bidang
TEKNIK

PERANCANGAN SISTEM MANAJEMEN KEAMANAN ASET INTELEKTUAL PUSLIT TELIMEK LIPI MENGGUNAKAN KERANGKA KERJA TOGAF DAN STANDAR ISO/IEC 17799:2005

RITAWARNI, YEFFRY HANDOKO, IMELDA
Program Studi Magister Sistem Informasi, Fakultas Pascasarjana
Universitas Komputer Indonesia

Puslit Telimek memiliki lima bidang, semua bidang tersebut setiap tahunnya melakukan berbagai macam program kegiatan penelitian. Yang dihasilkan dari penelitian tersebut berupa Hak Kekayaan Intelektual (HKI). Ancaman terhadap keamanan Hak Kekayaan Intelektual juga dapat terjadi yang beresiko pencurian informasi yang tidak terotorisasi, penggunaan yang tidak terotorisasi, modifikasi yang tidak terotorisasi dan penghancuran yang tidak terotorisasi. Dari permasalahan tersebut maka diusulkan untuk perancangan sistem manajemen keamanan aset Hak Kekayaan Intelektual menggunakan Kerangka Kerja TOGAF dan Standar ISO/IEC 17799:2005 pada Puslit Telimek dengan kajian mengenai Hak Kekayaan Intelektual. Metode penelitian yang digunakan yaitu TOGAF ADM (Architecture Development Method) yang terdiri dari lima tahapan yaitu : Architecture Vision, Business Architecture, Information Systems Architectures, Technology Architecture, Opportunities and Solutions. Hasil penelitian ini diperoleh bahwa : (1) Arsitektur Sistem Infomrasi dari kerangka kerja TOGAF dapat membantu mempermudah dalam mengelola, menelusuri Hak Kekayaan Intelektual. (2) Dengan menerapkan kebijakan dari Standar ISO/IEC 17799:2005 sebagai standar sistem manajemen keamanan informasi khususnya untuk Hak Kekayaan Intelektual sehingga dapat meminimalisir resiko terjadinya ancaman baik dari internal maupun eksternal seperti penggunaan dan modifikasi yang tidak terotorisasi. Adapun untuk sarannya yaitu menggunakan keseluruhan klausa yang terdapat pada kerangka kerja ISO/IEC 17799:2005 sehingga dapat meminimalisir risiko dari ancaman-ancaman keseluruhan aspek yang mendukung keberlangsungan proses bisnis di Puslit Telimek.

Keywords **:** *Sistem, Keamanan, Aset, Kerangka Kerja, TOGAF, ISO/IEC 17799:2005*

PENDAHULUAN

Puslit Telimek memiliki beberapa bidang seperti bidang mekatronik, bidang peralatan transportasi, bidang elektronika daya dan mesin listrik, bidang rekayasa, dan bidang sarana penelitian. Semua bidang tersebut setiap tahunnya melakukan berbagai macam program kegiatan penelitian. Yang dihasilkan dari penelitian tersebut seperti Hak kekayaan Intelektual (HKI), baik berupa Hak Cipta maupun Hak kekayaan Industri dan publikasi ilmiah yang termuat dalam buku ber-ISBN dan

terbitan berkala yang ber-ISSN. Semua hasil penelitian merupakan aset.

Aset dalam tata kelola teknologi informasi terdiri dari *Human Assets, Financial Assets, Physical Assets, Intellectual Property (IP) Assets, Information and IT Assets, Relationship Assets.* Hasil dari penelitian yang telah disebutkan sebelumnya termasuk ke dalam *Intellectual Property Assets*.

Pengelolaan aset perusahaan masih dalam proses terpisah-pisah (manual dan otomatis) yang belum terintegrasi untuk mendukung strategi bisnis.

Intellectual Property Assets belum adanya suatu arsitektur informasi, arsitektur aplikasi dan teknologi yang menyatukan secara keseluruhan sehingga untuk menelusuri historis penelitian yang pernah diajukan (data peneliti, tempat, judul dan biaya penelitian) , kemajuan pelaksanaan penelitian dan hasil penelitian membutuhkan waktu lama dan kemungkinan informasi tersebut tercecer atau hilang juga ada dikarenakan masih berada pada peneliti .

