PENILAIAN RESIKO TEKNOIOGI INFORMASI & KEAMANAN SISTEM INFORMASI DENGAN MENGGUNAKAN *FRAMEWORK* COBIT 4.1 DAN GUIDELINES NIST SP 800-30
(Studi Kasus : Rumah Sakit Umum Dr Slamet Garut)

Yana aditia gerhana[1], Erdiansyah, Undang syarifudin
Dosen Teknik Informatika UIN SGD Bandung

Abstrak

Every organization have a goal. In the digital era, organization use automated information technology to process their information for better support for their goals, and risk management plays and important role to protect information assets of organization and for that purpose can be accomplished.

An effective risk management process is an important component of the success of information technology security program. The principle objectives of an organization's risk management should be protect organization and the ability to perform their purpose is not to protect information technology assets only. For this risk management process should not be treated purely as a function but the technique is the basis of the management functions of the organization.

***Key Words**: Information Technology Security, Risk Management, Risk level*

A. **Pendahuluan**

Di banyak perusahaan, informasi dan teknologi merupakan hal yang sangat mendukung tetapi sedikit yang mengerti akan hal tersebut. Keberhasilan organisasi dikenali sebagai keuntungan dari penerapan teknologi informasi yang digunakan untuk menggerakan keuntungan *stakeholders.* Untuk itu organisasi harus mengerti dan mengatur hal hal yang berhubungan dengan resiko. Untuk memenuhi keperluan tersebut salah satunya adalah dengan merawat integritas informasi dan melindungi IT sebagai *asset* yang diperlukan untuk *security management process.*

Konsep dari kebijakan keamanan IT didasari antara lain dari kebijakan keamanan, standarisasi dan prosedur. Kontrol administrasi menjadi efektif karena diperlukan untuk mendefinisikan peraturan–peraturan, pertanggungjawaban dan syarat-syarat yang harus dipenuhi untuk keamanan IT.

Keamanan informasi merupakan aspek kunci dari kebijakan implementasi teknologi informasi, karena penggunaanya yang tersebar luas seperti *internet,*

handheld, portable computer device, mobile, dan wireless technologies memiliki akses data dan informasi semakin mudah dan terbuka. Kondisi ini berpeluang dalam terjadinya masalah-masalah seperti pencurian data, penyerangan melalui virus, *hacking*, serangan *Denial-of-Service* (DoS), dan semua cara baru yang berhubungan dengan kejahatan yang terorganisir. Resiko-resiko tersebut sama potensialnya dengan kesalahan kecerobohan, dapat mengakibatkan maslah yang serius di bidang keuangan, reputasi dan kerusakan lainnya.

Dalam hubungan dengan hal diatas, banyak RSUD yang harus mengimplementasikan penilaian sistem resiko yang dihadapi bila terdapat kegagalan atau *threat* terhadap sistem informasi yang mereka gunakan.

Mengenali keperluan akan keamanan yang baik memerlukan sebuah pedoman yang menjadi standar di dunia IT. COBIT (*Control Objectives for Information and related Technology*) menjadi pedoman dalam pembahasan penilaian di RSUD dr Selamet Garut memfokuskan pada spesifik resiko IT.

Banyaknya upaya yang dilakukan untuk implementasi keamanan dan lingkungan kerja yang terjamin harus didasari seberapa banyak akibat dari masalah keamanan dapat mempengaruhi bisnis, dan mengimplementasikan system keamanan yang baik tidak selalu memerlukan investasi mahal dengan waktu yang lama.

Keuntungan dari keamanan informasi yang baik tidak hanya mengurangi dari resiko atau mengurangi dari akibat. Keamanan yang baik akan memperbaiki reputasi, kepercayaan diri, dan kepercayaan pihak lain dimana bisnis dapat diatur, meningkatkan efisiensi tanpa meghilangkan waktu kerja dan meningkatkan waktu *recover* ketika terjadi insiden keamanan.

