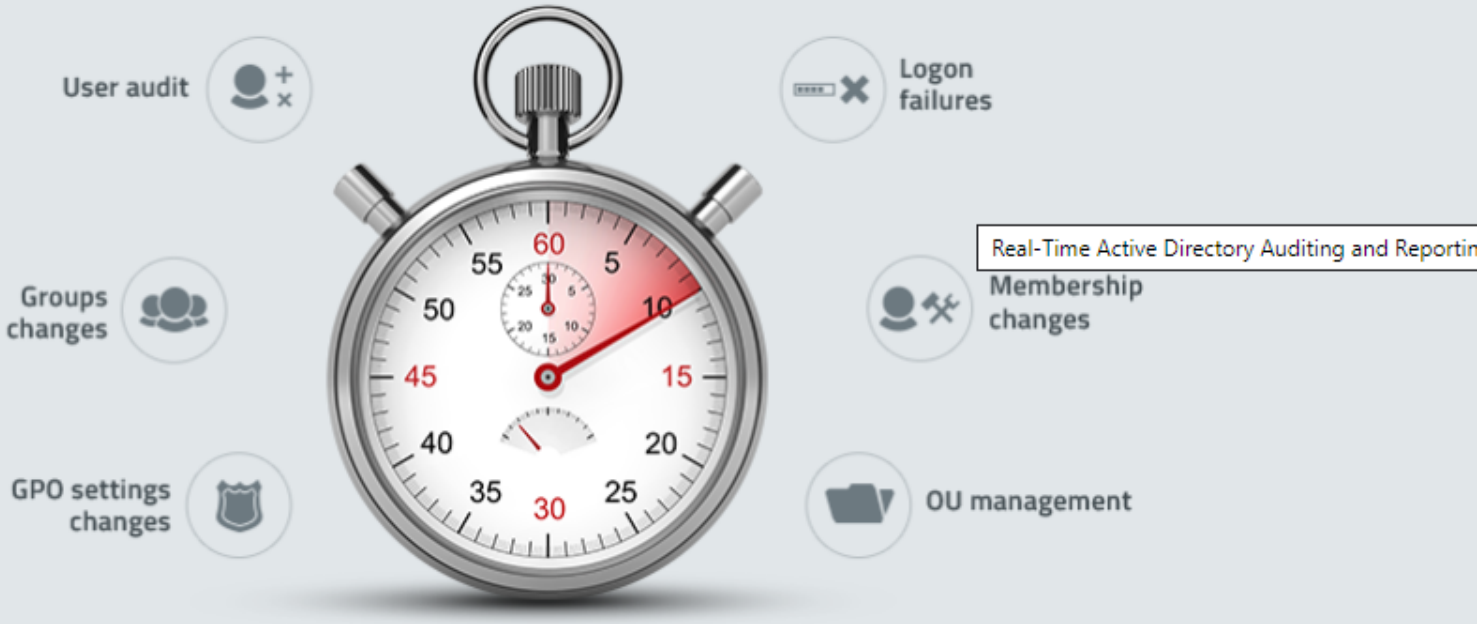
Products Store Partners Support |

Overview Features Demo Resources Get Quote Support Download

Real-Time Auditing for Active Directory

with 200+ audit reports & e-mail alerts

Download



Real-Time Active Directory Auditing and Reportin

ACTIVE DIRECTORY AUDITING

LOGON/LOGOFF AUDITING

FILE SERVER AUDITING

WINDOWS SERVERS AUDITING

REAL-TIME WINDOWS ACTIVE DIRECTORY AUDITING

In real-time, ensure critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes with 200+ detailed event specific GUI reports and email alerts.

Insider Threats

User Logon

Compliance

Reports & Alerts

Data Archiving

GPO Settings

WINDOWS LOGON/LOGOFF AUDITING

Audit the critical user workstation logon & logoff time to monitor the logon duration, logon failures, logon history and terminal services activity. View & Schedule graphical reports with Email alerts for periodic analysis & quick response during security threats.

Logon / Logoff

Compliance

Data Archiving

Reports & Alerts

All Workstation Reports

WINDOWS FILE SERVER AUDITING

Securely track the file creation, modification & deletion from an authorized / unauthorized access, with detailed forensics of security and permission changes to the documents in their files / folder structure and shares.

File Servers

Access Permissions

Failover Clusters

NetApp Filers

EMC Servers

All File Server Reports

WINDOWS SERVERS AUDITING

Track the Logon/Logoff, Schedule to track events like RADIUS Logon, Terminal Services Activity, Logon Duration and Logon History. Audit related processes can be kept tab by Tracking Windows Schedule jobs.

Windows Servers

Printer Auditing

File integrity Monitoring

Compliance

Reports & Alerts

All Windows Servers Reports

EX: HTTPS://WWW.YOUTUBE.COM/WATCH?V=X6SJRLSDQQU

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya "scope creep" (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Bagaimana cara mengendalikannya :
Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (*Control Objectives for Information and Related Technology*) adalah standar internasional untuk tata kelola TI

IT AUDIT

TASK 2 – PENGENDALIAN RESIKO

Oleh :

Dwi Septya Putri 182420057

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

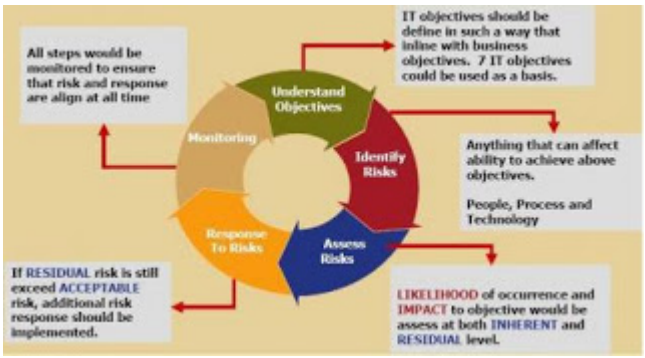
2019

Ada beberapa resiko yang dapat terjadi pada penggunaan TI antara lain :

- Malware : Infeksi pada system atau jaringan oleh virus, worm trojan adware atau spyware.
- Phising : Serangan terhadap organisasi melalui email atau elektronik dalam upaya untuk memperoleh informasi rahasia.
- Pharming penyimpangan lalu lintas internet ke situs penipu melalui DNS palsu atau address bar browser serangan ini dimasksudkan untuk memperoleh informasi rahasia.
- Spam pesan email yang tidak diminta atau tidak diinginkan
- Denial of Service upaya untuk mengalahkan atau membebani kinerja jaringan atau sumber daya sistem dengan maksud untuk menurunkan kinerja mereka atau membuat layanan tidak tersedia.
- Akses yang tidak sah oleh pihak luar, akses yang tidak sah atau penggunaan sistem olatau jaringan oleh pihak luar.
- Vandalisme / sabotase : pencatatan, kehancuran atau kerusakan pada jaringan sistem organisasi atau website.
- Pemerasan : Tuntutan untuk uang atau konsesi lainnya berdasarkan ancaman untuk menggunakan sarana elektronik untuk membahayakan jaringan organisasi, sistem atau reputasi
- Penipuan Transaksi : Transaksi elektronik palsu yang mengakibatkan kerugian keuangan atau kerusakan pada organisasi atau pelanggan.
- Kerugian fisik : fisik kehilangan atau pencurian atau komputer, media penyimpanan, atau perangkat lain yang terkait data.
- Akses tidak sah oleh orang dalam : menjalankan akses oleh orang dalam fungsi sistem atau informasi yang tidak berwenang.
- Insider : pelanggaran terhadap kebijakan organisasi mengenai penggunaan komputasi / sumber daya jaringan .

Resiko-resiko dikontrol dengan mengadopsi framework cobit yaitu kerangka panduan tata kelola TI dan atau bisa juga disebut sebagai toolset pendukung

yang bisa digunakan untuk menjembatani gap antara kebutuhan dan bagaimana teknis pelaksanaan pemenuhan kebutuhan tersebut dalam suatu organisasi. Framework manajemen resiko TI dengan menggunakan COBIT (lihat gambar) terdiri dari :



1. **Penetapan Objektif**
   Kriteria informasi dari COBIT dapat digunakan sebagai dasar dalam mendefinisikan objektif TI. Terdapat tujuh kriteria informasi dari COBIT yaitu : effectiveness, efficiency, confidentiality, integrity, availability, compliance, dan reliability.

2. **Identifikasi Resiko**

Objectives	Events
Effectiveness and Efficiency	Manajemen yang buruk (perencanaan dan kebijakan)
	Sistem (Hardware, software dan teknologi).
	Kemampuan TI dan non-TI.
	Manajemen proses (desain dan eksekusi)
Confidentiality	Manajemen Keamanan (kebijakan dan prosedur).
	Sistem (Hardware, software teknologi dan jaringan).
	Kesadaran pengguna
	Hacker dan virus
Integrity and Reliability	Desain sistem (input, proses, output)
	Hacker dan pelanggar akses
	Prosedur pemberian otoritas yang buruk.
Availability	Desain system dan jaringan
	Kegagalan hardware
	Sabotase dari luar
	Virus dan serangan
	Tidak ada BCP, backup dan recovery
Compliance	Tidak sadar atau tidak mengerti terhadap aturan dan regulasi
	Tidak ada monitoring

TABEL1 KEJADIAN (EVENTS) YANG MENGGANGU PENCAPAIAN OBJEKTIF PERUSAHAAN

Identifikasi resiko merupakan proses untuk mengetahui resiko. Sumber resiko bisa berasal dari :

- Manusia, proses dan teknologi
- Internal (dari dalam perusahaan) dan eksternal(dari luar perusahaan)
- Bencana (hazard), ketidakpastian (uncertainty) dan kesempatan (opportunity).

Dari ketiga sumber resiko tersebut dapat diketahui kejadian-kejadian yang dapat mengganggu perusahaan dalam mencapai objektifnya (lihat tabel event diatas).

3. **Penilaian Resiko**
   Proses untuk menilai seberapa sering resiko terjadi atau seberapa besar dampak dari resiko (tabel 2.2). Dampak resiko terhadap bisnis (business impact) bisa berupa : dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data), dan penundaan proses pengambilan keputusan.

   Sedangkan kecenderungan (likelihood) terjadinya resiko dapat disebabkan oleh sifat alami dari bisnis, struktur dan budaya organisasi, sifat alami dari sistem (tertutup atau terbuka, teknologi baru dan lama), dan kendali-kendali yang ada. Proses penilaian resiko bisa berupa resiko yang tidak dapat dipisahkan (inherent risks) dan sisa resiko (residual risks).

Level	Business Impacts	Likelihood
0	Kerusakan yang hampir tidak signifikan	Hampir mustahil terjadi
1	Kerusakan kecil	Jarang terjadi
2	Kerusakan yang signifikan tetapi dapat ditolerir	Mungkin terjadi
3	Kerusakan besar	Sering terjadi
4	Kerusakan yang dapat mengancam kelangsungan bisnis	Sangat sering terjadi

TABEL 2.2 TINGKATAN BESARNYA DAMPAK RESIKO DAN FREKUENSI TERJADINYA RESIKO

4. **Respon Resiko**
   Untuk melakukan respon terhadap resiko adalah dengan menerapkan kontrol objektif yang sesuai dalam melakukan manajemen resiko. Jika sisa resiko masih melebihi resiko yang dapat diterima (acceptable risks), maka diperlukan respon resiko tambahan. Proses-proses pada framework COBIT (dari 34 Control Objectives) yang sesuai untuk manajemen resiko adalah :
   - PO1 (Define a Stretegic IT Plan) dan PO9 (Assess and Manage Risks)
   - AI6 (Manages Change)
   - DS5 (Ensure System and Security) dan DS11 (Manage Data)
   - ME1 (Monitor and Evaluate IT Performance)

5. **Monitor Resiko**
   Setiap langkah dimonitor untuk menjamin bahwa resiko dan respon berjalan sepanjang waktu.

Jenis-jenis resiko

1. Risiko Bisnis (Bussiness Risks) Risiko bisnis adalah risiko yang dapat disebabkan oleh faktor-faktor intern maupun ekstern yang berakibat kemungkinan tidak tercapainya tujuan organisasi (business goals objectives).
   - Risiko ekstern (risk from external environment) ialah misalnya antara lain perubahan kondisi perekonomian tingkat kurs yang berubah mendadak, dan munculnya pesaing baru yang mempunyai potensi bersaing tinggi
   - Risiko internal ialah risiko yang berasal dari internal misalnya antara lain permasalahan kepegawaian, risiko-risiko yang berkaitan dengan peralatan atau mesin, risiko keputusan yang tidak tepat, dan kecurangan manajemen (Manajement Fraud).
2. Risiko Bawaan (Inherent Risks) Risiko bawaan ialah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan, jika tidak ada pengendalian intern. Misalnmya kegiatan kampus, apabila tidak ada absensi/daftar kehadiran kuliah akan banyak mahasiswa yang cenderung tidak disiplin hadir mengikuti kuliah.
3. Risiko Pengendalian (Control Risks) Dalam suatu organisasi yang baik seharusnya sudah ada risks assessment, dan dirancang pengendalian intern secara optimal terhadap setiap potensi risiko. Risiko pengendalian ialah masih adanya risiko meskipun sudah ada pengendalian.
4. Risiko Deteksi (Detection Risks) Risiko deteksi adalah risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya error yang cukup materialitas atau adanya kemungkinan fraud. Risiko deteksi mungkin dapat terjadi karena auditor ternyata dalam prosedur auditnya tidak dapat mendeteksi terjadinya existing control failures (system pengendalian intern yang ada ternyata tidak berjalan baik).
5. Audit (Audit Risks) Risiko audit sebenarnya adalah kombinasi dari inherent risks, control risks, dan detection risks. Risiko audit adalah risiko bahwa hasil pemeriksaan auditornya ternyata belum dapat mencerminkan keadaan yang sesungguhnya.

Kerangka Kerja Resiko Manajemen

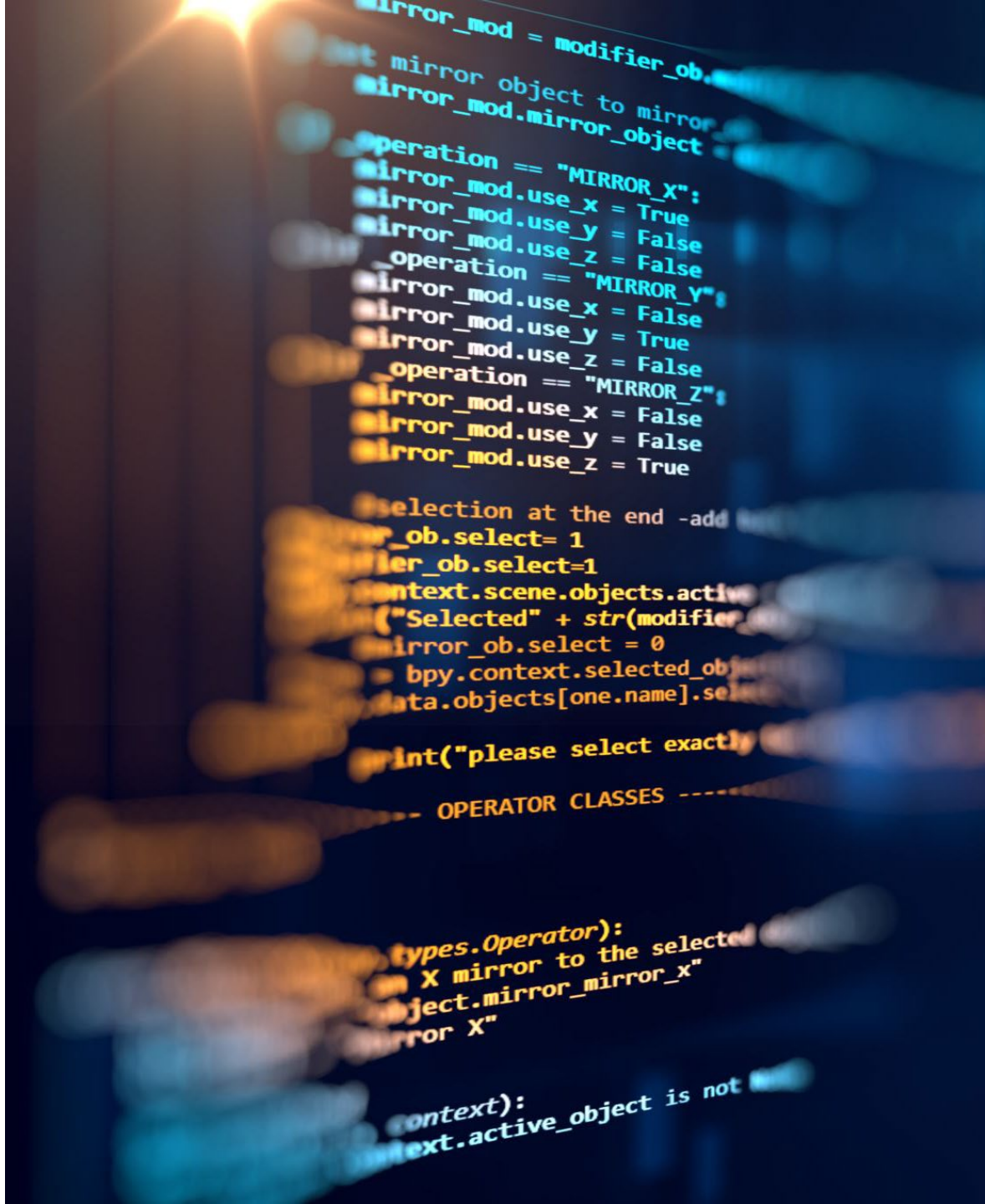
Secara umum ada enam tujuan *risk management* dalam perusahaan atau badan usaha, diantaranya adalah:

1. Melindungi Perusahaan
   Memberikan perlindungan terhadap perusahaan dari tingkat risiko signifikan yang bisa menghambat proses pencapaian tujuan perusahaan.
2. Membantu Pembuatan Kerangka Kerja
   Membantu dalam proses pembuatan kerangka kerja manajemen risiko yang konsisten atas ririko yang ada pada proses bisnis dan fungsi-fungsi di dalam sebuah perusahaan.
3. Mendorong Manajemen Agar Proaktif
   Mendorong manajemen agar bertindak proaktif dalam mengurangi potensi risiko, dan menjadikan manajemen risiko sebagai sumber keunggulan bersaing dan kinerja perusahaan

4. Sebagai Peringatan untuk Berhati-Hati
   Mendorong semua individu dalam perusahaan agar bertindak hati-hati dalam menghadapi risiko perusahaan demi tercapainya tujuan yang diinginkan bersama.
5. Meningkatkan Kinerja Perusahaan
   Membantu meningkatkan kinerja perusahaan dengan menyediakan informasi tingkat risiko yang disebutkan dalam peta risiko/ risk map. Hal ini juga berguna dalam pengembangan strategi dan perbaikan proses *risk management* secara berkesinambungan.
6. Sosialisasi Manajemen Risiko
   Membangun kemampuan individu maupun manajemen untuk mensosialisasikan pemahaman tentang risiko dan pentingnya *risk management*.

SOFTWARE IT AUDIT

Manage Engine AD Audit Plus



IT RISK

RESIKO YANG DIKHAWATIRKAN AKAN MUNCUL PADA BIDANG IT

JENIS RESIKO AUDIT

Control Risk (Risiko Pengendalian)
Adalah ukuran penetapan auditor akan kemungkinan adanya kekeliruan (salah saji) dalam segmen audit yang melampaui batas toleransi yang tidak terdeteksi atau tercegah oleh struktur pengendalian intern klien.

SALAH SATU RESIKO YANG MUNGKIN MUNCUL DI BIDANG IT

Data Breach

merupakan salah satu jenis serangan cyber yang dapat mengancam bisnis Anda. Data breach atau pelanggaran data merupakan suatu kondisi di mana hacker mampu menyusup masuk ke dalam sistem dan mengekstraksi data-data penting di dalamnya.

Hal ini mampu membawa berbagai dampak negatif untuk bisnis, mulai dari tercurinya data-data sensitif sampai hilangnya kepercayaan pelanggan. Untuk menghindarinya,

APA SAJA YANG DAPAT MENYEBABKAN DATA BREACH DAPAT TERJADI.

1. **Kredensial yang lemah**

Kredensial atau kata sandi yang lemah menjadi salah satu penyebab data breach dapat terjadi. Kata sandi dibuat dengan tujuan untuk mengamankan sistem. Namun sayangnya masih banyak yang menggunakan kata sandi dengan frasa sederhana seperti Password1 atau 123456. Jika hacker dapat menemukan kata sandi yang Anda gunakan, mereka dapat dengan mudah masuk ke dalam sistem dan mengakses data-data sensitif di dalamnya. Oleh karena itu, penting bagi perusahaan untuk selalu menggunakan kata sandi yang kuat dan secara regular memperbaruinya.

2. **Adanya kerentanan di dalam aplikasi**

Sebagian besar hacker akan melakukan sejumlah serangan ketika mereka menemukan kerentanan dalam sebuah sistem. Itulah sebabnya, penting bagi perusahaan untuk melakukan penetration testing secara rutin. Penetration testing dapat membantu perusahaan untuk menemukan celah keamanan agar bisa segera ditambal atau diperbaiki.