Selain itu ancaman terhadap keamanan informasi *Intellectual Property Assets* juga dapat terjadi. Ancaman keamanan informasi adalah orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan. Ancaman keamanan dapat bersifat internal maupun eksternal. Resiko dari ancaman tersebut seperti pencurian informasi yang tidak terotorisasi, penggunaan yang tidak terotorisasi, dan modifikasi yang tidak terotorisasi.

Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu (1) kerahasian : perusahaan berusaha melindungi data dan informasi dari pengungkapan kepada orang-orang yang tidak berwenang. (2) ketersediaan : menyediakan data dan informasi bagi pihak-pihak yang memiliki berwenang untuk menggunakannya.(3) integritas : semua sistem informasi harus memberikan representasi akurat atas sistem fisik yang direpresentasikannya [1].

Dari permasalahan tersebut diatas maka diusulkan untuk perancangan sistem manajemen keamanan aset menggunakan TOGAF dan ISO/IEC 17799:2005 untuk Puslit Telimek yang khususnya mengenai *Intellectual Property Assets*.

TOGAF memberikan metode yang detail mengenai bagaimana membangun, mengelola dan mengimplementasikan arsitektur *enterprise* dan sistem informasi yang disebut dengan *Architecture Development Method* (*ADM*).

Penggabungan *framework* ISO/IEC 17799:2005 dan TOGAF diharapkan dapat menghasilkan suatu perancangan sistem manajemen keamanan informasi yang dapat meminimalisir resiko dari ancaman-ancaman. Yang mana merancang sistem menggunakan TOGAF dan untuk keamanannya mengimplementasikan kebijakan yang terdapat pada ISO/IEC 17799:2005.

TINJAUAN PUSTAKA

Berikut ini adalah tinjauan pusataka yang berkaitan dengan penelitian ini :

1. Aset

Didalam tata kelola teknologi informasi aset yang dikelola terdiri dari enam jenis yaitu sebagai berikut :

a. *Human Assets*
   Orang, skil, riwayat kerja, pelatihan, laporan, mentor, kompetensi.
b. *Financial Assets*
   Uang, investasti, kewajiban, arus kas.
c. *Physical Assets*
   Bangunan, pabrik, peralatan, pemeliharaan, keamanan.
d. *Intellectual Property (IP) Assets*
   Intellectual Property mencakup produk, hak paten, hak cipta, dan sistem.

e. *Information and IT Assets*
   Data digital, informasi, dan pengetahuan tentang konsumen, proses, keuangan, sistem informasi.
f. *Relationship Assets*
   Hubungan baik dengan relasi, brand, reputasi dengan konsumen, pemasok, unit bisnis, peraturan, pesaing, mitra.

Tata kelola aset memiliki cakupan mekanisme yang luas dalam suatu organisasi. Beberapa mekanisme yang unik khususnya untuk aset dan persilangan lainnya dan mengintegrasikan berbagai macam tipe aset yang memastikan bersinerginya antara aset-aset penting [2].

2. Sistem Manajemen Keamanan Informasi (ISO/IEC 17799:2005)

Informasi adalah aset yang sangat penting bagi bisnis, yang merupakan hal mendasar bagi organisasi bisnis dan konsekwensi yang dibutuhkan untuk keamanan yang sesuai. Keamanan informasi adalah melindungi informasi dengan cakupan yang luas dari ancaman untuk keberlangsungan bisnis, meminimalisir resiko bisnis, meningkatkan pendapatan atas investasi dan peluang bisnis. Keamanan informasi dapat dicapai dengan mengimplementasi pengaturan kontrol yang sewajarnya mencakup kebijakan, proses, prosedur, struktur keorganisasian dan fungsi perangkat lunak dan perangkat keras. Keamanan informasi dibutuhkan untuk menetapkan, mengimplementasi, memonitor, meninjau dan meningkatkan keamanan secara keseluruhan [3].