B. **Tata Kelola TI**

Definisi *IT Governance* menurut ITGI adalah :

"Suatu bagian terintegrasi dari kepengurusan perusahaan serta mencakup kepemimpinan dan struktur serta proses organisasi yang memastikan bahwa TI perusahaan mempertahankan dan memperluas strategi dan tujuan organisasi."

Pokok pokok permasalahan yang tercakup dalam tata kelola IT adalah :

1. *Strategic Alignment*, penerapan IT harus benar benar mendukung pencapaian misi perusahaan, strategi

IT harus selaras dengan strategi bisnis perusahaan.

2. *Value Delivery*, penerapan IT harus dapat memberikan nilai tambah bagi pencapaian misi perusahaan.
3. *Risk Management*, penerapan IT harus disertai dengan pengidentifikasian resiko resiko IT sehingga dampaknya dapat diatasi.
4. *Resources Management*, peneripan IT harus didukung dengan sumber daya yang memadai dan penggunaan sumber daya yang optimal.
5. *Performance Measurement*, penerapan It harus diukur dan dievaluasi secara berkala untuk memastikan bahwa kinerja dan kapasitas IT sesuai dengan kebutuhan bisnis.

- **COBIT 4.1**

COBIT dapat diartikan sebagai tujuan pengendalian untuk informasi dan teknologi terkait dan merupakan standar terbuka untuk pengendalian terhadap teknologi informasi yang dikembangkan dan dipromosikan oleh Institut IT Governance. COBIT pertama sekali diperkenalkan pada tahun 1996 adalah merupakan alat (*tool*) yang disiapkan untuk mengatur teknologi informasi (*IT Governance tool*).

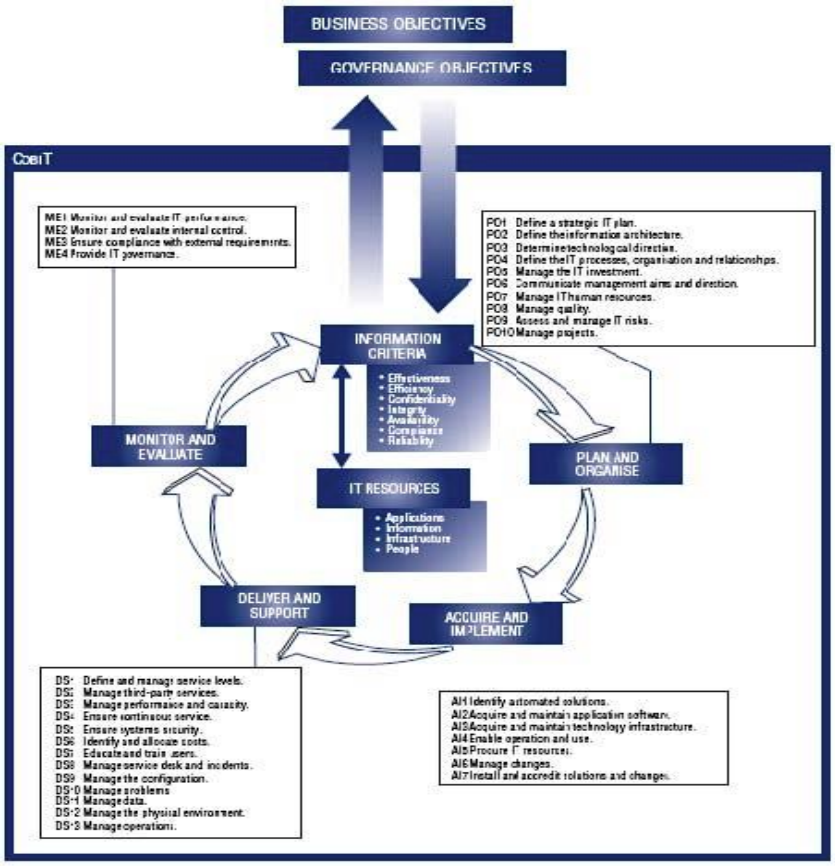
Suatu perencanaan audit TI dapat dimulai dengan menentukan area-area yang relevan dan berisiko paling tinggi, melalui analisa atas ke-34 proses tersebut. Sementara untuk kebutuhan penugasan tertentu, misalnya audit atas proyek TI, dapat dimulai dengan memilih proses yang relevan dari proses-proses tersebut.