3. Malware

Malware (malicious software) merupakan suatu program atau file berbahaya yang dibuat dengan tujuan jahat. Peretas dapat menyebarluaskan malware ketika sistem memiliki kerentanan keamanan. Mereka juga dapat menanamkan malware ketika karyawan Anda secara tidak sadar mengklik tautan berbahaya yang dikirim melalui email. Berbagai serangan malware ini biasanya digunakan oleh peretas untuk menghilangkan langkah otentikasi yang digunakan untuk melindungi sistem.

4. **Orang dalam yang berbahaya**
Selain karena faktor kesalahan teknis, data breach juga dapat terjadi karena faktor kesengajaan. Beberapa karyawan Anda mungkin memiliki akses untuk melihat data sensitif perusahaan. Terkadang karena iming-iming imbalan berupa uang, karyawan dapat menyalahgunakannya dan memberikan akses tersebut kepada peretas. Jika peretas berhasil membujuk karyawan Anda, mereka dapat mengakses data dengan mudah tanpa harus mengekploitasi sistem untuk menemukan celah keamanan.

Sumber Infografis : https://hostingtribunal.com/blog/biggest-data-breach-statistics/

SOFTWARE IT AUDIT

Penggunaan software IT audit untuk melakukan pemantauan dan pengujian terhadap aktivitas yang dilakukan user terhadap devices di organisasi

Melakukan pengujian untuk mengetahui apakah sistem yang digunakan memiliki celah keamanan yang dapat diretas oleh pihak yang tidak bertanggung jawab

Mengontrol setiap perubahan yang terjadi pada sistem.

ManageEngine
ADAudit Plus

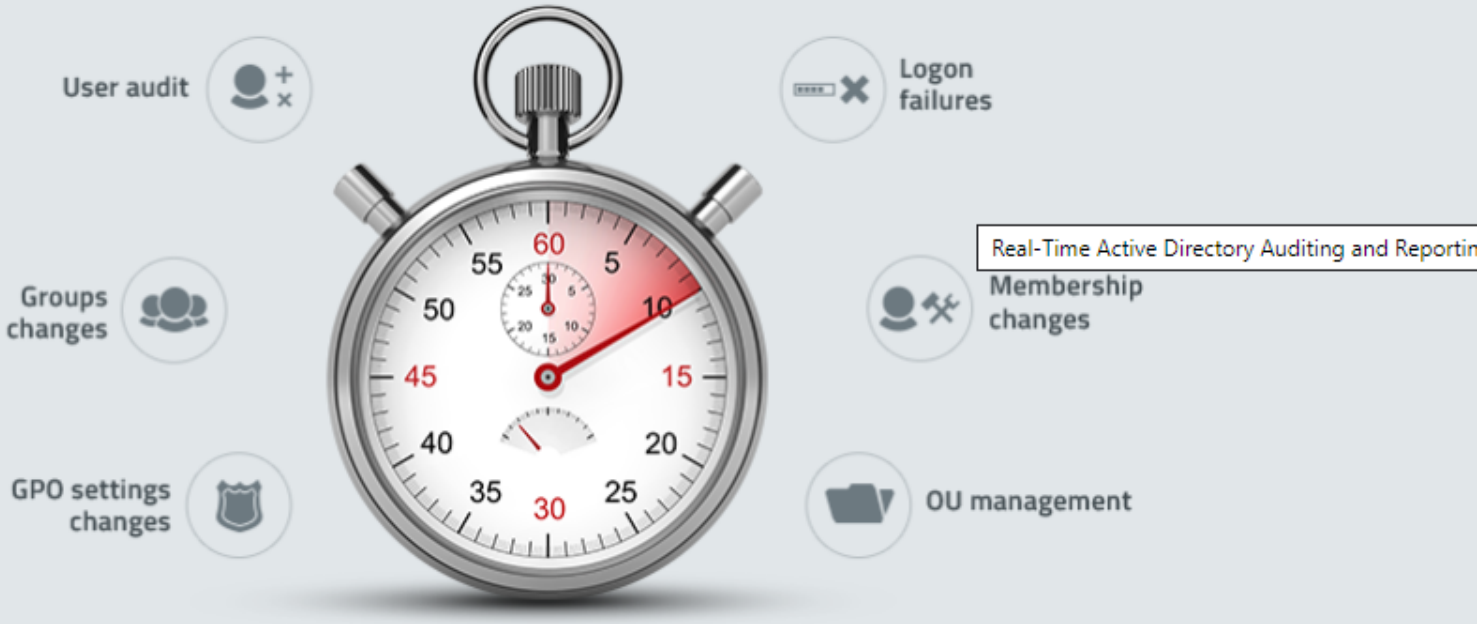
Products Store Partners Support |

Overview Features Demo Resources Get Quote Support Download

Real-Time Auditing for Active Directory

with 200+ audit reports & e-mail alerts

Download



Real-Time Active Directory Auditing and Reportin

ACTIVE DIRECTORY AUDITING

LOGON/LOGOFF AUDITING

FILE SERVER AUDITING

WINDOWS SERVERS AUDITING

REAL-TIME WINDOWS ACTIVE DIRECTORY AUDITING

In real-time, ensure critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes with 200+ detailed event specific GUI reports and email alerts.

Insider Threats

User Logon

Compliance

Reports & Alerts

Data Archiving

GPO Settings

WINDOWS LOGON/LOGOFF AUDITING

Audit the critical user workstation logon & logoff time to monitor the logon duration, logon failures, logon history and terminal services activity. View & Schedule graphical reports with Email alerts for periodic analysis & quick response during security threats.

Logon / Logoff

Compliance

Data Archiving

Reports & Alerts

All Workstation Reports

WINDOWS FILE SERVER AUDITING

Securely track the file creation, modification & deletion from an authorized / unauthorized access, with detailed forensics of security and permission changes to the documents in their files / folder structure and shares.

File Servers

Access Permissions

Failover Clusters

NetApp Filers

EMC Servers

All File Server Reports

WINDOWS SERVERS AUDITING

Track the Logon/Logoff, Schedule to track events like RADIUS Logon, Terminal Services Activity, Logon Duration and Logon History. Audit related processes can be kept tab by Tracking Windows Schedule jobs.

Windows Servers

Printer Auditing

File integrity Monitoring

Compliance

Reports & Alerts

All Windows Servers Reports

DEMO : HTTPS://WWW.YOUTUBE.COM/WATCH?V=X6SJRLSDQQU

NAMA : EVAN APRIADI DILATAMA

NIM :182420081

MATERI : TUGAS IT AUDIT TASK 2 :PENGENDALIAN RESIKO

MTI 19 B

Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

Jelaskan bagaimana resiko-resiko tersebut dikendalikan ?

Pada dasarnya, faktor resiko dalam suatu perencanaan sistem informasi, dapat diklasifikasikan ke dalam 4 kategori resiko, yaitu :

1. *Catastrophic* (Bencana)
2. *Critical* (Kritis)
3. *Marginal* (kecil)
4. *Negligible* (dapat diabaikan)

Cara mengatasinya dengan :

1. Identifikasi Resiko
Proses identifikasi resiko (gambar 3.1) terdiri dari sumber resiko, kejadian (event) yang dapat menyebabkan resiko dan dampak yang dihasilkan jika resiko itu terjadi (effect). Sumber resiko dan kelemahan (vulnerability) ini akan menjadi sumber ancaman (threat source).

2. Analisa Resiko
Setelah sumber dan kejadian yang menyebabkan resiko teridentifikasi, maka dilakukan analisa resiko yaitu menilai level resiko dan membuat ranking resiko dengan mempertimbangkan faktor kecenderungan (likelihood) dan besarnya dampak resiko (impact). Pendekatan analisa resiko dapat secara kualitatif atau kuantitatif. Level kecenderungan dan dampak dapat dikategorikan sesuai variasi yang ada, misalnya menjadi high, medium dan low seperti yang ada pada NIST dan OCTAVE.

3. Respon Resiko
Berdasarkan hasil analisa resiko, maka dilakukan perencanaan aksi yang ingin dilakukan terhadap resiko. Apakah akan menghilangkan resiko (risk retention), mengurangi resiko (risk reduction) hingga mencapai tingkat yang dapat diterima (acceptable level), mencegah resiko (risk avoidance) atau mentransfer resiko (risk transfer). Hasil perencanaan ini kemudian diimplementasikan oleh personil yang ditunjuk berdasarkan prioritas resiko, jadwal, budget dan kontrol yang telah ditetapkan.

4. Evaluasi Resiko
Proses ini berfungsi untuk mengetahui apakah implementasi kontrol terhadap resiko sudah sesuai, dan apakah masih ada sisa resiko (risk residual) atau ada resiko baru.

terdapat banyak jenis resiko yang dapat terjadi ketika kita menggunakan perangkat ataupun sistem TI, khususnya bagi perusahaan.

beberapa diantaranya:

- Email password may be disclosed
- Facebook account may be used by someone else
- Credit card information may be disclosed
- Customer information may be stolen
- IT Service delivery to the customers may be poor
- IT systems may be obsolete
- IT projects may be late or fail
- IT systems do not provide any busines
- benefit
- Risk of non-compliance with the
- regulator
- Own people may harm the systems

adapun untuk pengendaliannya, maka dapat melakukan manajemen terhadap resiko itu sendiri.Manajemen risiko pada dasarnya dilakukan melalui proses-proses berikut ini.

1. Identifikasi risiko.

2. Evaluasi dan Pengukuran Risiko, dan

3. Pengelolaan risiko.

dengan melakukan manajemen resiko yang baik maka akan diketahui resiko mana yang harus diselesaikan lebih dulu dan resiko mana yang bisa saja terjadi kedepannya.

KELOMPOK 3

" IT AUDIT "

Reni Septiyanti
Fero Triando
Evan Apriadi Dilatama
Fitrianto Puja Kesuma

Program Pascasarjana Magister Teknik Informatika
Universitas Bina Darma Palembang

2019

RISIKO AUDIT

Risiko Audit adalah istilah yang digunakan dalam kaitannya dengan audit atas laporan keuangan suatu entitas.

Risiko audit diartikan sebagai tingkat ketidakpastian tertentu yang dapat diterima auditor dalam pelaksanaan auditnya, seperti :

- ❑ Ketidakpastian validitas dan reliabilitas bukti audit.
- ❑ Ketidakpastian mengenai efektivitas pengendalian internal.

Risiko Audit (*Audit Risk*) adalah risiko yang terjadi dalam hal auditor tanpa disadari tidak memodifikasikan pendapatnya sebagaimana mestinya, atas suatu laporan keuangan yang mengandung salah saji material.

Risiko Audit (*Audit Risk*) terdiri dari 3 jenis :

1. Risiko Bawaan (*Inheren Risk*)
2. Risiko Pengendalian (*Control Risk*)
3. Risiko Deteksi (*Detection Risk*)

1. Risiko Bawaan (*Inheren Risk*)

Risiko bawaan adalah kerentanan suatu asersi terhadap salah saji material dengan asumsi tidak ada kebijakan dan prosedur struktur pengendalian intern yang terkait. Risiko bawaan selalu ada dan tidak pernah mencapai angka nol. Risiko bawaan tidak dapat diubah oleh penerapan prosedur audit yang paling baik sekalipun.

Risiko bawaan bervariasi untuk setiap asersi. Sebagai contoh, asersi keberadaan dan keterjadian kas mempunyai risiko bawaan yang lebih tinggi daripada aktiva tetap. Hal ini disebabkan uang tunai merupakan suatu aset yang sangat rawan terhadap manipulasi, dan semua orang berminat terhadap uang. Sedangkan aktiva tetap lebih terlihat jelas keberadaannya. Risiko bawaan juga dibedakan atas risiko bawaan setiap akun dan risiko bawaan keseluruhan untuk banyak akun.

Contoh Kasus 1 (Pada Kepolisian)

No	Contoh Inheren Risk	*Control Assesment*
1	Fasilitas negara digunakan sebagai kepentingan pribadi.	Peningkatan pengawasan yang tegas dan ketat terhadap para anggota polisi.
2	Masyarakat dikenakan tarif apabila meminta bantuan kepada kepolisian yang membebani si pelapor atau si peminta bantuan.	Adanya pusat-pusat pelayanan pelaporan bagi masyarakat yang lebih mudah dan dapat dijangkau.
3	Menyelenggarakan kegiatan atau razia tanpa izin di jalanan dengan tujuan mendapatkan penghasilan tambahan dan terkadang melakukan tindakan-tindakan dengan tidak sopan dan anarkis .	Setiap anggota polisi lebih di tekankan bahwa dalam melaksanakan tugas dan wewenangnya, pejabat kepolisian senantiasa bertindak berdasarkan norma agama, kesopanan, kesusilaan, serta menjunjung tinggi hak asasi manusia (Pasal 19 : Ayat 1).
4	Membunyikan sirine dan menyalakan lampu rotator hanya untuk menghindari kemacetan atau melintasi jalanan dengan bebas tanpa disertai tugas.	Setiap anggota polisi di uji apakah mereka mengetahui tugas dan wewenangnya yang Sesuai dengan tugas dan wewenang kepolisian yang diatur dalam UU pasal 14 dan pasal 13 tentang kepolisian.
5	Lebih banyak terlihat duduk santai di warung-warung atau di pos-pos polisi dari pada berdiri di jalanan mengatur kelancaran lalu lintas.	Kesejahteraan setiap anggota polisi lebih ditingkatkan dan diperhatikan.

Contoh Kasus 2
(Kasus Audit Asset Tetap)

Pada Desember 2006 Indonesia Corruptin Watch (ICW) melaporkan kasus dugaan korupsi ke Komisi Pemberantasan Korupsi (KPK) dalam ruislaag (tukar guling) antara asset PT. Industri Sandang Nusantara (ISN), sebuah BUMN yang bergerak di bidang tekstil, dengan asset PT. GDC, sebuah perusahaan swasta. Dalam ruislaag tersebut PT. ISN menukarkan tanah seluas 178.497 meter persegi di kawasan Senayan dengan Tanah seluas 47 hektar beserta Pabrik dan mesin di karawang.

Contoh Kasus 2
(Kasus Audit Asset Tetap) ....

Berdasarkan hasil temuan Badan Pemeriksaan Keuangan (BPK) semester II Tahun Anggaran 1998/1999, menyatakan ruislaag itu berpotensi merugikan keuangan Negara sebesar Rp. 121,628 miliar. Kerugian itu terdiri dari kekurangan luas bangunan pabrik dan mesin milik PT. GDC senilai Rp. 63,954 miliar, berdasarkan penilaian aktiva tetap oleh PT. Sucofindo pada 1999; penyusutan nilai asset pabrik milik PT. GDC senilai Rp. 31,546 miliar; dan kelebihan perhitungan harga tanah senilai Rp. 0,127 miliar. Selain itu juga ditemukan bahwa terdapat nilai saham yang belum dibayarkan oleh PT. GDC sebesar Rp. 26 miliar.

SOLUSI
(Kasus Audit Asset Tetap) ....

Seharusnya keputusan Tukar Guling tidak hanya menjadi wewenang salah satu pejabat saja, melainkan melibatkan beberapa pejabat sebagai pengendali dan control yang baik. Selain itu juga diperlukan sebuah aturan baku oleh perusahaan mengenai tukar guling, sehingga kemungkinan penyelewengan menjadi berkurang.

Diperlukan juga control dari lembaga bersangkutan terhadap penelitian tim penilik yang meneliti kelengkapan mengenai status asset, dokumen kelengkapan asset, sehingga tidak ada manipulasi dari nilai asset tersebut serta proses tukar menukar.

Dari kasus diatas dapat dibuktikan bahwa PT. ISN memiliki pengendalian intern yang sangat buruk. Sehingga PT. ISN rawan dicurangi oleh rekanan-rekanan bisnisnya maupun oleh oknum-oknum pejabat perusahaan yang ingin mengambil keuntungan. Oleh karena itu hal pertama yang harus dibenahi oleh PT. ISN adalah soal Pengendalian Internnya.

2. Risiko Pengendalian (*Control Risk*)

adalah risiko yang bisa timbul akibat kelemahan sistem pengendalian internal (SPI) auditee, tidak tahu karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain dan tidak mampu mencegah potensi salahsaji bersifat material dan/atau penggelapan (fraud). Jadi CR tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee jika mereka mau.

Risiko Pengendalian (*Control Risk*)

Contoh Kasus Denial of Service (DoS) dan Distributed DoS (DDos) attack. DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi

Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari berberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja. Adapun Modus yang dilakukan sang Cracker adalah ingin membuat suatu perusahaan atau organisasi rugi besar karena terganggunya system yang sedang berjalan. Bentuk Penyelesaiannya selain dilaporkan ke Kepolisian ada baiknya keamanan data dilakukan berlapis agar data tidak dengan mudah bocor atau mudah dicuri.

Risiko Pengendalian (*Control Risk*)

Mengantisipasi Serangan DDoS dengan DDoS Protection

Terkadang, seseorang tidak memperdulikan sisi keamanan sebuah website mereka dan cenderung merasa bahwa website mereka telah aman dari serangan DDoS tanpa fitur DDoS Protection. Pada nyatanya, sebuah serangan DDoS tidak hanya mengacu kepada resource yang dimiliki oleh server, namun juga kerentanan atau celah yang terdapat pada suatu website.

Cloudmatika sendiri bekerja sama dengan Cloudbric dalam menyediakan sebuah proteksi dari serangan DDoS untuk masyarakat di Indonesia dalam mengamankan websitenya dari segala serangan DDoS. Cloudbric DDoS Protection atau biasa disebut Anti DDoS dihadirkan di Indonesia untuk membuat masyarakat merasa lebih mudah dalam mengantisipasi dan juga mencegah segala bentuk serangan DDoS yang datang. Dengan fitur yang lengkap dan juga keamanan yang terjamin, membuat para developer tidak perlu takut lagi akan serangan-serangan DDoS yang ditujukan kepada websitenya

Risiko Pengendalian (*Control Risk*)

Contoh Kasus Denial of Service (DoS) dan Distributed DoS (DDos) attack. DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi

Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari berberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja. Adapun Modus yang dilakukan sang Cracker adalah ingin membuat suatu perusahaan atau organisasi rugi besar karena terganggunya system yang sedang berjalan. Bentuk Penyelesaiannya selain dilaporkan ke Kepolisian ada baiknya keamanan data dilakukan berlapis agar data tidak dengan mudah bocor atau mudah dicuri.

Keunggulan Cloudbric DDoS Protection

Beberapa keunggulan Cloudbric DDoS Protection yang harus diketahui oleh masyarakat di Indonesia untuk melengkapi sistem keamanan pada website mereka, diantaranya:

- **Identifikasi DDoS Lebih Awal dan Block Aktivitas Mencurigakan**

Memiliki sistem real-time protection yang menjadikan website Anda melakukan identifikasi setiap saat terhadap serangan-serangan yang datang dan melakukan blok secara langsung apabila teridentifikasi sebagai serangan. Pada Cloudbric DDoS Protection juga terdapat live monitor dari serangan yang datang dan juga serangan yang telah terblok. Sehingga Anda akan mengetahui detail serangan yang terjadi terhadap website Anda

- **Latency Rendah dan Pusat Data di Indonesia**

Menggunakan DDoS Protection Cloudmatika akan membuat Anda memiliki proteksi serangan DDoS dengan latency yang rendah karena server kami berada di Indonesia. Jika Anda menggunakan DDoS Protection yang memiliki server di luar Indonesia, maka akan menyebabkan layanan Anda sedikit terganggu akan latency yang ada. Sehingga mengakibatkan performa layanan Anda menjadi menurun dan sedikit lebih lambat

- **Biaya Yang Murah**

Anda tidak perlu takut akan biaya yang mahal untuk melakukan proteksi terhadap website Anda. Dengan Cloudbric DDoS Protection dari Cloudmatika, Anda akan mendapatkan biaya yang sangat terjangkau dan tentunya dengan fitur serta sistem keamanan yang canggih.

Contoh Kasus
(PT Kereta Api Indonesia (Persero)

No	Contoh Risiko Operasional PT KAI	Pengendalian Risiko (Control Risk)
1	Kebakaran dan kecelakaan kereta api	○ Penyiap-siagaan backup systems. ○ Prosedur kerja untuk sistem pemadam kebakaran, tangga darurat. ○ Coverage asuransi untuk meminimalkan kerugian/dampak negatif. ○ Pengendalian budaya keselamatan oleh polisi khusus kereta, petugas palang pintu kereta, dan sosialisasi secara berkala. ○ Pendidikan dan pelatihan dasar pemadam kebakaran.
2	Bencana alam	○ Memastikan adanya sistem peringatan dini (alarm) dan business continuity planning/contingency plan terhadap kondisi bencana. ○ Prosedur kerja untuk darurat bencana alam.
3	Keterbatasan suplai suku cadang	Pengaturan penggunaan dan suplai suku cadang yang lebih baik.