ISO/IEC 17799:2005 (sistem manajemen keamanan informasi) memiliki 11(sebelas) klausa kontrol keamanan yaitu sebagai berikut :

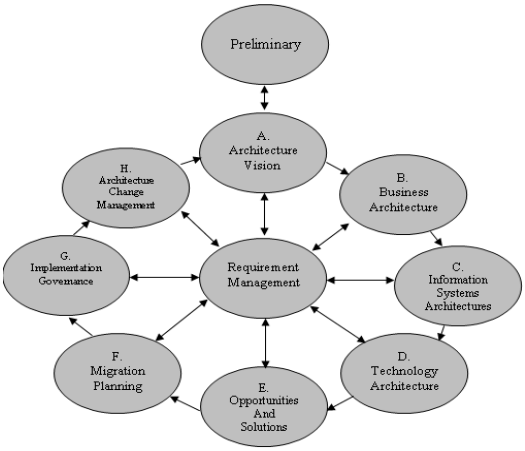
a. Kebijakan keamanan infromasi
b. Keamanan informasi organisasi
c. Manajemen aset
d. Keamanan sumber daya manusia
e. Keamanan fisik dan lingkungan
f. Komunikasi dan manajemen operasi
g. Akses Kontrol
h. Pengadaan/akuisisi,pengembangan dan pemeliharaan sistem informasi
i. Manajemen insisden keamanan informasi
j. Manajemen kelangsungan bisnis
k. Kepatuhan

3. *The Open Group Architecture Framework (* TOGAF)

TOGAF adalah suatu kerangka kerja arsitektur. TOGAF adalah suatu alat yang membantu penerimaan, produksi, penggunaan, dan pemeliharaan arsitektur *enterprise*. Hal mendasar yang mempunyai pendukung proses model praktis yang baik dan dapat digunakan ulang untuk kumpulan aset arsitektur yang ada. TOGAF dikembangkan oleh *The Open Group Architecture Forum*. Versi pertama TOGAF dikembangkan pada tahun 1995. Untuk TOGAF 9 dipublikasikan pada tahun 2009 [4].

4. *The Architecture Development Method* (*ADM*)

Architecture Development Method (ADM) membentuk inti dari TOGAF dan metode untuk menurunkan arsitektur *enterprise* suatu organisasi secara lebih spesifik, dimana akan menghasilkan kontribusi dari berbagai pengguna arsitektur. ADM mencakup penetapan kerangka kerja arsitektur, pengembangan isi arsitektur, peralihan, pengaturan realisasi dari arsitektur. ADM menjelaskan urutan fase dalam proses perubahan dengan grafik lingkaran ADM seperti yang ditunjukkan pada gambar berikut ini :



Gambar 1. Tahapan Proses *Architecture Development Method* (*ADM*)

METODOLOGI PENELITIAN

Berikut akan dijelaskan tahapan-tahapan metode yang dilakukan :

1. Pengumpulan Data

Ada berbagai macam teknik pengumpulan data salah satunya yaitu dengan wawancara. Wawancara adalah komunikasi dua arah untuk mendapatkan data dari responden. Dengan mewawancarai pihak-pihak yang terkait dengan tempat penelitian ini akan memudahkan dalam mengetahui semua kegiatan yang berlangsung saat ini dan memperoleh data yang dibutuhkan.

2. *Preliminary*

Tahap permulaan ini harus dapat dukungan dari organisasi untuk mengsukseskan penyusunan arsitektur perusahaan.

3. *Architecture Vision*

Pada tahap ini yang akan dilakukan yaitu memahami misi, visi, strategi, dan tujuan perusahaan sehingga akan membantu menghasilkan arsitektur perusahaan yang ideal untuk diterapkan.

4. *Business Architecture*

Pada tahapan ini yang harus dilakukan yaitu menjelaskan proses dasar dari *business architecture*, mengembangkan target *business architecture*, menganalisa kesenjangan antara garis dasar dan arsitektur target.

5. *Information Systems Architectures*

Pada tahapan ini ada dua langkah yang akan dikembangkan yaitu:

a. Arsitektur data : mendefinisikan tipe dan sumber data yang dibutuhkan untuk mendukung bisnis, dimana yang dapat dimengerti oleh pihak-pihak yang terlibat pada Puslit Telimek dalam proses pengelolaan aset.
b. Arsitektur aplikasi : mendefinisikan berbagai macam sistem aplikasi yang dibutuhkan untuk memproses data dan mendukung bisnis yang ada pada Puslit Telimek.

Selain dua langkah diatas, pada tahapan ini juga akan digunakan kebijakan-kebijakan ISO/IEC 17799:2005 yang berkaitan dengan sistem informasi seperti kontrol akses.

6. *Technology Architecture*

Tahapan ini adalah mendokumentasikan dasar organisasi dari sistem TI yang akan digunakan untuk menunjang pengelolaan aset di perusahaan berupa : perangkat keras, perangkat lunak dan teknologi komunikasi serta kebijakan ISO/IEC 17799:2005 yang berkaitan dengan arsitektur teknologi.