COBIT *Framework* dirancang terdiri dari 34 proses detil yang menggambarkan proses TI yang terdiri dari 4 domain yaitu:

1. *Plan and Organise* Domain ini menjelaskan mengenai proses perencanaan dan strategi informasi yang akan dikembangkan.
2. *Acquire and Implement* Domain ini menjelaskan pada proses pemilihan, pengadaan dan penerapan teknologi informasi.
3. *Deliver and Support* Domain ini berkaitan dengan penyampaian aktual dari layanan yang diperlukan, yaitu dengan menyusun operasi tradisional domain ini termasuk pada data aktual.
4. *Monitor and Evaluate* Domain ini mengarahkan terjadinya kesalahan manajemen pada proses pengendalian organisasi dan penjaminan independen yang disediakan oleh audit internal dan eksternal atau diperoleh dari sumber alternatif.

Berikut ini gambar 2.1 merupakan rancangan COBIT *Framework* yang

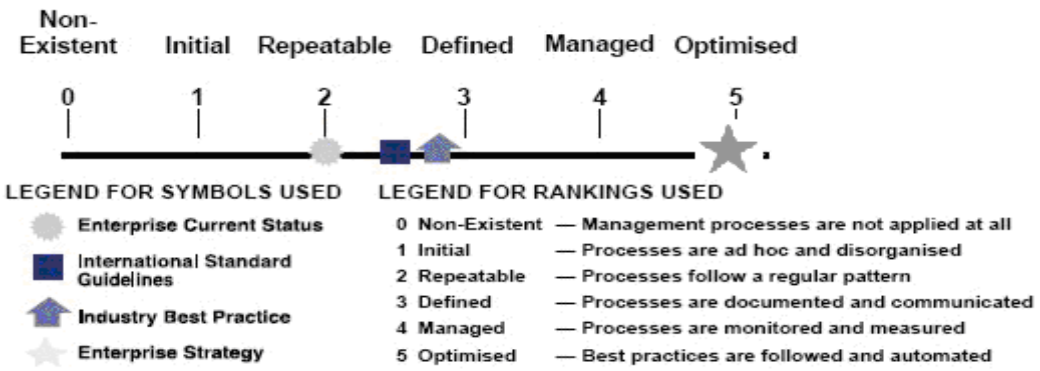
dibagi ke dalam 4 domain, selengkapnya dapat dilihat pada gambar



Gambar 2.1 COBIT Framework

(COBIT 4.1 Excerp, Executive Summary Framework, 2008)

COBIT mempunyai tingkat kematangan (*maturity level*) untuk mengontrol proses-proses TI dengan menggunakan metode penilaian (*scoring*) sehingga suatu organisasi dapat menilai proses-proses TI yang dimilikinya dari skala *non-existent* sampai dengan *optimised* (dari 0 sampai 5).



Gambar 2.2 COBIT Framework Maturity Level

(COBIT 4.1 Excerp, Executive Summary Framework, 2008)

1. **Keamanan Teknologi Informasi**

Keamanan berhubungan dengan perlindungan akan nilai asset yang berlawanan dengan kehilangan, penyalahgunaan, penyingkapan, atau kerusakan. Dalam konteks ini nilai asset adalah informasi yang dicatat dengan, diproses oleh, disimpan didalam, dibagi dengan, dikirim oleh atau diterima oleh, media elektronik. Informasi harus dilindungi atas kerusakan dari berbagai tipe ancaman, banyak akibat dari kehilangan, tidak bisanya akses, dan penyingkapan kesalahan. Ancaman termasuk kesalahan dan kelalaian, pencurian, kecelakaan, dan kerusakan yang disengaja.

Tujuan dari keamanan informasi adalah melindungi kepentingan yang mengandalkan informasi, sistem, dan komunikasi yang mengirim informasi dari yang mengakibatkan kerusakan, dari gangguan akan ketersediaan, kepercayaan dan integritas.