No	Contoh Risiko Operasional PT KAI	Pengendalian Risiko (Control Risk)
4	Keterbatasan kapasitas Depo/Balai Yasa	Optimalisasi kapasitas Depo/Balai Yasa, penjadwalan pemeliharaan dengan memperhitungkan saat sibuk *(peak season)* yaitu ketika liburan sekolah, lebaran, natal, tahun baru.
5	Gangguan dan kerusakan pada rel, peralatan persinyalan dan listrik aliran atas	○ Optimalisasi perawatan prasarana, ketelitian pemeriksaan, serta kerjasama tim yang baik. ○ Mempercepat pembangunan atau penyelesaian infrastruktur pendukung (stasiun *loading-unloading*). ○ Penambahan daya listrik dan penambahan sinyal dan stasiun. ○ Peremajaan gerbong kereta api, renovasi dan sterilisasi stasiun.
6	Terbatasnya mitra pengguna angkutan kereta api barang	Memprioritaskan pelayanan terhadap permintaan jasa angkutan barang dalam jumlah besar dan kontinu, berjarak tempuh jauh, dan bertarif tinggi serta pengangkutan berdasarkan perjanjian.

No	Contoh Risiko Operasional PT KAI	Pengendalian Risiko (Control Risk)
7	Meledaknya pengguna jasa transportasi pada musim-musim tertentu	○ Memperbanyak *point of sales* untuk penjualan tiket bekerjasama dengan mitra eksternal. ○ Melakukan sosialisasi dan promosi di media nasional terkait penjualan tiket kereta menjelang *peak season.* ○ Persiapan posko angkutan menjelang *peak season.* ○ Persiapan kereta api tambahan. ○ Peningkatan *bandwidth* dan kemudahan akses ke *website* untuk memfasilitasi pemesanan tiket secara online.
8	Keterlambatan jadwal keberangkatan dan kedatangan	○ Memanfaatkan teknologi informasi untuk memperbaiki proses perencanaan dan operasi untuk meningkatkan keselamatan, ketepatan waktu, pelayanan, dan keamanan. ○ Mengurangi toleransi terhadap keterlambatan.
9	Tidak diminatinya jasa-jasa penunjang perkeretaapian PT KAI	Membangun sistem pelayanan jasa transportasi unggulan yang terpadu dengan jasa pendukung, seperti kereta bandara, kereta wisata, biro jasa, dan *tour.*

PT Kereta Api Indonesia (Persero) dalam jangka waktu yang tidak terlalu lama, harus selalu mengidentifikasi risiko-risiko yang kemungkinan terjadi. Baik itu nanti risiko yang berklasifikasi dan berakibat tinggi, sedang atau rendah bagi perusahaan. Tidak hanya bagi perusahaan, namun juga bagi pengguna kereta api, yang tidak lain adalah masyarakat Indonesia sendiri. Apalagi setiap tahun pasti ada saja kecelakaan kereta api, yang disebabkan faktor internal maupun eksternal perusahaan. Mengembangkan inovasi terbaru itu juga perlu, apalagi dijaman yang sekarang sudah modern atau era globalisasi seperti ini. Harus banyak berkreatifitas agar mampu bersaing dengan transportasi darat yang lain.

Pengendalian risiko yang semaksimal mungkin, akan menghasilkan risiko yang seminimal mungkin. Sehingga juga akan meminimalkan kerugian bagi perusahaan dan pengguna jasa kereta api yaitu masyarakat. Dengan kenyamanan, perlindungan, asuransi, ketepatan waktu datang dan berangkat kereta api, harga tiket yang sesuai, peringatan dini bencana, dll yang dilakukan semaksimal mungkin oleh PT Kereta Api Indonesia (Persero), tentunya masyarakat juga akan mempercayai PT Kereta Api Indonesia (Persero) sebagai transportasi darat utama yang digunakan setiap hari. Sehingga akan berdampak pendapatan atau income yang tinggi untuk PT Kereta Api Indonesia (Persero).

3. Risiko Deteksi (*Detection Risk*)

adalah risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud). Jadi DR ada dalam kendali auditor. Itu karena DR sepenuhnya ada pada kendali auditor, maka sudah pasti mereka harus berupaya untuk menekan risiko ini hingga ke tingkatakan yang paling minimal (tidak mungkin menghilangkan risiko ini sepenuhnya).

Contoh Kasus

Risiko deteksi juga dapat terjadi karena auditor salah menetapkan langkah pengujiannya (prosedur audit). Sebagai contoh, prosedur pengeluaran barang menetapkan bahwa setiap pengeluaran barang harus didasarkan pada permintaan dari pihak yang akan menggunakan. Jadi dalam pelaksanaan pengeluaran barang akan terdapat dua populasi bukti yang saling terkait, bukti permintaan barang dan bukti pengeluaran barang. Dalam hal ini, risiko deteksi dapat terjadi jika dalam melakukan pengujian auditor menetapkan prosedur audit "periksa apakah atas setiap bukti permintaan barang terdapat bukti pengeluaran barangnya!" Prosedur ini dipastikan tidak akan menemukan kesalahan seperti kecurangan pihak gudang yang mengeluarkan barang walaupun tidak ada permintaan dari pihak yang membutuhkan barang, karena jika ada permintaan barang dapat dipastikan bagian gudang akan menerbitkan bukti pengeluaran barang.

Contoh Kasus

Sebaliknya, jika prosedur audit yang ditetapkan adalah: “periksa apakah atas setiap bukti pengeluaran barang terdapat bukti permintaan barangnya!” maka prosedur ini mungkin akan dapat menemukan kecurangan bagian gudang atas pengeluaran barang yang tidak didasarkan pada permintaan barang. Dengan prosedur tersebut, jika seandainya bagian gudang melakukan kecurangan mengeluarkan barang tetapi bukan untuk kepentingan perusahaan, maka akan dapat ditemukan dari sampel pengeluaran barang yang tidak ditemukan bukti permintaan barangnya.

Solusi

Berdasarkan penjelasan di atas, maka risiko deteksi berhubungan dengan luasnya pengumpulan dan pengujian bukti yang harus dilakukan auditor. Risiko deteksi yang rendah hanya dapat dicapai jika auditor melakukan pengujian yang luas. Hal ini berarti bahwa risiko deteksi berbanding terbalik dengan luasnya pengujian. Pemahaman mengenai model risiko audit tersebut akan dapat membantu auditor dalam merancang luasnya pengujian agar auditor tidak mengalami risiko audit (dalam arti audit menjadi tidak efektif), serta agar audit dapat dilaksanakan secara efisien (dalam arti audit dapat menghindarkan diri, melakukan perluasan pengujian yang tidak perlu).

TERIMA KASIH

IT AUDIT

Nama : Fido Rizki (182420060)

Program Studi Teknik Informatika S-2

Pascasarjana Universitas Bina Darma

1. Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

   Menurut pendapat saya ada 4 jenis reskio yang akan terjadi pada penggunaan TI yaitu

   - Pertama, **Kerugian bisnis, berkurangnya reputasi, dan melemahnya posisi kompetisi**. Pada hal ini saat perusahaan atau organisasi menggunakan penerapan it pada suatu perusahaan, namun yang kita terapkan tidak sesuai dengan apa yang perusahaan butuhkan, maka akan terjadi kerugian bisnis didalam suatu organisasi atau perusahaan tersebut.
   - Kedua, **membuang waktu**. Dalam hal ini, sebuah organisasi sudah menyiapkan beberapa pengelolaan ti dalam suatu organisasi, namun tidak digunakan karena tidak sesuai apa yang dibutuhkan organisasi, hal ini dapat memakan waktu yang seharusnya dapat digunakan untuk kebutuhan yang lebih penting, namun terbuang karena adanya penggunaan tatakelola yang tidak sesuai dengan apa yang dibutuhkan organisasi.
   - Ketiga, **biaya lebih tinggi dari yang diperkirakan**. Karena, disini suatu perusahaan atau organisasi sudah mengeluarkan biaya untuk membuat pengelolaan ti, namun biaya yag sudah dikeluarkan siasia karena pengelolaan ti tidak sesuai dengan apa yang dibutuhkan organisasi, sehingga diperlukan biaya tambahan untuk membuat pengelolaan ti yang baru agar sesuai dengan apa yang dibutuhkan organisasi.
   - Keempat, **Efisiensi dan proses inti perusahaan terpengaruh secara negatif** oleh rendahnya kualitas penggunaan TI.

2. Jelaskan bagaimana resiko-resiko tersebut dikendalikan

   Menurut pendapat saya resiko-resiko tersebut dapat dikendalikan cara melakukan review dan evaluasi terdapat pengembangan sistem informasi dan pengelolaan ti yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisasi.

1. Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

Menurut pendapat saya ada 4 jenis reskio yang akan terjadi pada penggunaan TI yaitu

- Pertama, **Kerugian bisnis, berkurangnya reputasi, dan melemahnya posisi kompetisi**. Pada hal ini saat perusahaan atau organisasi menggunakan penerapan it pada suatu perusahaan, namun yang kita terapkan tidak sesuai dengan apa yang perusahaan butuhkan, maka akan terjadi kerugian bisnis didalam suatu organisasi atau perusahaan tersebut.
- Kedua, **membuang waktu**. Dalam hal ini, sebuah organisasi sudah menyiapkan beberapa pengelolaan ti dalam suatu organisasi, namun tidak digunakan karena tidak sesuai apa yang dibutuhkan organisasi, hal ini dapat memakan waktu yang seharusnya dapat digunakan untuk kebutuhan yang lebih penting, namun terbuang karena adanya penggunaan tatakelola yang tidak sesuai dengan apa yang dibutuhkan organisasi.
- Ketiga, **biaya lebih tinggi dari yang diperkirakan**. Karena, disini suatu perusahaan atau organisasi sudah mengeluarkan biaya untuk membuat pengelolaan ti, namun biaya yag sudah dikeluarkan siasia karena pengelolaan ti tidak sesuai dengan apa yang dibutuhkan organisasi, sehingga diperlukan biaya tambahan untuk membuat pengelolaan ti yang baru agar sesuai dengan apa yang dibutuhkan organisasi.
- Keempat, **Efisiensi dan proses inti perusahaan terpengaruh secara negatif** oleh rendahnya kualitas penggunaan TI.

2. Jelaskan bagaimana resiko-resiko tersebut dikendalikan

Menurut pendapat saya resiko-resiko tersebut dapat dikendalikan cara melakukan review dan evaluasi terdapat pengembangan sistem informasi dan pengelolaan ti yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisasi.

Nama : Fitrianto Puja Kesuma

NIM : 182420082

Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

Beberapa jenis resiko yang dapat terjadi antara lain:

A. Risiko Inheren

Resiko inheren berkenaan dengan kemungkinan adanya kekeliruan dalam segmen audit yang melampaui batas toleransi sebelum memper-hitungkan faktor efektivitas pengendalian internal. Resiko inheren adalah faktor kerentanan laporan keuangan terhadap kekeliruan yang material dengan asumsi tidak adanya pengendalian internal. Oleh karena itu bila risiko inheren tinggi, maka auditor harus mengumpulkan bukti audit yang lebih banyak.

Faktor-faktor yang perlu ditelaah auditor dalam menetapkan risiko inheren adalah sifat bidang usaha organisasi, integritas manajemen, motivasi manajemen, hasil audit sebelumnya, hubungan istimewa, transaksi non rutin, dan kerentanan terhadap fraud.

Risiko inheren juga dapat dianggap sebagai risiko yang signifikan. Inherent risk represents the auditor's assessment that there may be a material misstatement relating to an assertion in the financial statements under audit, without taking the effectiveness of the related internal controls into account. Risiko inheren merupakan penilaian auditor yang mungkin ada salah saji material yang berkaitan dengan suatu pernyataan dalam laporan keuangan yang diaudit, tanpa mengambil efektivitas pengendalian internal terkait ke rekening. If the auditor concludes that there is a high likelihood of such a misstatement, ignoring internal controls, he would assess the inherent risk as being high. Jika auditor menyimpulkan bahwa ada kemungkinan salah saji yang tinggi seperti sebuah, mengabaikan kontrol internal, ia akan menilai risiko yang melekat sebagai tinggi. An example of inherent risk: the valuation of inventory is inherently more risky when the type of inventory is difficult to value due to its nature, so the valuation of diamonds are inherently much more risky than, say, tennis balls. Salah satu contoh risiko yang melekat: penilaian persediaan secara inheren lebih berisiko ketika jenis persediaan sulit untuk nilai karena sifatnya, sehingga penilaian berlian secara inheren jauh lebih berisiko daripada, katakanlah, bola tenis. Internal controls are ignored during the assessment of inherent risk

because they are considered when assessing another component of audit risk, namely control risk. kontrol internal diabaikan selama penilaian risiko yang melekat karena mereka dianggap saat menilai lain komponen risiko audit, yaitu pengendalian risiko. The assessment of inherent risk (and also control risk) is an exercise that requires professional judgement on the part of the auditor. Penilaian risiko yang melekat (dan juga risiko kontrol) adalah latihan yang memerlukan pertimbangan profesional di pihak auditor. Hence, two auditors assessing the same company may assess the inherent and control risks differently, but it is to be expected that their assessments should be in the same vicinity. Oleh karena itu, dua auditor menilai perusahaan yang sama dapat menilai risiko yang melekat dan kontrol berbeda, namun diharapkan bahwa penilaian mereka harus di sekitar sama. Auditors express their risk assessment in one of two ways (and this goes for all the components of the risk formula): as a percentage, or described as low, medium or high. Auditor mengungkapkan penilaian risiko mereka dalam salah satu dari dua cara (dan ini berlaku untuk semua komponen rumus resiko): sebagai persentase, atau digambarkan sebagai rendah, sedang atau tinggi. Unlevered beta requires the ratio between the equity value and the value of the firm measured in market value terms. Beta leverage membutuhkan rasio antara nilai ekuitas dan nilai perusahaan diukur dari segi nilai pasar. When a company has no debt, ie is unlevered, its asset beta is obviously equal to its equity beta. Ketika sebuah perusahaan memiliki utang tidak, yaitu adalah leverage, beta aset adalah jelas sama dengan beta ekuitas.

B. Risiko Kontrol (Pengendalian)

Kontrol risiko adalah risiko bahwa kebijakan pengendalian internal klien dan prosedur gagal untuk mendeteksi atau mencegah salah saji material dari terjadi. Risiko kontrol berkenaan dengan kemungkinan adanya kekeliruan dalam segmen audit yang melampaui batas toleransi yang tidak terdeteksi atau tidak dapat dicegah oleh pengendalian internal. Resiko pengendalian dipengaruhi oleh faktor efektivitas pengendalian internal, dan keandalan penetapan risiko yang direncanakan (penetapan di bawah 100%), oleh karena itu bila resiko pengendalian ditetapkan tinggi, maka auditor harus mengumpulkan bukti audit yang lebih banyak.

Like inherent risk, control risk is out of the hands of the auditor; however, its magnitude can be assessed. Seperti risiko bawaan, risiko pengendalian yang keluar dari tangan auditor, namun besarnya bisa dinilai. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed,

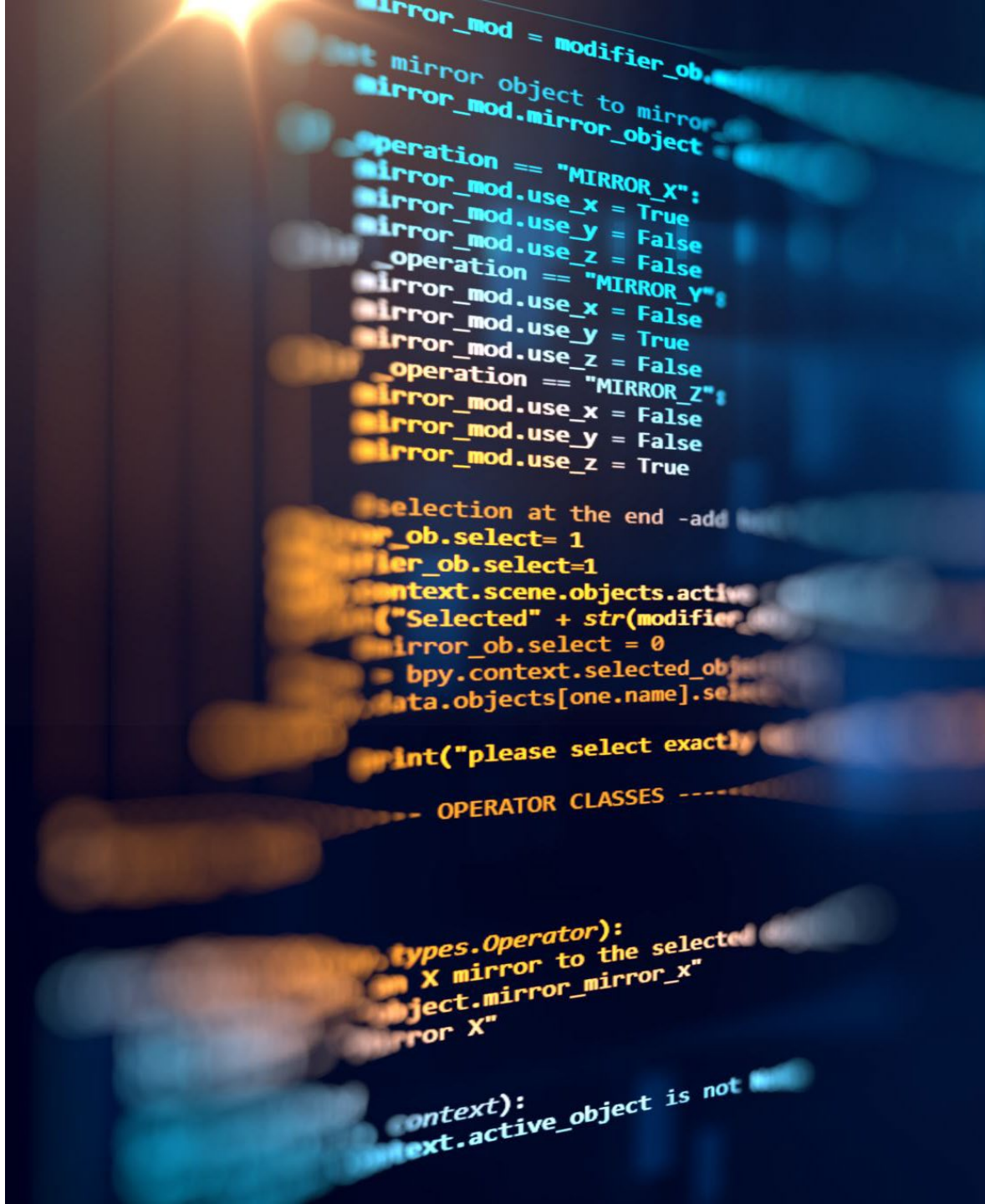
owing to the volume of logged information. Sebagai contoh, risiko pengendalian yang berhubungan dengan review manual log komputer bisa tinggi karena kegiatan memerlukan penyelidikan yang sering mudah terlewatkan, karena volume informasi login. The control risk associated with computerized data validation procedures is ordinarily low if the processes are consistently applied. Pengendalian risiko yang berkaitan dengan prosedur validasi data komputerisasi ini biasanya rendah bila proses ini diterapkan secara konsisten.

C. Resiko Deteksi

Resiko pendeteksian berkenaan dengan kemungkinan terjadinya kekeliruan dalam segmen audit yang melampaui batas toleransi yang tidak terdeteksi karena pengujian menggunakan uji petik, prosedur audit yang tidak tepat/ salah aplikasi, kekeliruan interpretasi atas hasil implementasi prosedur audit. Guna meminimalkan risiko pendeteksian, auditor harus mengembangkan perencanaan audit secara tepat, dan melakukan supervisi atas pelaksanaan audit.

Resiko deteksi didefinisikan sebagai kemungkinan bahwa salah saji material berkaitan dengan pernyataan yang tidak akan terdeteksi oleh substantif pengujian auditor. Risiko deteksi juga diartikan sebagai risiko bahwa auditor tidak akan dapat mendeteksi salah saji material yang ada dalam suatu asersi. Dalam tahap-tahap audit atas laporan keuangan, penentuan risiko deteksi terletak pada tahap auditor mendesain pengujian substantif.

SOFTWARE IT AUDIT



JENIS RESIKO AUDIT

Control Risk (Risiko Pengendalian)
Adalah ukuran penetapan auditor akan kemungkinan adanya kekeliruan (salah saji) dalam segmen audit yang melampaui batas toleransi yang tidak terdeteksi atau tercegah oleh struktur pengendalian intern klien.