7. *Opportunities and Solutions*

Tahapan ini adalah tahapan awal yang berkonsentrasi langsung dengan pelaksanaan. Ini menjelaskan proses identifikasi penerimaan untuk mencapai target arsitektur yang telah diidentifikasi pada tahapan sebelumnya.

HASIL PENELITIAN DAN PEMBAHASAN

Tahapan-tahapan dalam perancangan sistem manajemen keamanan aset yaitu :

1. Identifikasi Awal

Pada tahapan ini mengobservasi mengenai arsitektur aset yang berada di Puslit Telimek saat ini. Tujuannya untuk mengetahui sejauh mana arsitektur dan teknologi yang dimanfaatkan.

a. Analisis dan Identifikasi Resiko

Analisis dan diidentifikasi resiko yang mungkin terjadi dalam proses pengelolaan *Intellectual Property Assets* yaitu sebagai berikut :

Tabel 1. Analisis dan Identifikasi Resiko

No	Resiko	Aset
1	Keamanan dalam operasi	*Software*, data
	Penyebab Modifikasi yang dilakukan oleh pihak yang tidak berwenang. Perubahan sistem pengolahan data. Tidak ada mekanisme *back up* data.	
	Dampak Tidak tersedianya data, proses bisnis terhambat.	
	Kelemahan Kebijakan prosedur opersional. Kebijakan prosedur manajemen perubahan. Kebijakan prosedur *back up* data.	
2	*Social engineering*	*Software,* data
	Penyebab Tidak ada batasan waktu kepada pengguna yang telah masuk ke sistem. Tidak ada identifikasi dan otentikasi pengguna.	
	Dampak Pencurian data, tidak dapat mengkases sistem.	
	Kelemahan Kebijakan otentikasi pengguna pada saat login dan sesi *time out*	
3	*SQL Injection*	*Software*, data
	Penyebab Tidak ada mekanisme validasi data masukan pengguna. Tidak ada batasan hak akses setiap pengguna. Tidak ada pemberitahuan ketika terjadi kegagalan pada sistem.	
	Dampak Kehilangan data, perubahan data, penghapusan data, kegagalan sistem, proses bisnis terganggu.	
	Kelemahan Mekanisme validasi data masukan oleh sistem. Mekanisme pembatasan hak akses pengguna. Mekanisme pembatasan input karakter untuk form login.	
4	Virus	*Software*, data,
	Penyebab Penyebaran virus melalui *flasdisk*, dan *email.* Tidak update *antivirus*	
	Dampak Kerusakan data, kehilangan data.	
	Kelemahan Tidak ada antivirus yang membentengi virus untuk menyebar di laptop/komputer.	
5	Pengelolaan *Password*	*Software*, data
	Penyebab Memberi tahu *password* kepada orang lain. Mencatat *password* di kertas dan dibuang ke tempat sampah tidak dihancurkan terlebih dahulu. Tidak menggunakan variasi karakter untuk *password*.	
	Dampak Yang tidak berwenang dapat login ke sistem. Mencuri data/informasi dari sistem. Pembaharuan password oleh pihak yang tidak berwenang.	
	Kelemahan Kebijakan penggunaan password	

6	Kehilangan Laptop/ komputer	*Hardware*, *software*, data
	Penyebab Meletakkan laptop sembarangan di tempat umum tanpa pengamanan. Tidak ada pengamanan di sekitar kantor.	
	Dampak Kehilangan data yang disimpan di laptop/komputer tersebut.	
	Kelemahan Kesadaran akan pentingnya perlindungan keamanan terhadap laptop/ komputer. Kebijakan pengamanan terhadap laptop/komputer.	
7	*Hacking*	*Software*, data,jaringan
	Penyebab Adanya celah keamanan yang dimanfaatkan oleh *hacker* untuk mencuri data, merusak data dan memindahkan data ke tempat lain.	
	Dampak Kahilangan data, perubahan pada sistem.	
	Kelemahan Sistem keamanan server.	