2. **Manajemen Resiko IT**

NIST merupakan singkatan dari *National Institute of Standars and Technology*, SP 800-30 adalah *Special Document* seri 800-30 tentang keamanan komputer. Dokumen ini merupakan atau menjadi panduan pemerintah US untuk memproses data yang sangat sensitif. Panduan ini bukan bersifat perintah atau mengikat. Oleh karena itu penulis ingin membandingkan nilai *indeks* maturity dengan kaidah-kaidah yang ada dalam NIST SP 800-30.

Maksud

Resiko adalah akibat buruk dari suatu celah keamanan, mempertimbangkan keduanya kemungkinan dan akibat dari kejadian. Manajemen resiko adalah suatu proses mengidentifikasi resiko, menilai resiko, dan melakukan langkah untuk mengurangi resiko berdasarkan level yang dapat diterima dan ditetapkan. Sehingga tujuan utamanya adalah menolong organisasi untuk mengelola teknologi informasi menjadi lebih baik yang berhubungan dengan resiko.

Sasaran

Sasaran melakukan manajemen resiko adalah agar organisasi dapat mencapai tujuannya dengan :

- Keamanan yang lebih baik dalam sistem penyimpanan IT, proses,meneruskan informasi organisasi.
- Memungkinkan manajemen membuat informasi lebih baik keputusan

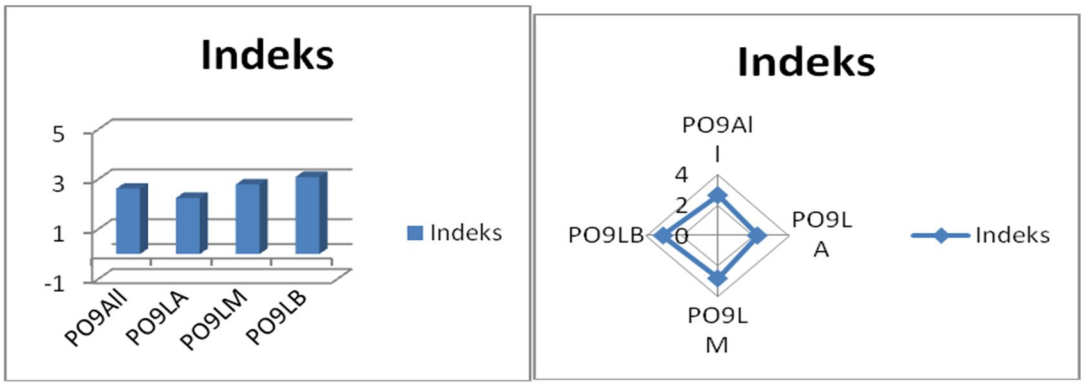
manajemen resiko untuk menilai pengeluaran biaya IT.

- Membantu manajemen untuk mengotorisasi sistem IT yang bertujuan untuk mendukung dokumen hasil performansi dari manajemen resiko.

C. **Hasil Penilaian**

✓ Domain PO9 - Menilai dan Pengaturan Resiko Teknologi Informasi

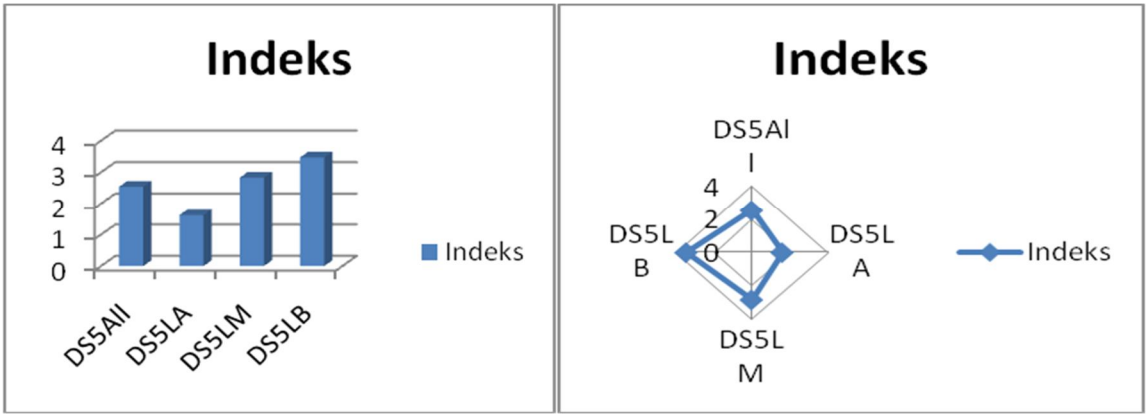
Dari hasil penilaian, terdapat perbedaan pengertian, pemahaman, dan kepentingan antara manajemen level atas, level menengah, dan level bawah dalam Menilai dan Pengaturan ResikoTeknologi Informasi. Lebih jelasnya terlihat pada gambar 5.1 dibawah ini :