ManageEngine
ADAudit Plus

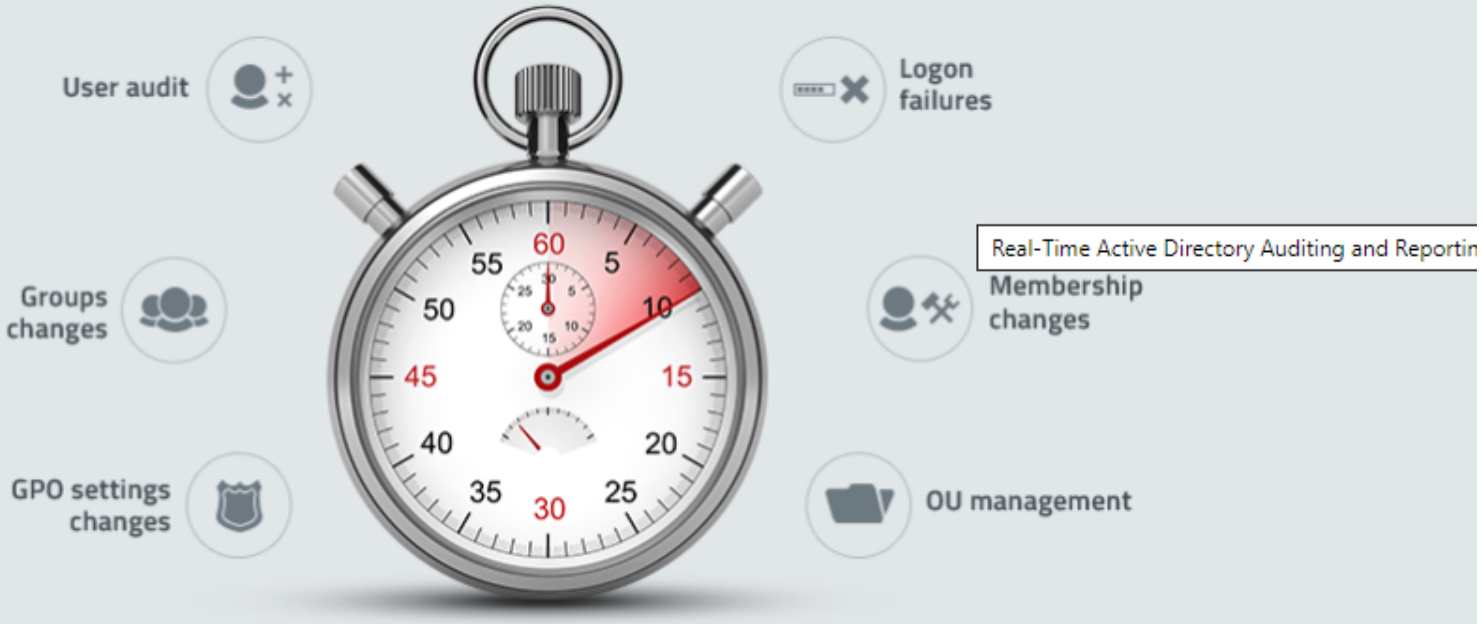
Products Store Partners Support |

Overview Features Demo Resources Get Quote Support Download

Real-Time Auditing for Active Directory

with 200+ audit reports & e-mail alerts

Download



Real-Time Active Directory Auditing and Reportin

ACTIVE DIRECTORY AUDITING

LOGON/LOGOFF AUDITING

FILE SERVER AUDITING

WINDOWS SERVERS AUDITING

REAL-TIME WINDOWS ACTIVE DIRECTORY AUDITING

In real-time, ensure critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes with 200+ detailed event specific GUI reports and email alerts.

Insider Threats

User Logon

Compliance

WINDOWS LOGON/LOGOFF AUDITING

Audit the critical user workstation logon & logoff time to monitor the logon duration, logon failures, logon history and terminal services activity. View & Schedule graphical reports with Email alerts for periodic analysis & quick response during security threats.

Logon / Logoff

Windows user workstations auditing reveals the exact logon and logoff time to quickly verify the user's status at the

Compliance

SMBs or Large organizations have to comply with industry specific Compliance Act like SOX, HIPAA, GLBA,

Data Archiving

From within the product, run periodic archiving of audited events data to save on disk space. View reports from past

WINDOWS FILE SERVER AUDITING

Securely track the file creation, modification & deletion from an authorized / unauthorized access, with detailed forensics of security and permission changes to the documents in their files / folder structure and shares.

File Servers

With Windows File Server Auditing in a Microsoft Server Environment, securely monitor and view pre-configured reports / get instant email alerts for the

Access Permissions

Audit the security settings to know-it-all on your network shares in Windows. Keep track of every 'file/folder, shares & permission' modifications! Track the

Failover Clusters

Audit and Monitor the Windows File Server Failover Clusters. Track user file server cluster share and access permissions. Also, Audit files share

WINDOWS SERVERS AUDITING

Track the Logon/Logoff, Schedule to track events like RADIUS Logon, Terminal Services Activity, Logon Duration and Logon History. Audit related processes can be kept tab by Tracking Windows Schedule jobs.

Windows Servers

With Windows Member Server Auditing, track logon / logoff and monitor critical Terminal Services activity like policy changes with scheduled jobs, object

Printer Auditing

Administrators can centrally audit, monitor and track all files that are printed over the Windows Server network, with thorough reports on the

File integrity Monitoring

File Integrity Monitoring helps monitor the changes to the Windows system, configuration, program files (Log, audit, text, exe, web, configuration, DB files),

DEMO : HTTPS://WWW.YOUTUBE.COM/WATCH?V=X6SJRLSDQQU

TIGA JENIS RISIKO AUDIT IT

KELOMPOK 4 :
Yuniarti Denita Sari
Raju Septa Wijaya
Hendri

JENIS RISIKO AUDIT

1. Inherent Risk (IR) / Risiko Bawaan

Adalah risiko yang mungkin timbul akibat karakter bawaan dari suatu transaksi, entah karena:

(a) kompleksitas transaksi dan klas transaksi; atau

(b) kompleksitas perhitungan; atau

(c) aset yg mudah tercuri/digelapkan; atau

(d) ketiadaan informasi yang sifatnya obyektif.

Sudah menjadi pemahaman publik bahwa inherent risk adalah diluar jangkauan auditor dalam melakuk an pencegahan. Bahkan, juga diluar kendali pihak auditee sendiri. Dengan kata lain, auditor hanya bisa menemukan tetapi tidak bisa melakukan apa-apa.

JENIS RISIKO AUDIT

2. Control Risk (CR) / Risiko Pengendalian

Adalah risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, entah karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain—thus tidak mampu mencegah potensi salahsaji bersifat material dan/atau penggelapan (fraud). CR tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee jika mereka mau.

3. Detection Risk (DR) / Risiko Deteksi

Adalah risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud). DR ada dalam kendali auditor. Karena DR sepenuhnya ada pada kendali auditor, maka sudah pasti mereka harus berupaya untuk menekan risiko ini hingga ke tingkatakan yang paling minimal (tidak mungkin menghilangkan risiko ini sepenuhnya).

CONTOH Control Risk (CR) / Risiko Pengendalian

PT Bank Mandiri (Persero) Tbk yang mengalami sistem error yang menyebabkan saldo nasabahnya berubah pada saat proses backup data rutin. Dimana Manajemen Bank Mandiri memastikan bahwa perubahan drastis saldo rekening yang dialami nasabahnya bukan karena penipuan atau fraud. Perubahan saldo terjadi karena sistem error saat proses backup data rutin.

Bila yang terjadi adalah fraud, seharusnya saldo nasabah berkurang. Namun, yang terjadi adalah saldo nasabah ada yang bertambah dan berkurang secara acak (random). Manajemen Bank Mandiri pun menjelaskan kronologi sistem eror yang menyebabkan 10% nasabahnya atau sekitar 1,5 juta nasabah mengalami perubahan saldo. Insiden Bank Mandiri ini dinilai terjadi karena human error, bukan karena kerusakan pada piranti keras atau hardware. Sebab bila terjadi kegagalan pada hardware, proses pemindahan data dari satu perangkat ke perangkat lain semestinya gagal dilakukan.Dengan demikian , perubahan nominal tabungan pada nasabah seharusnya tidak terjadi jika terdapat kerus akan pada hardware.

Perubahan saldo nasabah ini sendiri terjadi pada Sabtu dini hari dibulan Juli. Bermula dari bank yang melakukan proses tutup buku rutin di akhir hari. Saat proses itu berlangsung, data nasabah dipindahkan dalam sebuah backup server. Kemudian, core server memproses transaksi yang terjadi di hari sebelumnya. Namun gangguan itu tidak berpengaruh terhadap transaksi di luar rekening tabungan nasabah, misalnya e-money, pembayaran surat izin mengemudi (SIM), dan sebagainya. Sebab, menurutnya transaksi itu terlepas dari sistem backup data nasabahnya.

PENGENDALIAN DARI CONTOH AUDIT SEBELUMNYA :

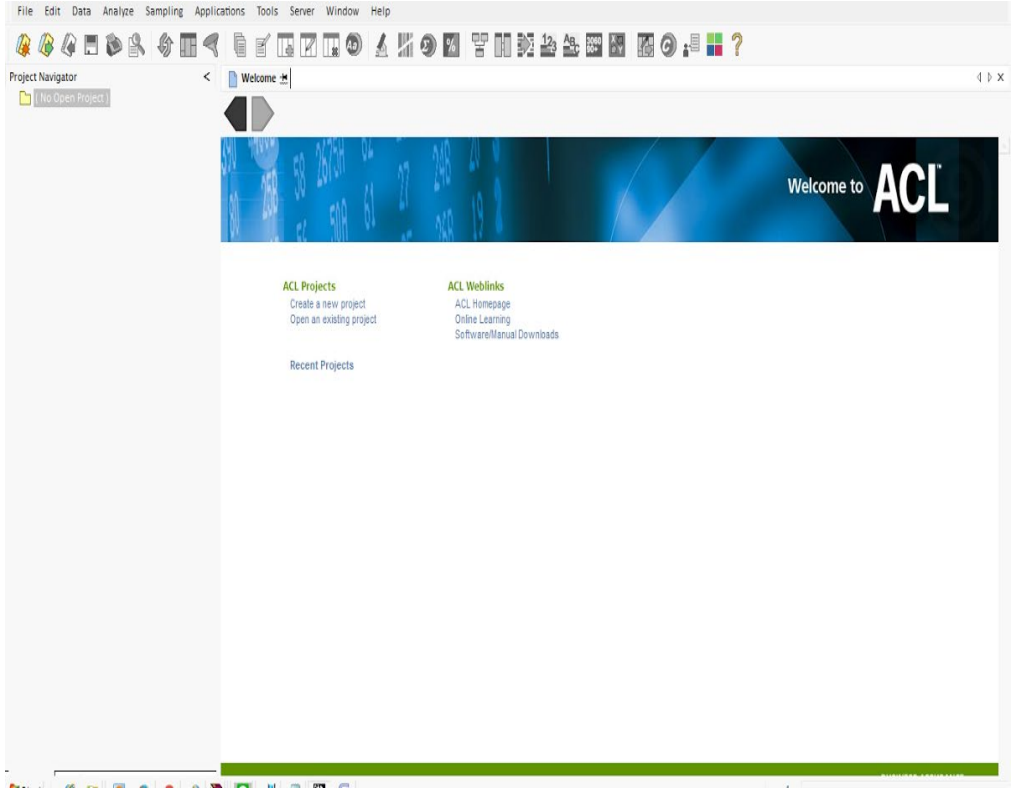
- Perlunya pengecekan secara berlapis (double checking). Dimana sebelum eksekusi perpindahan data, ada orang lain yang melakukan pengecekan ulang lagi (investigasi lebih lanjut, yang diperiksa kembali, apakah memang permasalahan tersebut dari hardware, software, atau human eror).
- Perlunya proses perekrutan pegawai TI sesuai dengan prosedur yang ada.

Tools yang digunakan :

ACL

ACL (Audit Command Language) merupakan sebuah software CAAT (Computer Assisted Audit Techniques) yang sudah sangat populer untuk melakukan analisa terhadap data dari berbagai macam sumber.

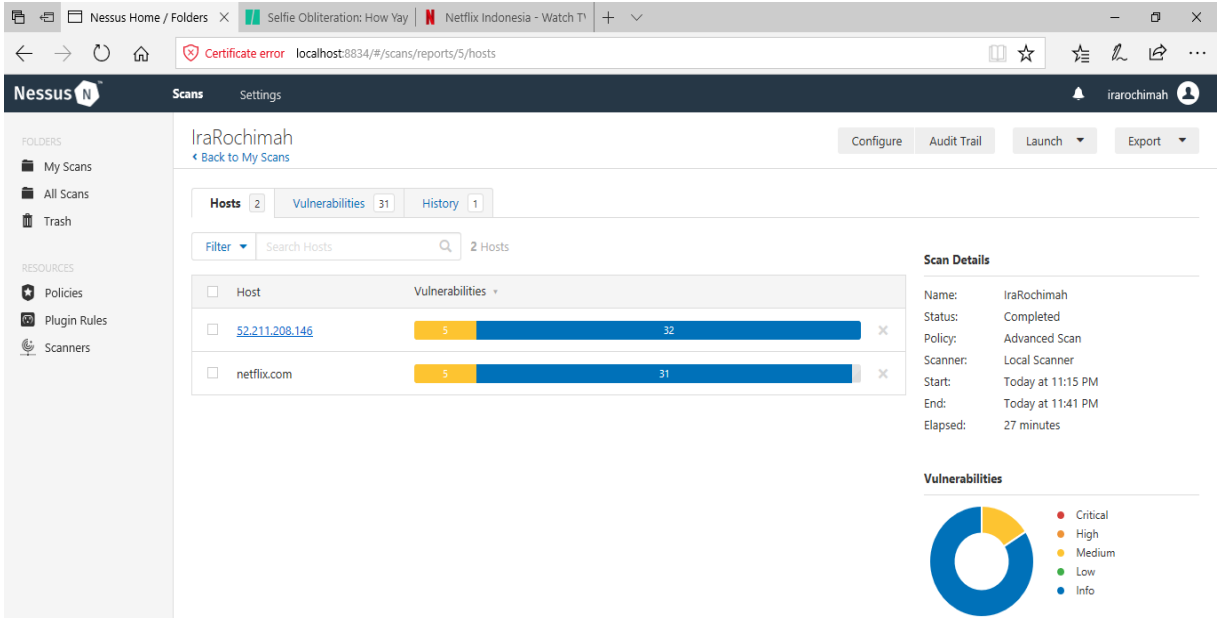
ACL for Windows (sering disebut ACL) adalah sebuah software TABK(TEKNIK AUDIT BERBASIS KOMPUTER) untuk membantu auditor dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik.



Tools yang digunakan :

NESSUS

Nessus adalah termasuk kelompok scanner gratis baru. Nessus bekerja dengan memeri ksa target yang anda telah anda tentukan, seperti Sekumpulan host / bisa juga host dalam fokus tersendiri. Begitu aktivitas scan selesai, anda dapat melihat informasi hasilnya, baik dalam bentuk grafikal atau baris. Interface (tampilan) grafikal Nessus dibangun dengan menggunakan Gimp Toolkit (gtk). Gtk adalah sebuah library gratis yang banyak digunakan untuk membangun interface grafikal dibawah X. Alasan kenapa kebanyakan Administrator Security Computer memilih Nessus adalah karena distribusi aplikasi ini selalu up to date (selalu diperbaharui), berbasis web interface, mudah dioperasikan dan gratis.



Fungsi Nessus yaitu digunakan untuk mencari kelemahan pada sebuah sistem komputer. Nessus juga dapat melakukan pengecekan terhadap kerentanan system komputer, dan meningkatkan keamanan sistem yang kita miliki.

TERIMA KASIH

IT AUDIT

Nama : Ilsa Palingga Ninditama (182420061)

Program Studi Teknik Informatika S-2

Pascasarjana Universitas Bina Darma

SOAL

- Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

  Jelaskan bagaimana resiko-resiko tersebut dikendalikan

JAWABAN :

Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan. Di lain pihak, seiring makin meluasnya implementasi sistem informasi maka kesadaran akan perlunya dilakukan review atas pengembangan suatu sistem informasi semakin meningkat. Kesadaran ini muncul karena munculnya berbagai kasus yang terkait dengan gagalnya sistem informasi, sehingga memberikan akibat yang sangat mempengaruhi kinerja organisasi.

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya “scope creep” (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang

telah diterima secara internasional adalah CISA (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Kemudian, menurut saya cara mengendalikan resiko yang ada yaitu dengan cara organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (*IT Governance*). Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (*Control Objectives for Information and Related Technology*) adalah standar internasional untuk tata kelola TI yang dikembangkan oleh ISACA (*Information System and Control Association*) dan ITGI (*IT Governance Institute*) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.

Tugas IT Audit

Indri Endang Lestari (182420046)

A. Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

Jawab :

Resiko :

1. Kehilangan data
2. Kesalahan pengambilan keputusan
3. Penyalahgunaan computer
4. Nilai investasi
5. Aspek privasi
6. Kesalahan pengoperasian computer
7. Evolusi teknologi

B. Jelaskan bagaimana resiko-resiko tersebut dikendalikan (lihat contoh Risk Management Framework yang terlampir)

Jawab :

Adapun resiko tersebut sejatinya tidak dapat diselesaikan hanya saja resiko tersebut dapat dikurangi, menggunakan best practices. Ada banyak macam best practices yang bisa digunakan, seperti COBIT, ITIL, ISO 2700 1/2, COSO ERM, PRINCE2, PMBOK, Six Sigma, dan Togaf.

- Email password may be disclosed
- Facebook account may be used by someone else
- Credit card information may be disclosed
- Customer information may be stolen
- IT Service delivery to the customers may be poor
- IT systems may be obsolete
- IT projects may be late or fail
- IT systems do not provide any business benefit
- Risk of non-compliance with the regulator
- Own people may harm the systems

TUGAS PENGEDALIAN RESIKO IT RISK

M APRILIANSYAH R

NIM 182420064

MEGITER TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BINA DARMA
PALEMBANG
2019

SOAL

Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi? jelaskan bagaimana resiko-resiko tersebut dikendalikan ?

JAWABAN

Pengendalian dan audit atas teknologi informasi perlu dilakukan mengingat besarnya risiko yang harus dihadapi oleh organisasi berkaitan dengan penggunaan teknologi informasi. Risiko-risiko tersebut antara lain :

Resiko Kehilangan Data

Data merupakan aset teknologi informasi yang sangat kritikal bagi kelangsungan operasional perusahaan. Dapat dibayangkan apabila sebuah organisasi mengalami kehilangan data,misalnya data piutang atau data pelanggan. Apa yangakan terjadi ?

Resiko Kesalahan Pengambilan Keputusan

Sebuah keputusan pada umumnya diambil berdasarkan data dan informasi yang tersedia. Apa yang akan terjadi apabila data dan informasi yang tersedia tidak akurat, tidak lengkap, tidak tepat waktu dan tidak relevan ?

Resiko Penyalahgunaan Komputer

Risiko kemungkinan penyalahgunaan teknologi yang dapat mengakibatkan kerugian yang bahkan tidak terbayangkan. Risiko tersebut dapat berupa ancaman fisik seperti penghancuran dan pencurian aset dan non-fisik seperti hacking, virus, penyalahgunaan akses.

Resiko Nilai Investasi

Sebagian besar investasi dalam teknologi informasi memerlukan dana yang tidak sedikit dan cenderung sulit dikendalikan. Di Indonesia, belum banyak organisasi yang melakukan analisa cost & benefit sebelum melakukan investasi teknologi informasi.

Resiko Aspek Privasi

Banyak data dan informasi yang bersifat pribadi tersimpan dalam sistem komputer, seperti misalnya apabila kita mempunyai kartu kredit, maka data tanggal lahir, tempat tinggal, pekerjaan dan lain-lainnya yang terkadang merupakan informasi pribadi akan tersimpan dalam sistem komputer penyedia kartu kredit.

Resiko Kesalahan Pengoperasian Komputer

Akibat kesalahan pengoperasian komputer dapat berupa kerugian finansial dari Rp.0 sampai kepada kebangkrutan bahkan kerugian jiwa.

Resiko Evolusi Teknologi

Teknologi informasi, seperti halnya teknologi yang lain mempunyai sifat netral. Sisi baik dan sisi buruk akibat pemanfaatannya tergantung kepada siapa penggunanya dan untuk apa digunakan.

SOAL

jelaskan bagaimana resiko-resiko tersebut dikendalikan ?

JAWABAN

Pengendalian adalah salah satu fungsi manajemen yang merupakan pengukuran dan koreksi semua kegiatan di dalam rangka memastikan bahwa tujuan dan rencana perusahaan dapat terlaksana dengan baik . Dengan kata lain, pengendalian risiko adalah suatu tindakan atau usaha untuk menyelamatkan perusahaan dari kerugian.

beberapa cara yang dapat dilakukan perusahaan untuk Pengendalian meminimumkan risiko :

1. Melakukan pencegahan dan penggurangan terhadap kemungkinan terjadinya peristiwa yang menimbulkan kerugian,

2. Melakukan retensi, mentolerir membiarkan terjadinya kerugian, dan untuk mencegah tergantungnya operasi perusahaan akibat kerugian tersebut disediakan sejumlah dana untuk menanggulanginya (contoh: pos biaya lain-lain atau tak terduga dalam anggaran perusahaan
3. Melakukan pengendalian terhadap risiko, contohnya melakukan hedging(perdagangan berjangka) untuk menanggulangi risiko kelangkaan dan fluktuasi harga dan bahan baku/pembantu yang diperlukan.
4. Mengalihkan/memindahkan risiko kepada pihak lain, yaitu dengan cara mengadakan kontrak pertanggungan (asuransi) dengan perusahaan asuransi terhadap risiko tertentu, dengan membayar sejumlah premi asuransi yang telah ditetapkan, sehingga perusahaan asuransi akan mengganti kerugian bila betul-betul terjadi kerugian yang sesuai perjanjian
5. pada prinsipnya dapat menggunakan dua pendekatan/cara menanggulangi risiko:
    1. Penanganan Risiko (Risk Control)
    2. Pembiayaan Risiko (Risk Financing)

TASK 2: PENGENDALIAN RISIKO

OLEH:

MUHAMMAD DIAH MAULIDIN (182420075)

KELAS : **REGULER A R1**
MATA KULIAH : **IT AUDIT**

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

SOAL

Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

Jelaskan bagaimana resiko-resiko tersebut dikendalikan (lihat contoh Risk Management Framework yang terlampir)

JAWABAN

Jenis risiko penggunaan TI yang dapat terjadi pada suatu organisasi yaitu:

1. Karyawan atau orang yang berada di dalam suatu organisasi yang dapat membahayakan sistem TI.
2. Risiko ketidakpatuhan organisasi terhadap regulator, salah satu contoh perusahaan TI dengan pemerintah.
3. Penggunaan sistem TI yang tidak memberikan manfaat atau keuntungan dari proses bisnis suatu organisasi.
4. Waktu proyek TI yang dijalankan suatu organisasi tidak dimanfaatkan dengan baik dan proyek TI yang tidak selesai (gagal).
5. Penggunaan sistem TI dalam organisasi yang tidak update.
6. Servis TI yang dijalankan suatu organisasi tidak sesuai apa yang diharapkan oleh pelanggan.
7. Informasi atau data pelanggan yang rentan diambil oleh orang yang bukan memiliki hak data tersebut.
8. Informasi data finansial seperti data kartu kredit dari pelanggan yang ditampilkan oleh suatu organisasi.
9. Akun sosial media dari karyawan suatu organisasi digunakan oleh orang yang tidak bertanggung jawab.

Beberapa risiko penggunaan TI tersebut dapat dikendalikan dengan penerapan *best practices*. Tidak ada 100% solusi yang dapat meminimalisir masalah penggunaan TI. Tetapi dapat mengurangi masalah tersebut dengan penerapan *best practices* (panduan/standar)

Keuntungan menggunakan *best practices* yaitu:

1. Kepemilikan dengan akuntanbilitas dan tanggung jawab yang lebih baik.
2. Tidak menyalahkan risiko penggunaan TI.
3. Manajemen yang lebih baik.
4. Manfaat yang baik melalui investasi TI.
5. Kepatuhan yang baik.
6. Pemantauan yang lebih baik.
7. Dapat dibandingkan dengan yang lain.

Beberapa contoh dari *best practices* yang dapat diterapkan oleh suatu organisasi yaitu:

- COBIT
- ITIL
- ISO 27001/2
- COSO ERM
- PRINCE2
- PMBOK
- Six Sigma
- TOGAF

PENGENDALIAN RESIKO

Oleh:

Muhammad Irvai (182420063)

Mata Kuliah : IT Audit

Dosen Pengampu: Dr. Widya Cholil., M.IT

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

PENGENDALIAN RESIKO

Resiko merupakan suatu sistem informasi dapat dikembangkan karena adanya kebijakan dan perencanaan telebih dahulu. Tanpa adanya perencanaan sistem yang baik, pengembangan sistem tidak akan dapat berjalan sesuai dengan yang diharapkan. Tanpa adanya kebijakan pengembangan sistem oleh manajemen puncak, maka pengembangan sistem tidak akan mendapat dukungan dari manajemen puncak tersebut.

Suatu organisasi perlu memiliki fungsi penerapan manjemen resiko penggunaan sistem informasi dalam suatu organisasi yang melibatkan pihak-pihak yang memiliki resiko dan yang memantau suatu resiko serta yang melakukan test dan verifikasi. Suatu organisasi perlu memiliki kebijakan bahwa identifikasi, pengukuran dan pemantauan risiko setiap aktivitas secara periodik yang dilakukan oleh lembaga yang dibuat seperti Satuan Kerja Manajemen Resiko bekerjasama dengan satuan penyelenggara informasi dan satuan kerja pengguna informasi. Pelaksannan pengelolaan resiko tetap merupakan tanggung jawab dari tim kerja atau petugas yang melaksanakan fungsi-fungsi tersebut,oleh karena itu suatu manajemen informasi wajib memastikan pemantauan yang memadai dan pelaporan mengenai aktivitas terkait informasi dan resikonya.

Berikut adalah **pengertian resiko** menurut para ahli :

1. Pengertian resiko menurut A. Abas Salim
   “Resiko adalah ketidaktentuan (uncertainty) yang mungkin melahirkan peristiwa kerugian (loss)”.
2. Arthur Williams dan Richard, M. H
   “Resiko adalah suatu variasi dari hasil-hasil yang dapat terjadi selama periode tertentu”.
3. Prof Dr.Ir. Soemarno, M.S.
   “Suatu kondisi yang timbul karena ketidakpastian dengan seluruh konsekuensi tidak menguntungkan yang mungkin terjadi disebut resiko”.

4. Sri Redjeki Hartono

   ”Resiko adalah suatu ketidakpastian di masa yang akan datang tentang kerugian”.

5. Sedangkan menurut Kamus Besar Bahasa Indonesia

   “Resiko adalah kemungkinan terjadinya peristiwa yang dapat merugikan perusahaan".

Sedangkan jenis-jenis resiko di bagi menjadi 4 bagian yaitu :

1. **Resiko murni (pure risk)**

   Adalah suatu resiko dengan kemungkinan yang timbul hanya 2 (dua) yaitu ada kerugian (loss) atau sama sekali tidak ada kerugian (no loss atau break even).

2. **Resiko khusus (partikulasis)**

   Adalah suatu resiko yang berasal dari kejadian – kejadian khusus dan dampak nya dirasakan dari local saja

3. **Resiko spekulatif risk**

   Adalah suatu resiko yang kemungkinan terjadinya hanya ada 3 yaitu ada kerugian (loss), tidak ada kerugian (no loss), atau ada keuntungan (profit)

4. **Resiko fundamental**

   Adalah resiko yang tidak menyangkut diri pribadi baik, resiko ini disebabkan oleh sikap masyarakat tertentu dan dampak nya dirasakan dari masyarakat luar.

Pada **dunia teknologi** terutama dibidang teknologi informasi atau sistem informasi, **jenis – jenis resiko** di bagi menjadi 6 (enam) bagian yaitu :

1. **Technologi Risk**, seperti:
   a. Komponen file tidak lengkap
   b. Sistem operasi tidak kompatibel, device tidak dikenal
   c. Perangkat keras tidak mendukung (mis: resolusi monitor, resolusi printer)

d. Spesifikasi tidak memenuhi
e. Kualitas Network dibawah standar kebutuhan
f. Browser, software tidak memenuhi

2. **People Risk**, seperti:
   a. Keluarnya programmer utama
   b. Skill/kemampuan tidak memenuhi
   c. Project manager tidak mampu membuat/melakukan koordinasi
   d. Tim yang terlibat tidak mematuhi job disk
   e. Tim tidak punya disiplin dan target(hanya berorientasi hasil, proses diabaikan)

3. **Organizational Risk**, seperti:
   a. Restruturisasi
   b. Pembuatan fungsi dan tugas
   c. Perpindahan penugasan/kebijakan
   d. Overload/kemampuan organisasi tidak sesuai kapasitasnya

4. **Tools Risk**, seperti:
   a. Hasil pengembangan tidak bisa diintegrasikan
   b. Tools yang dikehendaki tidak dikuasai pengembang
   c. Versi pengembangan tidak memenuhi kebutuhan

5. **Requirement Risk**, seperti:
   a. Adanya pemahaman yang berbeda antar bagian yang terlibat
   b. Adanya batasan yang melebihi ruang lingkup
   c. Adanya informasi yang tidak lengkap
   d. Kurang detailnya proses bisnis
   e. Ketidakjelasan dari costumer tentang proses bisnisnya

6. **Estimate Risk**, seperti:
   a. Berkaitan dengan *over budget*, perlunya menghitung ulang akibat kesalahan estimasi
   b. Berkaitan dengan ketepatan waktu, perlunya menskedule ulang jadwal
   c. Berkaitan dengan *Resource*

Resiko-resiko dapat dikendalikan menggunakan *framework* manajemen resiko Teknologi Informasi, salah satu diantaranya menggunakan **COBIT**.

COBIT (Control Objectives for Information and Related Technology) merupakan standard yangdikeluarkan oleh *ITGI (The IT Governance Institute)*. COBIT merupakan suatu koleksi dokumen dan *framework* yang diklasifikasikan dan secara umum diterima sebagai *best practice* untuk tata kelola *(IT Governance)*, kontrol dan jaminan TI. Referensi perihal manajemen resiko secara khusus dibahas pada proses PO9 dalam COBIT. Proses-proses yang lain juga menjelaskan tentang manajemen resiko namun tidak terlalu detail.

Resiko adalah segala hal yang mungkin berdampak pada kemampuan organisasi dalam mencapai tujuantujuannya. *Framework* manajemen resiko TI dengan menggunakan COBIT terdiri dari :

1. **Penetapan Objektif**

   Kriteria informasi dari COBIT dapat digunakan sebagai dasar dalam mendefinisikan objektif TI. Terdapat tujuh kriteria informasi dari COBIT yaitu : *effectiveness, efficiency, confidentiality, integrity, availability, compliance*, dan *reliability*.

2. **Identifikasi Resiko**

   Identifikasi resiko merupakan proses untuk mengetahui resiko. Sumber resiko bisa berasal dari :
   a. Manusia, proses dan teknologi
   b. Internal (dari dalam perusahaan) dan eksternal (dari luar perusahaan)

c. Bencana (hazard), ketidakpastian (uncertainty) dan kesempatan (opportunity).

   Dari ketiga sumber resiko tersebut dapat diketahui kejadian-kejadian yang dapat mengganggu perusahaan dalam mencapai objektifnya.

3. Penilaian Resiko Proses

untuk menilai seberapa sering resiko terjadi atau seberapa besar dampak dari resiko. Dampak resiko terhadap bisnis (business impact) bisa berupa : dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapatdinilai (sistem dan data), dan penundaan proses pengambilan keputusan.

Sedangkan kecenderungan *(likelihood)* terjadinya resiko dapat disebabkan oleh sifat alami dari bisnis, struktur dan budaya organisasi, sifat alami dari sistem (tertutup atau terbuka, teknologi baru dan lama), dan kendali-kendali yang ada. Proses penilaian resiko bisa berupa resiko yang tidak dapat dipisahkan *(inherent risks)* dan sisa resiko *(residual risks).*

4. Respon Resiko

Untuk melakukan respon terhadap resiko adalah dengan menerapkan kontrol objektif yang sesuai dalam melakukan manajemen resiko. Jika sisa resiko masih melebihi resiko yang dapat diterima *(acceptable risks)*, maka diperlukan respon resiko tambahan. Proses-proses pada framework COBIT (dari 34 *Control Objectives*) yang sesuai untuk manajemen resiko adalah :

a. PO1 *(Define a Stretegic IT Plan)* dan PO9 *(Assess and Manage Risks)*

b. AI6 *(Manages Change)*

c. DS5 *(Ensure System and Security)* dan DS11 *(Manage Data)*

d. ME1 *(Monitor and Evaluate IT Performance)*

5. **Monitor Resiko**

   Setiap langkah dimonitor untuk menjamin bahwa resiko dan respon berjalan sepanjang waktu

TUGAS PENGENDALIAN RESIKO

Nama : Nurhachita

Kelas : MTi Reguler A

NIK : 182420065

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

PASCASARJANA UNIVERSITAS BINA DARMA

PALEMBANG

2019

Resiko adalah suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisa serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko.

Seiring dengan berkembangnya teknologi informasi yang bergerak sangat cepat dewasa ini, pengembangan unit usaha yang berupaya menerapkan sistem informasi dalam organisasinya telah menjadi kebutuhan dasar dan semakin meningkat dari tahun ke tahun. Akan tetapi pola pembangunan sistem informasi yang mengindahkan faktor resiko telah menyebabkan beberapa organisasi mengalami kegagalan menerapkan teknologi informasi tersebut, atau meningkatnya nilai investasi dari *plafon* yang seharusnya, hal ini juga dapat menghambat proses pencapaian misi organisasi.

Jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi :

Pada dasarnya, faktor resiko dalam suatu perencanaan sistem informasi, dapat diklasifikasikan ke dalam 4 kategori resiko, yaitu :

a. *Catastrophic* (Bencana)

b. *Critical* (Kritis)

c. *Marginal* (kecil)

d. *Negligible* (dapat diabaikan)

Adapun pengaruh atau dampak yang ditimbulkan terhadap suatu proyek sistem informasi dapat berpengaruh kepada

a) nilai unjuk kerja dari sistem yang dikembangkan,

b) biaya yang dikeluarkan oleh suatu organisasi yang mengembangkan teknologi informasi,

c) dukungan pihak manajemen terhadap pengembangan teknologi informasi, dan

d) Jadwal waktu penerapan pengembangan teknologi informasi.

Suatu resiko perlu didefinisikan dalam suatu pendekatan yang sistematis, sehingga pengaruh dari resiko yang timbul atas pengembangan teknologi informasi pada suatu organisasi dapat diantisipasi dan di identifikasi sebelumnya. Mendefinisikan suatu resiko dalam pengembangan teknologi informasi pada suatu organisasi terkait dengan Siklus Hidup Pengembangan Sistem (*System Development Life Cycle* [SDLC]), dimana fase-fase penerapan SDLC dalam pengembangan teknologi informasi di spesifikasikan analisa resiko.

Pola Pendekatan

System Development Life Cycle [SDLC] adalah suatu tahapan proses perancangan suatu sistem yang dimulai dari tahap investigasi; pembangunan; implementasi; operasi/perawatan; serta tahap penyelesaian [4]. Dari dasar tersebut di atas, strategi penerapan manajemen resiko perlu mempertimbangkan dampak yang mungkin timbul dengan tingkat probabilitas yang berbeda untuk setiap komponen pengembangan sistem informasi.

Pola pendekatan manajemen resiko juga perlu mempertimbangkan faktor-faktor pada *System Development Life Cycle* (SDLC) yang terintegrasi, yaitu Mengindentifikasikan faktor-faktor resiko yang timbul dan diuraikan disetiap tahap perancangan sistem, yang tersusun sebagai berikut :

1. ***Tahap 1. Investigasi*** : Tahap ini suatu sistem didefinisikan, menyangkut ruang lingkup pengembangan yang akan dibuat, yang semua perencanaan atas pengembangan sistem di dokumentasikan terlebih dahulu. Dukungan yang dibutuhkan dari manajemen resiko pada tahap ini adalah faktor resiko yang mungkin terjadi dari suatu sistem informasi di identifikasikan, termasuk di dalamnya masalah serta konsep pengoperasian keamanan sistem yang semuanya bersifat strategis.
2. ***Pengembangan*** : Tahap ini merupakan tahap dimana suatu sistem informasi dirancang, pembelian komponen pendukung sistem di laksanakan, aplikasi di susun dalam program tertentu, atau masa dimana konstruksi atas sistem di laksanakan. Pada proses ini, faktor resiko diidentifikasikan selama tahap ini dilalui, dapat berupa analisa atas keamanan sistem sampai dengan kemungkinan yang timbul selama masa konstruksi sistem di laksanakan.
3. ***Implementasi*** : Tahap ini kebutuhan atas keamanan sistem dikonfigurasikan, aplikasi sistem di uji coba sampai pada verifikasi atas suatu sistem informasi di lakukan. Pada tahap ini faktor resiko di rancang guna mendukung proses pelaksanaan atas implementasi sistem informasi sehingga kebutuhan riil di lapangan serta pengoperasian yang benar dapat dilaksanakan.
4. ***Pengoperasian dan Perawatan*** : Tahap ini merupakan tahap dimana sistem informasi telah berjalan sebagaimana mestinya, akan tetapi secara secara berkala sistem membutuhkan modifikasi, penambahan peralatan baik perangkat keras maupun perangkat lunak pendukung, perubahan tenaga pendukung operasi, perbaikan kebijakan maupun prosedur dari suatu organisasi. Pada tahap ini manajemen resiko lebih menitik beratkan pada kontrol berkala dari semua faktor yang menentukan berjalannya sistem, seperti perangkat keras, perangkat lunak, analisa sumber daya manusia, analisa basis data, maupun analisa atas jaringan sistem informasi yang ada.
5. **Penyelesaian/penyebaran** : Tahap ini merupakan tahap dimana system informasi yang telah digunakan perlu di lakukan investasi baru karena unjuk kerja atas sistem tersebut telah berkurang, sehingga proses pemusnahan data, penggantian perangkat keras dan perangkat lunak, ataupun berhentinya kegiatan atau kepindahan organisasi ke tempat yang baru. Manajemen resiko yang perlu di perhatikan dalam tahap ini adalah memastikan proses pemusnahan atas komponen-komponen system informasi dapat berjalan dengan baik, terkelola dari segi keamanan.

Setelah pola pendekatan manajemen resiko di definisikan dalam masing-masing tahap SDLC, maka tahap selanjutnya adalah menilai manajemen resiko dalam metodologi tertentu. Upaya memberikan penilaian atas dampak resiko dalam pengembangan sistem informasi,

perlu dilakukan karena dapat memberikan gambaran atas besar atau kecilnya dampak ancaman yang mungkin timbul selama proses pengembangan sistem.

Metodologi Penilaian Resiko

Untuk menentukan kemungkinan resiko yang timbul selama proses pengembangan sistem informasi berlangsung, maka organisasi yang bermaksud mengembangkan sistem informasi perlu menganalisa beberapa kemungkinan yang timbul dari pengembangan sistem informasi tersebut. Adapun metodologi penilaian resiko pengembangan sistem informasi dapat diuraikan dalam 9 langkah, yang tersusun sebagai berikut :

a. Menentukan karakteristik dari suatu sistem

b. Mengidentifikasikan ancaman-ancaman

c. Mengidentifikasikan kelemahan sistem

d. Menganalisa pengawasan

e. Menentukan beberapa kemungkinan pemecahan masalah

f. Menganalisa pengaruh resiko terhadap pengembangan sistem

g. Menentukan resiko

h. Merekomendasikan cara-cara pengendalian resiko

i. Mendokumentasikan hasil keputusan

Tahap ke dua, tiga, empat dan enam dari langkah tersebut di atas dapat dilakukan secara paralel setelah langkah pertama dilaksanakan. Adapun dari setiap langkah tersebut adalah sebagai berikut :

Langkah 1. Menentukan Karakterisasi Sistem

Pada langkah pertama ini batasan suatu sistem yang akan dikembangan di identifikasikan, meliputi perangkat keras, perangkat lunak, sistem interface, data dan informasi, sumber daya manusia yang mendukung sistem IT, tujuan dari sistem, sistem dan data kritis, serta sistem dan data sensitif. Beberapa hal tambahan yang dapat diklasifikasikan pada karakteristik sistem selain hal tersebut di atas seperti bentuk dari arsitektur keamanan sistem, kebijakan yang dibuat dalam penanganan keamanan sistem informasi, bentuk topologi jaringan komputer yang dimiliki oleh organisasi tersebut, Manajemen pengawasan yang dipakai pada sistem TI di organisasi tersebut, dan hal lain yang berhubungan dengan masalah keamanan seputar penerapan Teknologi Informasi di organisasi yang bermaksud mengembangkan sistem informasi.

Adapun teknik pengumpulan informasi yang dapat diterapkan pada langkah ini meliputi :

1. ***Membuat daftar kuesinoner***. Daftar kuesioner ini di susun untuk semua level manajemen yang terlibat dalam sistem dengan tujuan mengumpulkan informasi

seputar keamanan data dan informasi dengan tujuan untuk memperoleh pola resiko yang mungkin dihadapi oleh sistem.

2. ***Interview.*** Bentuk lain dari pengumpulan data dengan cara interview terhadap IT Support atau personil yang terlibat dalam sistem informasi.
3. ***Review atas dokumen.*** Review atas dokumen pengembangan sistem, Dokumen kebijakan, atau dokumen keamanan informasi dapat memberikan gambaran yang bermanfaat tentang bentuk dari kontrol yang saat ini diterapkan oleh SI maupun rencanan pengembangan dari pengawasan di masa depan.
4. ***Penerapan Tool.*** Menggunakan suatu tool aplikasi yang memiliki tujuan untuk mengumpulkan informasi tentang sistem informasi yang digunakan merupakan salah satu cara untuk dapat memetakan sistem secara keseluruhan, seperti penggunakan network monitor, maupun tools lain.

Hasil output dari langkah pertama ini akan menghasilkan Penaksiran atas karakteristik sistem IT, Gambaran tentang lingkungan sistem IT serta gambaran tentang batasan dari sistem yang dikembangkan.

Langkah 2. Mengidentifikasikan ancaman-ancaman

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Timbulnya ancaman dapat dipicu oleh suatu kondisi dari sumber ancaman. Sumber ancaman dapat muncul dari kegiatan pengolahan informasi yang berasal dari 3 hal utama, yaitu (1) Ancaman Alam; (2) Ancaman Manusia, dan (3) Ancaman Lingkungan. Ancaman yang berasal dari manusia memiliki karakteristik tersendiri, serta memiliki alasan tersendiri dalam melakukan gangguan terhadap sistem informasi yang ada. Adapun alasan yang timbul dari ancaman manusia ini dapat di definisikan dalam tabel berikut :

Sumber Ancaman	Alasan	Aksi yang timbul
Hacker, Cracker	• Tantangan • Ego • Memberontak	• Hacking • Social Engineering • Gangguan sistem • Akses terhadap sistem
Kriminal	• Perusakan informasi • Penyingkapan informasi secara ilegal • Keuntungan moneter • Merubah data	• Tindak Kriminal • Perbuatan curang • Penyuapan • Spoofing • Intrusi atas sistem
Teroris	• Surat kaleng • Perusakan • Peledakan • Balas dendam	• Bom/teror • Perang informasi • Penyerangan sistem • Penembusan atas sistem • Tampering sistem
Mata-mata	• Persaingan usaha	• Pencurian informasi • Social engineering

	• Mata-mata ekonomi	• Penembusan atas sistem
Orang dalam Organisasi	• Keingintahuan • Ego • Mata-mata • Balas dendam • Kelalaian kerja	• Surat kaleng • Sabotase atas sistem • Bug sistem • Pencurian/penipuan • Perubahan data • Virus, trojan, dll • Penyalahgunaan komputer

Organisasi yang membutuhkan daftar dari sumber ancaman, perlu melakukan hubungan dengan badan-badan atau sumber-sumber yang berhubungan dengan keamanan, seperti misalnya sumber ancaman dari alam diharapkan hubungan dengan BMG yang menangani masalah alam, atau pihak intelijen atau media massa yang dapat mendeteksi sumber ancaman dari manusia. Hasil output dari ancaman ini merupakan pernyataan atau daftar yang berisikan sumber ancaman yang mungkin dapat mengganggu sistem secara keseluruhan.