Gambar 5.1 Ringkasan Hasil Penilaian PO9

✓ Domain DS5 - Memastikan Keamanan Sistem

Dari hasil penilaian, manajemen level atas, level menengah, dan level bawah tidak memiliki pengertian dan kepentingan yang sama akan keamanan sistem secara utuh.



Gambar 5.2 Ringkasan Hasil Penilaian DS5

✓ Integrasi Indeks Maturity kedalam Risk Level Matrix

Tabel 5.1 menerangkan integrasi indeks maturity kedalam risk level matrix secara keseluruhan

Tabel 5.1 Integrasi Indeks Maturity Kedalam Risk Level Matrix PO9

PO9	Indeks	Skala Resiko	Threat Likelihood	Level Resiko
PO9 All	2.62	52.4	0.5 (sedang)	26.2
PO9 LA	2.25	45	0.5 (sedang)	22.5
PO9 LM	2.79	55.8	0.5 (sedang)	27.9
PO9 LB	3.09	61.8	0.5 (sedang)	30.9

1. Nilai indeks maturity domain PO9LA adalah 2.25 yang berarti *repeatable* / proses dapat diulang, mempunyai nilai yang ekivalen dengan *risk-level matrix* sebesar 22.5 yang didefinisikan bahwa sistem mempunyai level resiko sedang. Hal ini dikuatkan dengan hasil wawancara yang menyatakan resiko implementasi IT sistem yang ada masih belum secara optimal dilakukan.

2. Nilai indeks maturity domain PO9LM dan PO9LB mempunyai nilai *define* / prosestelah ditetapkan, mempunyai nilai yang ekivalen dengan *risk-level matrix* yang mendefinisikan bahwa sistem mempunyai level resiko sedang. Hal ini terlihat dari hasil kuesioner yang cenderung tingkat kepuasan tinggi dengan sistem yang ada. Hal ini berbahaya karena ketidakpahaman akan akibat yang mungkin terjadi dengan pengembangan sistem yang ada dapat membuat celah keamanan semakin besar.

Tabel 5.2 Integrasi Indeks Maturity Kedalam Risk Level Matrix DS5

DS5	Indeks	Skala Resiko	Threat Likelihood	Level Resiko
DS5 All	2.54	50.8	0.5 (sedang)	25.4
DS5 LA	1.62	32.4	0.5 (sedang)	16.2
DS5 LM	2.83	56.6	0.5 (sedang)	28.3
DS5 LB	3.47	69.4	0.5 (sedang)	34.7

1. Nilai indeks maturity domain DS5LA adalah 1.62 yang berarti *repeatable* / proses dapat diulang, mempunyai nilai yang ekivalen dengan *risk-level matrix* sebesar 16.2 yang didefinisikan bahwa sistem mempunyai level resiko sedang. Hal ini merefleksikan tingkat kepuasan dan tingkat

kebutuhan akan keamanan sistem yang rendah di RSUD dr.Selamet Garut yang mana dapat meningkatkan level resiko apabila SDM dan kebijakan organisasi tidak mendukung akan perbaikan tingkat keamanan.