Langkah 3. Identifikasi kelemahan

Cacat atau kelemahan dari suatu sistem adalah suatu kesalahan yang tidak terdeteksi yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh sumber ancaman yang mencoba menyusup terhadap sistem tersebut.

Pada beberapa vendor besar, informasi atas kelemahan sistem yang dibuat oleh vendor tersebut ditutup atau dihilangkan dengan penyediaan layanan purna jual dengan menyediakan hot fixes, service pack, pathces ataupun bentuk layanan lain.

Penerapan metode proaktif atau tersedianya karyawan yang bertugas untuk melakukan sistem test dapat di pakai untuk mencek kelemahan sistem secara efisien, dimana hal tersebut tergantung kepada keberadaan sumber daya atau kondisi IT yang bersifat kritis. Metode tes yang diterapkan dapat berbentuk :

- Penggunaan tool yang menscan kelemahan sistem secara automatis
- Adanya Evaluasi dan sekuriti tes (ST&E), atau
- Melakukan penetrasi tes

Penggunaan tools untuk mencek kelemahan sistem diterapkan pada grup perusahaan dengan kelengkapan jaringan komputer yang memadai, yang digunakan untuk memindai beberapa servis sistem yang disinyalir lemah (seperti : Diperbolehkannya anonymous FTP, sendmail automatis, dll). Strategi ST&E merupakan metode tes yang di terapkan pada saat proses penilaian atas resiko dilakukan. Metode ini diterapkan saat pengembangan dan eksekusi atas Sistem Informasi berjalan yaitu pada bagian *test plan*. Kegunaan dari metode ini adalah untuk melihat efektifitas dari kontrol atas sekuriti dari sistem IT terimplementasikan dalam kondisi sistem beroperasi. Penetrasi tes merupakan metode yang digunakan sebagai pelengkap dalam memeriksa kontrol atas sekuriti dan menjamin tidak adanya masalah sekuriti yang mungkin timbul pada sistem IT.

Bentuk keluaran yang timbul pada langkah ketiga ini memungkinkan pihak penilai resiko mendapatkan daftar dari kelemahan sistem yang dapat dianggap sebagai potensi dari sumber ancaman di kemudian hari.

Langkah 4. Analisa pengawasan

Tujuan yang diharapkan pada langkah ini adalah untuk menganalisa penerapan kontrol yang telah diimplementasikan atau yang direncanakan. Bagi organisasi langkah ini perlu untuk meminimalisasi atau bahkan mengeliminasi probabilitas kemungkinan yang timbul dari sumber ancaman atau potensi kelemahan atas sistem.

Metode pengawasan

Metode pengawasan terdiri atas metode yang bersifat teknis maupun non teknis. Metode pengawasan secara teknis merupakan salah satu upaya perlindungan kepada organisasi dalam hal perlindungan terhadap perangkat keras komputer, perangkat lunak maupun mekanisme akses kontrol yang digunakan, sedangkan metode nonteknis lebih ditekankan kepada pengawasan atas manajemen dan operasional penggunaan sistem IT di organisasi tersebut, seperti penerapan policy keamanan, prosedur operasional, maupun manajemen personel yang ada.

Kategori pengawasan

Kategori pengawasan baik secara teknis maupun non teknis dapat diklasifikasikan dalam 2 pendekatan yaitu pendekatan preventif atau detektif.

Pendekatan preventif adalah upaya untuk mencegah upaya pelanggaran atas policy keamanan seperti pengaksesan atas sistem IT atau tindakan lain misalnya dengan cara mengenkripsi informasi atau menerapkan otentifikasi atas informasi.

Pendekatan detektif adalah cara untuk memperingati pengguna atas terjadinya pelanggaran atau percobaan pelanggaran atas policy keamanan yang ada, metode ini contoh pada Microsoft Windows dengan menggunakan teknik audit trails, metode deteksi penyusupan atau teknik checksum.

Teknis analisa pengawasan

Analisa pengawasan atas policy keamanan dapat menggunakan teknik checklist pengguna yang mengakses sistem IT atau dengan penggunaan checklist yang tersedia untuk memvalidasi keamanan, hal paling penting pada tahap ini adalah mengupdate terus menerus atas checklist pengguna sistem untuk mengontrol pemakai.

Hasil yang diharapkan muncul pada tahap ini adalah tersedianya daftar kontrol yang digunakan dan yang sedang direncanakan oleh sistem IT untuk memitigasi kemungkinan adanya kelemahan atas sistem dan memperkecil dampak yang mungkin timbul atas penerapan policy keamanan.

Langkah 5. Menerapkan beberapa kemungkinan

Pada langkah ini, semua skalabilitas kemungkinan yang mungkin timbul dari kelemahan sistem didefinisikan. Terdapat beberapa faktor yang perlu dipertimbangkan dalam upaya mendefinisikan skalabilitas seperti :

- Motif dan kapabilitas dari sumber ancaman
- Kelemahan bawaan dari sistem
- Eksistensi dan efektifitas kontrol yang di terapkan

Tugas

Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan.

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya "scope creep" (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Contohnya :

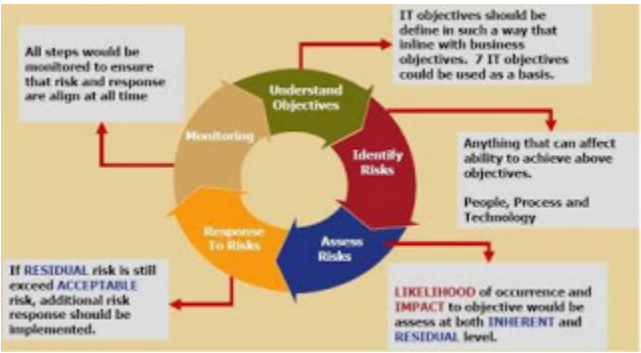
Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (Control Objectives for Information and Related Technology) adalah standar internasional untuk tata kelola TIyang dikembangkan oleh ISACA (Information System and Control Association) dan ITGI (IT Governance Institute) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.

IT Risk Management Framework by COBIT

COBIT (Control Objectives for Information and Related Technology) merupakan standard yang dikeluarkan oleh ITGI (The IT Governance Institute). COBIT merupakan suatu koleksi dokumen dan framework yang diklasifikasikan dan secara umum diterima sebagai best practice untuk tata kelola (IT Governance), kontrol dan jaminan TI.

Referensi perihal manajemen resiko secara khusus dibahas pada proses PO9 dalam COBIT. Prosesproses yang lain juga menjelaskan tentang manajemen resiko namun tidak terlalu detil.



Gambar Framework Manajemen Resiko COBIT

Resiko adalah segala hal yang mungkin berdampak pada kemampuan organisasi dalam mencapai tujuantujuannya. Framework manajemen resiko TI dengan menggunakan COBIT (lihat gambar) terdiri dari :

1. **Penetapan Objektif**

Kriteria informasi dari COBIT dapat digunakan sebagai dasar dalam mendefinisikan objektif TI. Terdapat tujuh kriteria informasi dari COBIT yaitu : effectiveness, efficiency, confidentiality, integrity, availability, compliance, dan reliability.

2. **Identifikasi Resiko**

TABEL KEJADIAN (EVENTS) YANG MENGGANGU PENCAPAIAN OBJEKTIF PERUSAHAAN :

Objectives	Events
Effectiveness and Efficiency	Manajemen yang buruk (perencanaan dan kebijakan)
	Sistem (Hardware, software dan teknologi).
	Kemampuan TI dan non-TI.
	Manajemen proses (desain dan eksekusi)
Confidentiality	Manajemen Keamanan (kebijakan dan prosedur).
	Sistem (Hardware, software teknologi dan jaringan).
	Kesadaran pengguna
	Hacker dan virus
Integrity and Reliability	Desain sistem (input, proses, output)
	Hacker dan pelanggar akses
	Prosedur pemberian otoritas yang buruk.
Availability	Desain system dan jaringan
	Kegagalan hardware
	Sabotase dari luar
	Virus dan serangan
	Tidak ada BCP, backup dan recovery
Compliance	Tidak sadar atau tidak mengerti terhadap aturan dan regulasi
	Tidak ada monitoring

Identifikasi resiko merupakan proses untuk mengetahui resiko. Sumber resiko bisa berasal dari :

- Manusia, proses dan teknologi
- Internal (dari dalam perusahaan) dan eksternal(dari luar perusahaan)
- Bencana (hazard), ketidakpastian (uncertainty) dan kesempatan (opportunity).

Dari ketiga sumber resiko tersebut dapat diketahui kejadian-kejadian yang dapat mengganggu perusahaan dalam mencapai objektifnya (lihat tabel event diatas).

3. **Penilaian Resiko**

Proses untuk menilai seberapa sering resiko terjadi atau seberapa besar dampak dari resiko (tabel 2.2). Dampak resiko terhadap bisnis (business impact) bisa berupa : dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data), dan penundaan proses pengambilan keputusan.

Sedangkan kecenderungan (likelihood) terjadinya resiko dapat disebabkan oleh sifat alami dari bisnis, struktur dan budaya organisasi, sifat alami dari sistem (tertutup atau terbuka, teknologi baru dan lama), dan kendali-kendali yang ada. Proses penilaian resiko bisa berupa resiko yang tidak dapat dipisahkan (inherent risks) dan sisa resiko (residual risks).

TABEL TINGKATAN BESARNYA DAMPAK RESIKO DAN FREKUENSI TERJADINYA RESIKO

Level	Business Impacts	Likelihood
0	Kerusakan yang hampir tidak signifikan	Hampir mustahil terjadi
1	Kerusakan kecil	Jarang terjadi
2	Kerusakan yang signifikan tetapi dapat ditolerir	Mungkin terjadi
3	Kerusakan besar	Sering terjadi
4	Kerusakan yang dapat mengancam kelangsungan bisnis	Sangat sering terjadi

4. **Respon Resiko**

Untuk melakukan respon terhadap resiko adalah dengan menerapkan kontrol objektif yang sesuai dalam melakukan manajemen resiko. Jika sisa resiko masih melebihi resiko yang dapat diterima (acceptable risks), maka diperlukan respon resiko tambahan. Proses-proses pada framework COBIT (dari 34 Control Objectives) yang sesuai untuk manajemen resiko adalah :

- PO1 (Define a Stretegic IT Plan) dan PO9 (Assess and Manage Risks)
- AI6 (Manages Change)
- DS5 (Ensure System and Security) dan DS11 (Manage Data)
- ME1 (Monitor and Evaluate IT Performance)

5. **Monitor Resiko**

Setiap langkah dimonitor untuk menjamin bahwa resiko dan respon berjalan sepanjang waktu.

Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan.

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.

2. Melonjaknya biaya pengembangan sistem informasi karena adanya “scope creep” (atau pengembangan berlebihan) yang tanpa terkendali.

3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Cara mengendalikan resiko yang ada yaitu dengan cara organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI. Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi.

TIGA JENIS RISIKO AUDIT IT

KELOMPOK 4 :
Yuniarti Denita Sari
Raju Septa Wijaya
Hendri

JENIS RISIKO AUDIT

1. Inherent Risk (IR) / Risiko Bawaan

Adalah risiko yang mungkin timbul akibat karakter bawaan dari suatu transaksi, entah karena:

(a) kompleksitas transaksi dan klas transaksi; atau

(b) kompleksitas perhitungan; atau

(c) aset yg mudah tercuri/digelapkan; atau

(d) ketiadaan informasi yang sifatnya obyektif.

Sudah menjadi pemahaman publik bahwa inherent risk adalah diluar jangkauan auditor dalam melakuk an pencegahan. Bahkan, juga diluar kendali pihak auditee sendiri. Dengan kata lain, auditor hanya bisa menemukan tetapi tidak bisa melakukan apa-apa.

JENIS RISIKO AUDIT

2. Control Risk (CR) / Risiko Pengendalian

Adalah risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, entah karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain—thus tidak mampu mencegah potensi salahsaji bersifat material dan/atau penggelapan (fraud). CR tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee jika mereka mau.

3. Detection Risk (DR) / Risiko Deteksi

Adalah risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud). DR ada dalam kendali auditor. Karena DR sepenuhnya ada pada kendali auditor, maka sudah pasti mereka harus berupaya untuk menekan risiko ini hingga ke tingkatakan yang paling minimal (tidak mungkin menghilangkan risiko ini sepenuhnya).

CONTOH Control Risk (CR) / Risiko Pengendalian

PT Bank Mandiri (Persero) Tbk yang mengalami sistem error yang menyebabkan saldo nasabahnya berubah pada saat proses backup data rutin. Dimana Manajemen Bank Mandiri memastikan bahwa perubahan drastis saldo rekening yang dialami nasabahnya bukan karena penipuan atau fraud. Perubahan saldo terjadi karena sistem error saat proses backup data rutin.

Bila yang terjadi adalah fraud, seharusnya saldo nasabah berkurang. Namun, yang terjadi adalah saldo nasabah ada yang bertambah dan berkurang secara acak (random). Manajemen Bank Mandiri pun menjelaskan kronologi sistem eror yang menyebabkan 10% nasabahnya atau sekitar 1,5 juta nasabah mengalami perubahan saldo. Insiden Bank Mandiri ini dinilai terjadi karena human error, bukan karena kerusakan pada piranti keras atau hardware. Sebab bila terjadi kegagalan pada hardware, proses pemindahan data dari satu perangkat ke perangkat lain semestinya gagal dilakukan.Dengan demikian , perubahan nominal tabungan pada nasabah seharusnya tidak terjadi jika terdapat kerus akan pada hardware.

Perubahan saldo nasabah ini sendiri terjadi pada Sabtu dini hari dibulan Juli. Bermula dari bank yang melakukan proses tutup buku rutin di akhir hari. Saat proses itu berlangsung, data nasabah dipindahkan dalam sebuah backup server. Kemudian, core server memproses transaksi yang terjadi di hari sebelumnya. Namun gangguan itu tidak berpengaruh terhadap transaksi di luar rekening tabungan nasabah, misalnya e-money, pembayaran surat izin mengemudi (SIM), dan sebagainya. Sebab, menurutnya transaksi itu terlepas dari sistem backup data nasabahnya.

PENGENDALIAN DARI CONTOH AUDIT SEBELUMNYA :

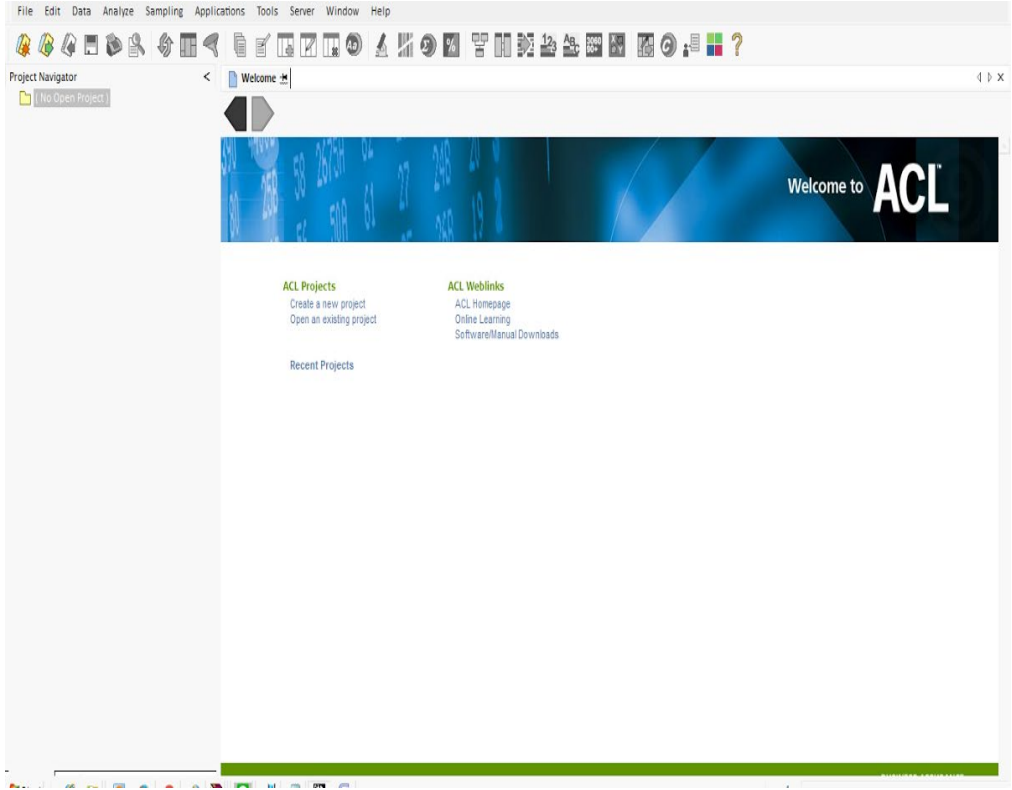
- Perlunya pengecekan secara berlapis (double checking). Dimana sebelum eksekusi perpindahan data, ada orang lain yang melakukan pengecekan ulang lagi (investigasi lebih lanjut, yang diperiksa kembali, apakah memang permasalahan tersebut dari hardware, software, atau human eror).
- Perlunya proses perekrutan pegawai TI sesuai dengan prosedur yang ada.

Tools yang digunakan :

ACL

ACL (Audit Command Language) merupakan sebuah software CAAT (Computer Assisted Audit Techniques) yang sudah sangat populer untuk melakukan analisa terhadap data dari berbagai macam sumber.

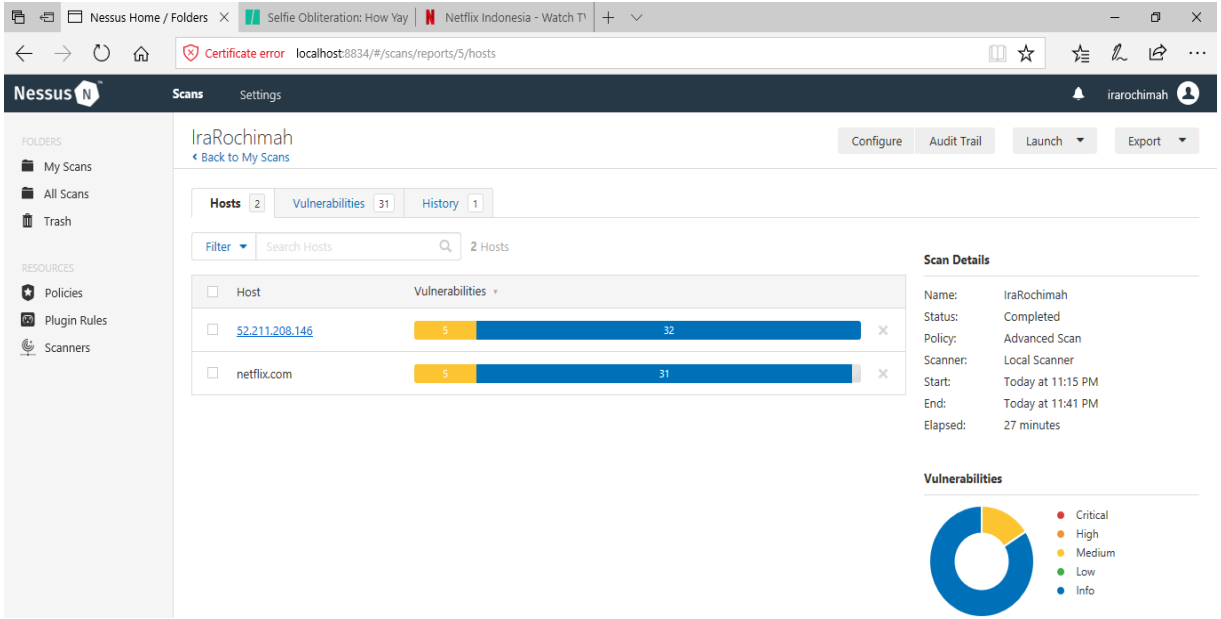
ACL for Windows (sering disebut ACL) adalah sebuah software TABK(TEKNIK AUDIT BERBASIS KOMPUTER) untuk membantu auditor dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik.



Tools yang digunakan :

NESSUS

Nessus adalah termasuk kelompok scanner gratis baru. Nessus bekerja dengan memeri ksa target yang anda telah anda tentukan, seperti Sekumpulan host / bisa juga host dalam fokus tersendiri. Begitu aktivitas scan selesai, anda dapat melihat informasi hasilnya, baik dalam bentuk grafikal atau baris. Interface (tampilan) grafikal Nessus dibangun dengan menggunakan Gimp Toolkit (gtk). Gtk adalah sebuah library gratis yang banyak digunakan untuk membangun interface grafikal dibawah X. Alasan kenapa kebanyakan Administrator Security Computer memilih Nessus adalah karena distribusi aplikasi ini selalu up to date (selalu diperbaharui), berbasis web interface, mudah dioperasikan dan gratis.



Fungsi Nessus yaitu digunakan untuk mencari kelemahan pada sebuah sistem komputer. Nessus juga dapat melakukan pengecekan terhadap kerentanan system komputer, dan meningkatkan keamanan sistem yang kita miliki.

TERIMA KASIH

KELOMPOK 3

" IT AUDIT "

Reni Septiyanti
Fero Triando
Evan Apriadi Dilatama
Fitrianto Puja Kesuma

Program Pascasarjana Magister Teknik Informatika
Universitas Bina Darma Palembang

2019

RISIKO AUDIT

Risiko Audit adalah istilah yang digunakan dalam kaitannya dengan audit atas laporan keuangan suatu entitas.

Risiko audit diartikan sebagai tingkat ketidakpastian tertentu yang dapat diterima auditor dalam pelaksanaan auditnya, seperti :

- ❑ Ketidakpastian validitas dan reliabilitas bukti audit.
- ❑ Ketidakpastian mengenai efektivitas pengendalian internal.

Risiko Audit (*Audit Risk*) adalah risiko yang terjadi dalam hal auditor tanpa disadari tidak memodifikasikan pendapatnya sebagaimana mestinya, atas suatu laporan keuangan yang mengandung salah saji material.

Risiko Audit (*Audit Risk*) terdiri dari 3 jenis :

1. Risiko Bawaan (*Inheren Risk*)
2. Risiko Pengendalian (*Control Risk*)
3. Risiko Deteksi (*Detection Risk*)

1. Risiko Bawaan (*Inheren Risk*)

Risiko bawaan adalah kerentanan suatu asersi terhadap salah saji material dengan asumsi tidak ada kebijakan dan prosedur struktur pengendalian intern yang terkait. Risiko bawaan selalu ada dan tidak pernah mencapai angka nol. Risiko bawaan tidak dapat diubah oleh penerapan prosedur audit yang paling baik sekalipun.

Risiko bawaan bervariasi untuk setiap asersi. Sebagai contoh, asersi keberadaan dan keterjadian kas mempunyai risiko bawaan yang lebih tinggi daripada aktiva tetap. Hal ini disebabkan uang tunai merupakan suatu aset yang sangat rawan terhadap manipulasi, dan semua orang berminat terhadap uang. Sedangkan aktiva tetap lebih terlihat jelas keberadaannya. Risiko bawaan juga dibedakan atas risiko bawaan setiap akun dan risiko bawaan keseluruhan untuk banyak akun.

Contoh Kasus 1 (Pada Kepolisian)

No	Contoh Inheren Risk	*Control Assesment*
1	Fasilitas negara digunakan sebagai kepentingan pribadi.	Peningkatan pengawasan yang tegas dan ketat terhadap para anggota polisi.
2	Masyarakat dikenakan tarif apabila meminta bantuan kepada kepolisian yang membebani si pelapor atau si peminta bantuan.	Adanya pusat-pusat pelayanan pelaporan bagi masyarakat yang lebih mudah dan dapat dijangkau.
3	Menyelenggarakan kegiatan atau razia tanpa izin di jalanan dengan tujuan mendapatkan penghasilan tambahan dan terkadang melakukan tindakan-tindakan dengan tidak sopan dan anarkis .	Setiap anggota polisi lebih di tekankan bahwa dalam melaksanakan tugas dan wewenangnya, pejabat kepolisian senantiasa bertindak berdasarkan norma agama, kesopanan, kesusilaan, serta menjunjung tinggi hak asasi manusia (Pasal 19 : Ayat 1).
4	Membunyikan sirine dan menyalakan lampu rotator hanya untuk menghindari kemacetan atau melintasi jalanan dengan bebas tanpa disertai tugas.	Setiap anggota polisi di uji apakah mereka mengetahui tugas dan wewenangnya yang Sesuai dengan tugas dan wewenang kepolisian yang diatur dalam UU pasal 14 dan pasal 13 tentang kepolisian.
5	Lebih banyak terlihat duduk santai di warung-warung atau di pos-pos polisi dari pada berdiri di jalanan mengatur kelancaran lalu lintas.	Kesejahteraan setiap anggota polisi lebih ditingkatkan dan diperhatikan.

Contoh Kasus 2
(Kasus Audit Asset Tetap)

Pada Desember 2006 Indonesia Corruptin Watch (ICW) melaporkan kasus dugaan korupsi ke Komisi Pemberantasan Korupsi (KPK) dalam ruislaag (tukar guling) antara asset PT. Industri Sandang Nusantara (ISN), sebuah BUMN yang bergerak di bidang tekstil, dengan asset PT. GDC, sebuah perusahaan swasta. Dalam ruislaag tersebut PT. ISN menukarkan tanah seluas 178.497 meter persegi di kawasan Senayan dengan Tanah seluas 47 hektar beserta Pabrik dan mesin di karawang.

Contoh Kasus 2
(Kasus Audit Asset Tetap) ....

Berdasarkan hasil temuan Badan Pemeriksaan Keuangan (BPK) semester II Tahun Anggaran 1998/1999, menyatakan ruislaag itu berpotensi merugikan keuangan Negara sebesar Rp. 121,628 miliar. Kerugian itu terdiri dari kekurangan luas bangunan pabrik dan mesin milik PT. GDC senilai Rp. 63,954 miliar, berdasarkan penilaian aktiva tetap oleh PT. Sucofindo pada 1999; penyusutan nilai asset pabrik milik PT. GDC senilai Rp. 31,546 miliar; dan kelebihan perhitungan harga tanah senilai Rp. 0,127 miliar. Selain itu juga ditemukan bahwa terdapat nilai saham yang belum dibayarkan oleh PT. GDC sebesar Rp. 26 miliar.

SOLUSI
(Kasus Audit Asset Tetap) ....

Seharusnya keputusan Tukar Guling tidak hanya menjadi wewenang salah satu pejabat saja, melainkan melibatkan beberapa pejabat sebagai pengendali dan control yang baik. Selain itu juga diperlukan sebuah aturan baku oleh perusahaan mengenai tukar guling, sehingga kemungkinan penyelewengan menjadi berkurang.

Diperlukan juga control dari lembaga bersangkutan terhadap penelitian tim penilik yang meneliti kelengkapan mengenai status asset, dokumen kelengkapan asset, sehingga tidak ada manipulasi dari nilai asset tersebut serta proses tukar menukar.

Dari kasus diatas dapat dibuktikan bahwa PT. ISN memiliki pengendalian intern yang sangat buruk. Sehingga PT. ISN rawan dicurangi oleh rekanan-rekanan bisnisnya maupun oleh oknum-oknum pejabat perusahaan yang ingin mengambil keuntungan. Oleh karena itu hal pertama yang harus dibenahi oleh PT. ISN adalah soal Pengendalian Internnya.

2. Risiko Pengendalian (*Control Risk*)

adalah risiko yang bisa timbul akibat kelemahan sistem pengendalian internal (SPI) auditee, tidak tahu karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain dan tidak mampu mencegah potensi salahsaji bersifat material dan/atau penggelapan (fraud). Jadi CR tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee jika mereka mau.

Risiko Pengendalian (*Control Risk*)

Contoh Kasus Denial of Service (DoS) dan Distributed DoS (DDos) attack. DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi

Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari berberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja. Adapun Modus yang dilakukan sang Cracker adalah ingin membuat suatu perusahaan atau organisasi rugi besar karena terganggunya system yang sedang berjalan. Bentuk Penyelesaiannya selain dilaporkan ke Kepolisian ada baiknya keamanan data dilakukan berlapis agar data tidak dengan mudah bocor atau mudah dicuri.

Risiko Pengendalian (*Control Risk*)

Mengantisipasi Serangan DDoS dengan DDoS Protection

Terkadang, seseorang tidak memperdulikan sisi keamanan sebuah website mereka dan cenderung merasa bahwa website mereka telah aman dari serangan DDoS tanpa fitur DDoS Protection. Pada nyatanya, sebuah serangan DDoS tidak hanya mengacu kepada resource yang dimiliki oleh server, namun juga kerentanan atau celah yang terdapat pada suatu website.

Cloudmatika sendiri bekerja sama dengan Cloudbric dalam menyediakan sebuah proteksi dari serangan DDoS untuk masyarakat di Indonesia dalam mengamankan websitenya dari segala serangan DDoS. Cloudbric DDoS Protection atau biasa disebut Anti DDoS dihadirkan di Indonesia untuk membuat masyarakat merasa lebih mudah dalam mengantisipasi dan juga mencegah segala bentuk serangan DDoS yang datang. Dengan fitur yang lengkap dan juga keamanan yang terjamin, membuat para developer tidak perlu takut lagi akan serangan-serangan DDoS yang ditujukan kepada websitenya

Risiko Pengendalian (*Control Risk*)

Contoh Kasus Denial of Service (DoS) dan Distributed DoS (DDos) attack. DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi

Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari berberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja. Adapun Modus yang dilakukan sang Cracker adalah ingin membuat suatu perusahaan atau organisasi rugi besar karena terganggunya system yang sedang berjalan. Bentuk Penyelesaiannya selain dilaporkan ke Kepolisian ada baiknya keamanan data dilakukan berlapis agar data tidak dengan mudah bocor atau mudah dicuri.

Keunggulan Cloudbric DDoS Protection

Beberapa keunggulan Cloudbric DDoS Protection yang harus diketahui oleh masyarakat di Indonesia untuk melengkapi sistem keamanan pada website mereka, diantaranya:

- **Identifikasi DDoS Lebih Awal dan Block Aktivitas Mencurigakan**

Memiliki sistem real-time protection yang menjadikan website Anda melakukan identifikasi setiap saat terhadap serangan-serangan yang datang dan melakukan blok secara langsung apabila teridentifikasi sebagai serangan. Pada Cloudbric DDoS Protection juga terdapat live monitor dari serangan yang datang dan juga serangan yang telah terblok. Sehingga Anda akan mengetahui detail serangan yang terjadi terhadap website Anda

- **Latency Rendah dan Pusat Data di Indonesia**

Menggunakan DDoS Protection Cloudmatika akan membuat Anda memiliki proteksi serangan DDoS dengan latency yang rendah karena server kami berada di Indonesia. Jika Anda menggunakan DDoS Protection yang memiliki server di luar Indonesia, maka akan menyebabkan layanan Anda sedikit terganggu akan latency yang ada. Sehingga mengakibatkan performa layanan Anda menjadi menurun dan sedikit lebih lambat

- **Biaya Yang Murah**

Anda tidak perlu takut akan biaya yang mahal untuk melakukan proteksi terhadap website Anda. Dengan Cloudbric DDoS Protection dari Cloudmatika, Anda akan mendapatkan biaya yang sangat terjangkau dan tentunya dengan fitur serta sistem keamanan yang canggih.

Contoh Kasus
(PT Kereta Api Indonesia (Persero)

No	Contoh Risiko Operasional PT KAI	Pengendalian Risiko (Control Risk)
1	Kebakaran dan kecelakaan kereta api	○ Penyiap-siagaan backup systems. ○ Prosedur kerja untuk sistem pemadam kebakaran, tangga darurat. ○ Coverage asuransi untuk meminimalkan kerugian/dampak negatif. ○ Pengendalian budaya keselamatan oleh polisi khusus kereta, petugas palang pintu kereta, dan sosialisasi secara berkala. ○ Pendidikan dan pelatihan dasar pemadam kebakaran.
2	Bencana alam	○ Memastikan adanya sistem peringatan dini (alarm) dan business continuity planning/contingency plan terhadap kondisi bencana. ○ Prosedur kerja untuk darurat bencana alam.
3	Keterbatasan suplai suku cadang	Pengaturan penggunaan dan suplai suku cadang yang lebih baik.

No	Contoh Risiko Operasional PT KAI	Pengendalian Risiko (Control Risk)
4	Keterbatasan kapasitas Depo/Balai Yasa	Optimalisasi kapasitas Depo/Balai Yasa, penjadwalan pemeliharaan dengan memperhitungkan saat sibuk *(peak season)* yaitu ketika liburan sekolah, lebaran, natal, tahun baru.
5	Gangguan dan kerusakan pada rel, peralatan persinyalan dan listrik aliran atas	○ Optimalisasi perawatan prasarana, ketelitian pemeriksaan, serta kerjasama tim yang baik. ○ Mempercepat pembangunan atau penyelesaian infrastruktur pendukung (stasiun *loading-unloading*). ○ Penambahan daya listrik dan penambahan sinyal dan stasiun. ○ Peremajaan gerbong kereta api, renovasi dan sterilisasi stasiun.
6	Terbatasnya mitra pengguna angkutan kereta api barang	Memprioritaskan pelayanan terhadap permintaan jasa angkutan barang dalam jumlah besar dan kontinu, berjarak tempuh jauh, dan bertarif tinggi serta pengangkutan berdasarkan perjanjian.

No	Contoh Risiko Operasional PT KAI	Pengendalian Risiko (Control Risk)
7	Meledaknya pengguna jasa transportasi pada musim-musim tertentu	○ Memperbanyak *point of sales* untuk penjualan tiket bekerjasama dengan mitra eksternal. ○ Melakukan sosialisasi dan promosi di media nasional terkait penjualan tiket kereta menjelang *peak season.* ○ Persiapan posko angkutan menjelang *peak season.* ○ Persiapan kereta api tambahan. ○ Peningkatan *bandwidth* dan kemudahan akses ke *website* untuk memfasilitasi pemesanan tiket secara online.
8	Keterlambatan jadwal keberangkatan dan kedatangan	○ Memanfaatkan teknologi informasi untuk memperbaiki proses perencanaan dan operasi untuk meningkatkan keselamatan, ketepatan waktu, pelayanan, dan keamanan. ○ Mengurangi toleransi terhadap keterlambatan.
9	Tidak diminatinya jasa-jasa penunjang perkeretaapian PT KAI	Membangun sistem pelayanan jasa transportasi unggulan yang terpadu dengan jasa pendukung, seperti kereta bandara, kereta wisata, biro jasa, dan *tour.*

PT Kereta Api Indonesia (Persero) dalam jangka waktu yang tidak terlalu lama, harus selalu mengidentifikasi risiko-risiko yang kemungkinan terjadi. Baik itu nanti risiko yang berklasifikasi dan berakibat tinggi, sedang atau rendah bagi perusahaan. Tidak hanya bagi perusahaan, namun juga bagi pengguna kereta api, yang tidak lain adalah masyarakat Indonesia sendiri. Apalagi setiap tahun pasti ada saja kecelakaan kereta api, yang disebabkan faktor internal maupun eksternal perusahaan. Mengembangkan inovasi terbaru itu juga perlu, apalagi dijaman yang sekarang sudah modern atau era globalisasi seperti ini. Harus banyak berkreatifitas agar mampu bersaing dengan transportasi darat yang lain.

Pengendalian risiko yang semaksimal mungkin, akan menghasilkan risiko yang seminimal mungkin. Sehingga juga akan meminimalkan kerugian bagi perusahaan dan pengguna jasa kereta api yaitu masyarakat. Dengan kenyamanan, perlindungan, asuransi, ketepatan waktu datang dan berangkat kereta api, harga tiket yang sesuai, peringatan dini bencana, dll yang dilakukan semaksimal mungkin oleh PT Kereta Api Indonesia (Persero), tentunya masyarakat juga akan mempercayai PT Kereta Api Indonesia (Persero) sebagai transportasi darat utama yang digunakan setiap hari. Sehingga akan berdampak pendapatan atau income yang tinggi untuk PT Kereta Api Indonesia (Persero).

3. Risiko Deteksi (*Detection Risk*)

adalah risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud). Jadi DR ada dalam kendali auditor. Itu karena DR sepenuhnya ada pada kendali auditor, maka sudah pasti mereka harus berupaya untuk menekan risiko ini hingga ke tingkatakan yang paling minimal (tidak mungkin menghilangkan risiko ini sepenuhnya).

Contoh Kasus

Risiko deteksi juga dapat terjadi karena auditor salah menetapkan langkah pengujiannya (prosedur audit). Sebagai contoh, prosedur pengeluaran barang menetapkan bahwa setiap pengeluaran barang harus didasarkan pada permintaan dari pihak yang akan menggunakan. Jadi dalam pelaksanaan pengeluaran barang akan terdapat dua populasi bukti yang saling terkait, bukti permintaan barang dan bukti pengeluaran barang. Dalam hal ini, risiko deteksi dapat terjadi jika dalam melakukan pengujian auditor menetapkan prosedur audit "periksa apakah atas setiap bukti permintaan barang terdapat bukti pengeluaran barangnya!" Prosedur ini dipastikan tidak akan menemukan kesalahan seperti kecurangan pihak gudang yang mengeluarkan barang walaupun tidak ada permintaan dari pihak yang membutuhkan barang, karena jika ada permintaan barang dapat dipastikan bagian gudang akan menerbitkan bukti pengeluaran barang.

Contoh Kasus

Sebaliknya, jika prosedur audit yang ditetapkan adalah: “periksa apakah atas setiap bukti pengeluaran barang terdapat bukti permintaan barangnya!” maka prosedur ini mungkin akan dapat menemukan kecurangan bagian gudang atas pengeluaran barang yang tidak didasarkan pada permintaan barang. Dengan prosedur tersebut, jika seandainya bagian gudang melakukan kecurangan mengeluarkan barang tetapi bukan untuk kepentingan perusahaan, maka akan dapat ditemukan dari sampel pengeluaran barang yang tidak ditemukan bukti permintaan barangnya.

Solusi

Berdasarkan penjelasan di atas, maka risiko deteksi berhubungan dengan luasnya pengumpulan dan pengujian bukti yang harus dilakukan auditor. Risiko deteksi yang rendah hanya dapat dicapai jika auditor melakukan pengujian yang luas. Hal ini berarti bahwa risiko deteksi berbanding terbalik dengan luasnya pengujian. Pemahaman mengenai model risiko audit tersebut akan dapat membantu auditor dalam merancang luasnya pengujian agar auditor tidak mengalami risiko audit (dalam arti audit menjadi tidak efektif), serta agar audit dapat dilaksanakan secara efisien (dalam arti audit dapat menghindarkan diri, melakukan perluasan pengujian yang tidak perlu).

TERIMA KASIH

TUGAS PENGENDALIAN RESIKO

Nama : RiccaVerana Sari

Kelas : MTi Reguler A

NIK : 182420067

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

PASCASARJANA UNIVERSITAS BINA DARMA

PALEMBANG

2019

Resiko adalah suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisa serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko.

Seiring dengan berkembangnya teknologi informasi yang bergerak sangat cepat dewasa ini, pengembangan unit usaha yang berupaya menerapkan sistem informasi dalam organisasinya telah menjadi kebutuhan dasar dan semakin meningkat dari tahun ke tahun. Akan tetapi pola pembangunan sistem informasi yang mengindahkan faktor resiko telah menyebabkan beberapa organisasi mengalami kegagalan menerapkan teknologi informasi tersebut, atau meningkatnya nilai investasi dari *plafon* yang seharusnya, hal ini juga dapat menghambat proses pencapaian misi organisasi.

Jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi :

Pada dasarnya, faktor resiko dalam suatu perencanaan sistem informasi, dapat diklasifikasikan ke dalam 4 kategori resiko, yaitu :

a. *Catastrophic* (Bencana)

b. *Critical* (Kritis)

c. *Marginal* (kecil)

d. *Negligible* (dapat diabaikan)

Adapun pengaruh atau dampak yang ditimbulkan terhadap suatu proyek sistem informasi dapat berpengaruh kepada

a) nilai unjuk kerja dari sistem yang dikembangkan,

b) biaya yang dikeluarkan oleh suatu organisasi yang mengembangkan teknologi informasi,

c) dukungan pihak manajemen terhadap pengembangan teknologi informasi, dan

d) Jadwal waktu penerapan pengembangan teknologi informasi.

Suatu resiko perlu didefinisikan dalam suatu pendekatan yang sistematis, sehingga pengaruh dari resiko yang timbul atas pengembangan teknologi informasi pada suatu organisasi dapat diantisipasi dan di identifikasi sebelumnya. Mendefinisikan suatu resiko dalam pengembangan teknologi informasi pada suatu organisasi terkait dengan Siklus Hidup Pengembangan Sistem (*System Development Life Cycle* [SDLC]), dimana fase-fase penerapan SDLC dalam pengembangan teknologi informasi di spesifikasikan analisa resiko.

Pola Pendekatan

System Development Life Cycle [SDLC] adalah suatu tahapan proses perancangan suatu sistem yang dimulai dari tahap investigasi; pembangunan; implementasi; operasi/perawatan; serta tahap penyelesaian [4]. Dari dasar tersebut di atas, strategi penerapan manajemen resiko perlu mempertimbangkan dampak yang mungkin timbul dengan tingkat probabilitas yang berbeda untuk setiap komponen pengembangan sistem informasi.