2. Nilai indeks maturity domain DS5LM dan DS5LB mempunyai nilai define / prosestelah ditetapkan, mempunyai nilai yang ekivalen dengan risk-level matrix yang mendefinisikan bahwa sistem mempunyai level resiko sedang. Hal ini terlihat dari hasil kuesioner yang cenderung tingkat kepuasan tinggi dengan sistem keamanan yang ada. Pihak manajemen level menengah belum pernah melakukan tes tingkat keamanan oleh pihak ke tiga yang mana bertujuan untuk mengetahui sejauh mana kebijakan organisasi telah mampu melindungi aset SI/TI dari ancaman.

D. **Kesimpulan**

Dari kajian terhadap rancangan model *IT Governance* dan audit sistem informasi institusi dapat ditarik kesimpulan :

1. Rumah Sakit Umum dr. Slamet sudah memiliki dan menetapkan rencana rancangan model *IT Governance* dan audit SI sebagai bagian dari pengaturan TI dalam rangka mencapai tujuan institusi secara efektif dan efisien.
2. COBIT versi 4.1 dapat digunakan sebagai standar model audit Sistem Informasi Rumah Sakit Umum dr. Slamet. Kerangka kerja COBIT disesuaikan pada model audit Sistem Informasi Rumah Sakit Umum dr. Slamet dengan melihat proses bisnis dan tanggungjawab proses teknologi informasi terhadap aktivitas rumah sakit.
3. Model audit yang dikembangkan pada tesis ini dapat digunakan bagi pihak manajemen Rumah Sakit Umum dr. Slamet sebagai pedoman terhadap pengendalian internal.
4. Hubungan antara nilai indeks maturity yang berdasarkan dari kerangka kerja COBIT 4.1 sesuai dengan level resiko yang dihitung dari level matrik resiko yang didasari dari kerangka kerja NIST SP 800-30.
5. Berdasarkan dua buah kerangka kerja yang dijadikan acuan penilaian dapat dikatakan bahwa RSUD dr. Selamet Garut :

6. Mempunyai tingkat keamanan yang cukup untuk mendukung tujuan organisasinya akan tetapi untuk jangka menengah dan panjang.

7. Pengertian, pemahaman akan prinsip, tujuan dari keamanan sistem tiap level manajemen terdapat kesenjangan yang kentara.

8. Dari penilaian resiko yang berdasarkan COBIT 4.1 dan NIST SP 800-30, RSUD dr.Selamet Garut mempunyi tingkat resiko sedang(medium).

9. Proses mitigasi resiko belum dikerjakan karena belum teridentifikasinya sumber-sumber ancaman oleh pihak RSUD dr.Selamet Garut.

E. **Daftar Pustaka**

An Introductory Overview of ITIL V3 – The IT Service Management Service.

CISA (Certified Information Systems Auditor) Study Guide, 2008

CEH (Certified Ethical Hacker) Study Guide V.5, 2008.

COBIT 4.1 – IT Governance Implementation Guide.

COBIT - Implementation Set.

COBIT - Security Baseline 2004-Rec.

Computer Security, NIST (National Institute of Standard and Technology) SP 800-30, 2002 – United State Department of Commerce.

Hack Attack Testing – How to Conduct Your Own Security Audit, Jhon Chirillo.

Information Security, NIST (National Institute of Standard and Technology) 2004 – United State Department of Commerce.

Information System Risk Assesment – Practice of Leading Organizations, GAO – US General Accounting Office, 1998.

ISO/IEC 17799 – Information Technology – Security Techniques – Code of practice for Information Security Management, ISO / IEC 2006.

Maximum Security : A Hacker's Guide to Protecting Your Internet Site and Network.

Technical Guide to Information Security Testing and Assesment, NIST (National Institute of Standard and Technology) 2004 – United State Department of Commerce.

The CISSP Prep Guide – Mastering the Ten Domains of Computer Security, Ronald L Krutz dan Russell Dean Vines -2002.

The Ethical Hack : A Framework for Business Value Penetration Testing, James S Tiller.

The Hacker Handbook, The Strategy behind Breaking into Defending Network.