Pola pendekatan manajemen resiko juga perlu mempertimbangkan faktor-faktor pada *System Development Life Cycle* (SDLC) yang terintegrasi, yaitu Mengindentifikasikan faktor-faktor resiko yang timbul dan diuraikan disetiap tahap perancangan sistem, yang tersusun sebagai berikut :

1. ***Tahap 1. Investigasi*** : Tahap ini suatu sistem didefinisikan, menyangkut ruang lingkup pengembangan yang akan dibuat, yang semua perencanaan atas pengembangan sistem di dokumentasikan terlebih dahulu. Dukungan yang dibutuhkan dari manajemen resiko pada tahap ini adalah faktor resiko yang mungkin terjadi dari suatu sistem informasi di identifikasikan, termasuk di dalamnya masalah serta konsep pengoperasian keamanan sistem yang semuanya bersifat strategis.
2. ***Pengembangan*** : Tahap ini merupakan tahap dimana suatu sistem informasi dirancang, pembelian komponen pendukung sistem di laksanakan, aplikasi di susun dalam program tertentu, atau masa dimana konstruksi atas sistem di laksanakan. Pada proses ini, faktor resiko diidentifikasikan selama tahap ini dilalui, dapat berupa analisa atas keamanan sistem sampai dengan kemungkinan yang timbul selama masa konstruksi sistem di laksanakan.
3. ***Implementasi*** : Tahap ini kebutuhan atas keamanan sistem dikonfigurasikan, aplikasi sistem di uji coba sampai pada verifikasi atas suatu sistem informasi di lakukan. Pada tahap ini faktor resiko di rancang guna mendukung proses pelaksanaan atas implementasi sistem informasi sehingga kebutuhan riil di lapangan serta pengoperasian yang benar dapat dilaksanakan.
4. ***Pengoperasian dan Perawatan*** : Tahap ini merupakan tahap dimana sistem informasi telah berjalan sebagaimana mestinya, akan tetapi secara secara berkala sistem membutuhkan modifikasi, penambahan peralatan baik perangkat keras maupun perangkat lunak pendukung, perubahan tenaga pendukung operasi, perbaikan kebijakan maupun prosedur dari suatu organisasi. Pada tahap ini manajemen resiko lebih menitik beratkan pada kontrol berkala dari semua faktor yang menentukan berjalannya sistem, seperti perangkat keras, perangkat lunak, analisa sumber daya manusia, analisa basis data, maupun analisa atas jaringan sistem informasi yang ada.
5. **Penyelesaian/penyebaran** : Tahap ini merupakan tahap dimana system informasi yang telah digunakan perlu di lakukan investasi baru karena unjuk kerja atas sistem tersebut telah berkurang, sehingga proses pemusnahan data, penggantian perangkat keras dan perangkat lunak, ataupun berhentinya kegiatan atau kepindahan organisasi ke tempat yang baru. Manajemen resiko yang perlu di perhatikan dalam tahap ini adalah memastikan proses pemusnahan atas komponen-komponen system informasi dapat berjalan dengan baik, terkelola dari segi keamanan.

Setelah pola pendekatan manajemen resiko di definisikan dalam masing-masing tahap SDLC, maka tahap selanjutnya adalah menilai manajemen resiko dalam metodologi tertentu. Upaya memberikan penilaian atas dampak resiko dalam pengembangan sistem informasi,

perlu dilakukan karena dapat memberikan gambaran atas besar atau kecilnya dampak ancaman yang mungkin timbul selama proses pengembangan sistem.

Metodologi Penilaian Resiko

Untuk menentukan kemungkinan resiko yang timbul selama proses pengembangan sistem informasi berlangsung, maka organisasi yang bermaksud mengembangkan sistem informasi perlu menganalisa beberapa kemungkinan yang timbul dari pengembangan sistem informasi tersebut. Adapun metodologi penilaian resiko pengembangan sistem informasi dapat diuraikan dalam 9 langkah, yang tersusun sebagai berikut :

a. Menentukan karakteristik dari suatu sistem

b. Mengidentifikasikan ancaman-ancaman

c. Mengidentifikasikan kelemahan sistem

d. Menganalisa pengawasan

e. Menentukan beberapa kemungkinan pemecahan masalah

f. Menganalisa pengaruh resiko terhadap pengembangan sistem

g. Menentukan resiko

h. Merekomendasikan cara-cara pengendalian resiko

i. Mendokumentasikan hasil keputusan

Tahap ke dua, tiga, empat dan enam dari langkah tersebut di atas dapat dilakukan secara paralel setelah langkah pertama dilaksanakan. Adapun dari setiap langkah tersebut adalah sebagai berikut :

Langkah 1. Menentukan Karakterisasi Sistem

Pada langkah pertama ini batasan suatu sistem yang akan dikembangan di identifikasikan, meliputi perangkat keras, perangkat lunak, sistem interface, data dan informasi, sumber daya manusia yang mendukung sistem IT, tujuan dari sistem, sistem dan data kritis, serta sistem dan data sensitif. Beberapa hal tambahan yang dapat diklasifikasikan pada karakteristik sistem selain hal tersebut di atas seperti bentuk dari arsitektur keamanan sistem, kebijakan yang dibuat dalam penanganan keamanan sistem informasi, bentuk topologi jaringan komputer yang dimiliki oleh organisasi tersebut, Manajemen pengawasan yang dipakai pada sistem TI di organisasi tersebut, dan hal lain yang berhubungan dengan masalah keamanan seputar penerapan Teknologi Informasi di organisasi yang bermaksud mengembangkan sistem informasi.

Adapun teknik pengumpulan informasi yang dapat diterapkan pada langkah ini meliputi :

1. ***Membuat daftar kuesinoner***. Daftar kuesioner ini di susun untuk semua level manajemen yang terlibat dalam sistem dengan tujuan mengumpulkan informasi

seputar keamanan data dan informasi dengan tujuan untuk memperoleh pola resiko yang mungkin dihadapi oleh sistem.

2. ***Interview.*** Bentuk lain dari pengumpulan data dengan cara interview terhadap IT Support atau personil yang terlibat dalam sistem informasi.
3. ***Review atas dokumen.*** Review atas dokumen pengembangan sistem, Dokumen kebijakan, atau dokumen keamanan informasi dapat memberikan gambaran yang bermanfaat tentang bentuk dari kontrol yang saat ini diterapkan oleh SI maupun rencanan pengembangan dari pengawasan di masa depan.
4. ***Penerapan Tool.*** Menggunakan suatu tool aplikasi yang memiliki tujuan untuk mengumpulkan informasi tentang sistem informasi yang digunakan merupakan salah satu cara untuk dapat memetakan sistem secara keseluruhan, seperti penggunakan network monitor, maupun tools lain.

Hasil output dari langkah pertama ini akan menghasilkan Penaksiran atas karakteristik sistem IT, Gambaran tentang lingkungan sistem IT serta gambaran tentang batasan dari sistem yang dikembangkan.

Langkah 2. Mengidentifikasikan ancaman-ancaman

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Timbulnya ancaman dapat dipicu oleh suatu kondisi dari sumber ancaman. Sumber ancaman dapat muncul dari kegiatan pengolahan informasi yang berasal dari 3 hal utama, yaitu (1) Ancaman Alam; (2) Ancaman Manusia, dan (3) Ancaman Lingkungan. Ancaman yang berasal dari manusia memiliki karakteristik tersendiri, serta memiliki alasan tersendiri dalam melakukan gangguan terhadap sistem informasi yang ada. Adapun alasan yang timbul dari ancaman manusia ini dapat di definisikan dalam tabel berikut :

Sumber Ancaman	Alasan	Aksi yang timbul
Hacker, Cracker	• Tantangan • Ego • Memberontak	• Hacking • Social Engineering • Gangguan sistem • Akses terhadap sistem
Kriminal	• Perusakan informasi • Penyingkapan informasi secara ilegal • Keuntungan moneter • Merubah data	• Tindak Kriminal • Perbuatan curang • Penyuapan • Spoofing • Intrusi atas sistem
Teroris	• Surat kaleng • Perusakan • Peledakan • Balas dendam	• Bom/teror • Perang informasi • Penyerangan sistem • Penembusan atas sistem • Tampering sistem
Mata-mata	• Persaingan usaha	• Pencurian informasi • Social engineering

	• Mata-mata ekonomi	• Penembusan atas sistem
Orang dalam Organisasi	• Keingintahuan • Ego • Mata-mata • Balas dendam • Kelalaian kerja	• Surat kaleng • Sabotase atas sistem • Bug sistem • Pencurian/penipuan • Perubahan data • Virus, trojan, dll • Penyalahgunaan komputer

Organisasi yang membutuhkan daftar dari sumber ancaman, perlu melakukan hubungan dengan badan-badan atau sumber-sumber yang berhubungan dengan keamanan, seperti misalnya sumber ancaman dari alam diharapkan hubungan dengan BMG yang menangani masalah alam, atau pihak intelijen atau media massa yang dapat mendeteksi sumber ancaman dari manusia. Hasil output dari ancaman ini merupakan pernyataan atau daftar yang berisikan sumber ancaman yang mungkin dapat mengganggu sistem secara keseluruhan.

Langkah 3. Identifikasi kelemahan

Cacat atau kelemahan dari suatu sistem adalah suatu kesalahan yang tidak terdeteksi yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh sumber ancaman yang mencoba menyusup terhadap sistem tersebut.

Pada beberapa vendor besar, informasi atas kelemahan sistem yang dibuat oleh vendor tersebut ditutup atau dihilangkan dengan penyediaan layanan purna jual dengan menyediakan hot fixes, service pack, pathces ataupun bentuk layanan lain.

Penerapan metode proaktif atau tersedianya karyawan yang bertugas untuk melakukan sistem test dapat di pakai untuk mencek kelemahan sistem secara efisien, dimana hal tersebut tergantung kepada keberadaan sumber daya atau kondisi IT yang bersifat kritis. Metode tes yang diterapkan dapat berbentuk :

- Penggunaan tool yang menscan kelemahan sistem secara automatis
- Adanya Evaluasi dan sekuriti tes (ST&E), atau
- Melakukan penetrasi tes

Penggunaan tools untuk mencek kelemahan sistem diterapkan pada grup perusahaan dengan kelengkapan jaringan komputer yang memadai, yang digunakan untuk memindai beberapa servis sistem yang disinyalir lemah (seperti : Diperbolehkannya anonymous FTP, sendmail automatis, dll). Strategi ST&E merupakan metode tes yang di terapkan pada saat proses penilaian atas resiko dilakukan. Metode ini diterapkan saat pengembangan dan eksekusi atas Sistem Informasi berjalan yaitu pada bagian *test plan*. Kegunaan dari metode ini adalah untuk melihat efektifitas dari kontrol atas sekuriti dari sistem IT terimplementasikan dalam kondisi sistem beroperasi. Penetrasi tes merupakan metode yang digunakan sebagai pelengkap dalam memeriksa kontrol atas sekuriti dan menjamin tidak adanya masalah sekuriti yang mungkin timbul pada sistem IT.

Bentuk keluaran yang timbul pada langkah ketiga ini memungkinkan pihak penilai resiko mendapatkan daftar dari kelemahan sistem yang dapat dianggap sebagai potensi dari sumber ancaman di kemudian hari.

Langkah 4. Analisa pengawasan

Tujuan yang diharapkan pada langkah ini adalah untuk menganalisa penerapan kontrol yang telah diimplementasikan atau yang direncanakan. Bagi organisasi langkah ini perlu untuk meminimalisasi atau bahkan mengeliminasi probabilitas kemungkinan yang timbul dari sumber ancaman atau potensi kelemahan atas sistem.

Metode pengawasan

Metode pengawasan terdiri atas metode yang bersifat teknis maupun non teknis. Metode pengawasan secara teknis merupakan salah satu upaya perlindungan kepada organisasi dalam hal perlindungan terhadap perangkat keras komputer, perangkat lunak maupun mekanisme akses kontrol yang digunakan, sedangkan metode nonteknis lebih ditekankan kepada pengawasan atas manajemen dan operasional penggunaan sistem IT di organisasi tersebut, seperti penerapan policy keamanan, prosedur operasional, maupun manajemen personel yang ada.

Kategori pengawasan

Kategori pengawasan baik secara teknis maupun non teknis dapat diklasifikasikan dalam 2 pendekatan yaitu pendekatan preventif atau detektif.

Pendekatan preventif adalah upaya untuk mencegah upaya pelanggaran atas policy keamanan seperti pengaksesan atas sistem IT atau tindakan lain misalnya dengan cara mengenkripsi informasi atau menerapkan otentifikasi atas informasi.

Pendekatan detektif adalah cara untuk memperingati pengguna atas terjadinya pelanggaran atau percobaan pelanggaran atas policy keamanan yang ada, metode ini contoh pada Microsoft Windows dengan menggunakan teknik audit trails, metode deteksi penyusupan atau teknik checksum.

Teknis analisa pengawasan

Analisa pengawasan atas policy keamanan dapat menggunakan teknik checklist pengguna yang mengakses sistem IT atau dengan penggunaan checklist yang tersedia untuk memvalidasi keamanan, hal paling penting pada tahap ini adalah mengupdate terus menerus atas checklist pengguna sistem untuk mengontrol pemakai.

Hasil yang diharapkan muncul pada tahap ini adalah tersedianya daftar kontrol yang digunakan dan yang sedang direncanakan oleh sistem IT untuk memitigasi kemungkinan adanya kelemahan atas sistem dan memperkecil dampak yang mungkin timbul atas penerapan policy keamanan.

Langkah 5. Menerapkan beberapa kemungkinan

Pada langkah ini, semua skalabilitas kemungkinan yang mungkin timbul dari kelemahan sistem didefinisikan. Terdapat beberapa faktor yang perlu dipertimbangkan dalam upaya mendefinisikan skalabilitas seperti :

- Motif dan kapabilitas dari sumber ancaman
- Kelemahan bawaan dari sistem
- Eksistensi dan efektifitas kontrol yang di terapkan

Threat Source Action & Threat Source

Threat Action	Threat Source	Probability	Impact	Risk Score	Qualtative Values	Risk Accaptance
Compromising confidential information (Berusaha untuk mengambil informasi rahasia)	Human, Terminated Employees	4 (Likely)	4 (Major)	16	High	High
Concealing user identity (Membuka/membongkar identitas pengguna)	Human, User, Hacker, Cracker	2 (Unlikely)	3 (Moderate)	6	Low	Low
Damage caused by a third party (Kerusakan yang disebabkan oleh pihak ketiga)	Human, Corporation (Vendor), Hacker	3 (Possible)	2 (Minor)	6	Low	Low
Damages resulting from penetration testing (Kerusakan akibat pengujian penetrasi)	Employees	3 (Possible)	2 (Minor)	6	Low	Low
Destruction of records (Penghancuran Catatan/Data)	Human, Computer Criminal, Unauthorize users	5 (Almost Certain)	5 (Catasropic)	25	Very High	Very high

Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi?

Jawab :

Kegunaan teknologi informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Teknologi informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Teknologi informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan teknolgi informasi untuk berbagai tujuan. Di lain pihak, seiring makin meluasnya implementasi teknologi informasi maka kesadaran akan perlunya dilakukan review atas pengembangan suatu teknologi informasi semakin meningkat. Kesadaran ini muncul karena munculnya berbagai kasus yang terkait dengan gagalnya teknologi informasi, sehingga memberikan akibat yang sangat mempengaruhi kinerja organisasi.

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu teknologi informasi, antara lain:

1. Teknologi informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan teknologi informasi karena adanya “scope creep” (atau pengembangan berlebihan) yang tanpa terkendali.
3. Teknologi informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi.

TASK 2: PENGENDALIAN RISIKO

NAMA : Rumondang Martha A

NIM : 182420069

KELAS : MTI 19 A

JENIS-JENIS RISIKO PENGGUNAAN TI PADA ORGANISASI SERTA PENGENDALIANNYA

Risiko pada penggunaan Teknologi Informasi terbagi dalam 3 jenis yaitu:

1. Alam / Lingkungan
    - Kebakaran
    - Banjir
    - Gempa Bumi
    - Suhu yang bervariasi
    - Kelembaban
2. Manusia
    - Pencurian perangkat
    - Informasi diakses oleh pihak yang tidak berwenang
    - Kebocoran data/informasi organisasi
    - Penyalahgunaan hak akses
    - Cybercrime
3. Sistem dan Infrastruktur
    - Kegagalan/kerusakan hardware
    - Server down
    - Overheat
    - Koneksi jaringan terputus
    - Data corrupt

Sebelum melakukan pengendalian terhadap risiko-risiko tersebut perlu dilakukan analisis risiko yang merupakan upaya untuk memahami risiko lebih dalam. Hasil analisis risiko ini akan menjadi masukan bagi evaluasi risiko dan proses pengambilan keputusan mengenai perlakuan terhadap risiko tersebut. Analisis risiko meninjau dua aspek risiko, yaitu dampak dan kemungkinan. Tingkat risiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan.

Lalu setelah itu, dilakukan evaluasi risiko dengan tujuan untuk membantu proses pengambilan keputusan berdasarkan hasil analisis risiko. Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas risiko-risiko tersebut.

Perlakuan risiko meliputi upaya untuk menyeleksi pilihan-pilihan yang dapat mengurangi atau meniadakan dampak serta kemungkinan terjadinya risiko. Secara umum, perlakuan terhadap suatu risiko dapat berupa salah satu dari empat perlakuan sebagai berikut :

a. Menghindari risiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan risiko tersebut.
b. Berbagi risiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya risiko atau dampak risiko.
c. Mitigasi (mitigation), yaitu melakukan perlakuan risiko untuk mengurangi kemungkinan timbulnya risiko, atau mengurangi dampak risiko bila terjadi, atau mengurangi keduanya.
d. Menerima risiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap risiko tersebut.

TUGAS TOPIC 2

IT AUDIT

OLEH:

SAFTA HASTINI

(NIM : 18240084)

DOSEN:

Dr. WIDYA CHOLIL, S.Kom., M.I.T

PROGRAM PASCASARJANA

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA PALEMBANG

TAHUN 2019

PERTANYAAN:

Sebutkan ada berapa jenis resiko yang dapat terjadi pada penggunaan TI pada suatu organisasi? Jelaskan bagaimana resiko-resiko tersebut dikendalikan (lihat contoh Risk Management Framework yang terlampir)

JAWABAN:

Jenis resiko pada penggunaan TI dan pengendaliannya adalah:

a. Resiko Bawaan (*Inherent Risks)*

   Resiko bawaan ialah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan, jika tidak ada pengendalian intern. Misalnya penyusupan virus (Trojan,malware) komputer dimana data yang terkena virus tidak dapat digunakan lagi/menjadi rusak. **Pengendalian resiko** dengan cara *uninstal* program yang mengerikan dan tidak diketahui, dan update anti virus dan antimalware secara berkala dan scan dalam *safe mode*.

b. Resiko Pengendalian (*Control Risks*)

   Dalam suatu organisasi yang baik seharusnya sudah ada risks assessment, dan dirancang pengendalian intern secara optimal terhadap setiap potensi resiko. Resiko pengendalian ialah masih adanya resiko meskipun sudah ada pengendalian. Contoh: Resiko Pengendalian yang berhubungan dengan review manual log komputer bisa tinggi karena kegiatan memerlukan penyelidikan yang mudah terlewatkan, karena volume informasi login. **Pengendalian resiko** yang berkaitan dengan prosedur validasi data komputerisasi ini biasanya rendah bila proses ini di terapkan secara konsisten.

c. Resiko Deteksi (*Detection Risks*)

   Resiko deteksi merupakan resiko bahwa auditor tidak dapat mendeteksi salah saji material yang terdapat dalam suatu asersi. Resiko deteksi tergantung atas penerapan auditor terhadap resiko audit, resiko bawaan dan resiko pengendalian. Semakin besar resiko audit, semakin besar pula resiko deteksi. Sebaliknya semakin besar resiko bawaan ataupu resiko pengendalian, semakin kecil resiko deteksi. **Pengendalian resiko** pada tahap perencanaan audit, *Planned assessed level of detection risk* untuk setiap asersi signifikan ditentukan dengan cara menerapkan model resiko audit. Actual level of detection risk dapat diubah auditor dengan cara memodifikasi sifdat, penentuan waktu dan luas test substantive yang dilakukan atas suatu asersi. Dalam penentuan resiko deteksi, auditor mempertimbangkan kemungkinan dia melakukan kesalahan seperti kesalahan penerapan prosedur auditing atasu salah melakukan interpretasi terhadap bukti --bukti audit yang telah dihimpun. Contoh: Auditor tak memeriksa 100% saldo akun-akun. Dan Ketidakpastian, kesalahan merancang prosedur audit, salah terap prosedur audit, salah tafsir terhadap hasil audit.

Jenis Resiko dan pengendaliannya:

1. resiko Bawaan (inherent risks)

penyalahgunaan yang melekat pada suatu kegiatan contoh penyusupan virus. pengendaliannya: update antivirus dan unti malware, uninstall program mengerikan dan scan dalam safe mode.

2. resiko Pengendalian (controls risk) ialah masih adanya resiko meskipun sudah ada pengendalian. contoh: resiko pengendalian yang berhubungan dengan review manual log komputer. pengendaliannya: dengan validasi data yg konsisten

3. resiko Deteksi adalah resiko bahwa auditor tidak dapat mendeteksi salah saji material yang terdapat dalam asersi. pengendaliannya dilakukan perencanaan audit, planned assessed level of detection risk untuk setiap asersi