Tabel 2. Probabilitas Kejadian

Probabilitas Kejadian	Frekuensi	Nilai
Tidak pernah terjadi	Tidak pernah	0
Sangat rendah	2-3 kali setiap 5 tahun	1
Rendah	<= 1 kali per tahun	2
Sedang	<= 1 kali setiap 6 bulan	3
Tinggi	<= 1 kali setiap bulan	4
Sangat tinggi	<= 1 kali setiap bulan	5
Ekstrim	<= 1 kali setiap hari	6

Tabel 3. Dampak Resiko

Dampak kejadian	Derajat dampak	Nilai
Tidak berpengaruh	Tidak mempunyai dampak	0
Minor	Tidak perlu usaha lebih untuk memperbaiki	1
Signifikan	Dampak dapat diukur, perlu usaha lebih untuk memperbaiki	2
Merusak	Merusak reputasi dan keyakinan perusahaan. Memerlukan sumber daya lebih untuk memperbaiki	3
Serius	Kehilangan konektivitas. Kehilangan banyak data atau layanan.	4
Parah	Kegagalan sistem permanen	5

Tabel 4. Perhitungan Resiko

Perhitungan resiko (probabilitas x dampak)	Nilai
0	Tidak berpengaruh
1-3	Rendah
4-7	Sedang
8-14	Tinggi
15-19	Ekstrim

Tabel 5. Penilaian Resiko

Jenis Resiko	Komponen nilai	Nilai
Keamanan dalam operasi	Probabilitas	4
	Dampak	2
	Nilai Resiko	8
Kategori resiko : TINGGI		
Social engineering	Probabilitas	3
	Dampak	2
	Nilai Resiko	6
Kategori resiko : SEDANG		
SQL Injection	Probabilitas	3
	Dampak	2
	Nilai Resiko	6
Kategori resiko : SEDANG		
Virus	Probabilitas	4
	Dampak	3
	Nilai Resiko	12
Kategori resiko : TINGGI		
Pengelolaan *Password*	Probabilitas	3
	Dampak	2
	Nilai Resiko	6
Kategori resiko : SEDANG		
Kehilangan Laptop/ komputer	Probabilitas	1
	Dampak	4
	Nilai Resiko	5
Kategori resiko : SEDANG		
Hacking	Probabilitas	3
	Dampak	4
	Nilai Resiko	12
Kategori resiko : TINGGI		

Dari hasil analisis dan identifikasi resiko dapat disimpulkan bahwa :

1) Resiko-resiko terjadi karena belum adanya kebijakan untuk manajemen keamanan aset khususnya untuk *Intellectual Property Assets.*
2) Resiko dengan kategori sedang maupun tinggi dapat memberi dampak yang kurang baik bagi Puslit Telimek dalam proses bisnisnya seperti terhambatnya proses pembuatan laporan hasil penelitian karena datanya hilang atau rusak karena kena virus.
3) Dengan adanya indikasi kategori tinggi ini menunjukkan bahwa proses pengelolaan *Intellectual Property Assets* masih sangat lemah sehingga menimbulkan ancaman yang serius jika tidak ditangani dengan segera.

2. *Architecture vision*

Dalam penelitian ini yang menjadi visi dari perancangan sistem manajemen keamanan aset di Puslit Telimek yaitu :

a. Merancang arsitektur aset di Puslit Telimek yang meliputi *Architecture Vision, Business Architecture, Information Systems Architectures, Technology Architecture, Opportunities and Solutions* yang memadai untuk mengelola *Intellectual Property Assets*.
b. Memanfaatkan ISO/IEC 17799:2005 sebagai standar sistem manajemen keamanan informasi khususnya *Intellectual Property Assets* untuk meminimalisir terjadinya ancaman seperti penggunaan dan modifikasi yang tidak terotorisasi.

3. *Business Architecture*

Pada tahapan ini dilakukan perancangan arsitektur terhadap proses-proses bisnis yang terkait langsung dengan *Intellectual Property Assets.*

a. Analisis Kesenjangan *Business Architecture*

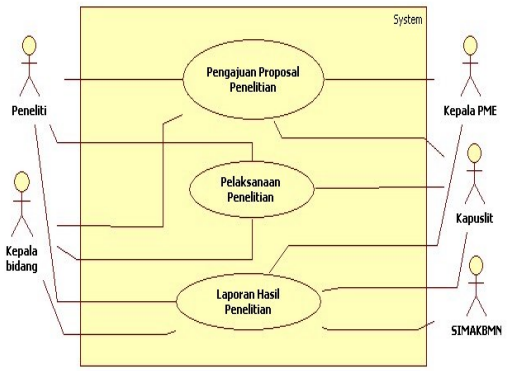
Analisis kesenjangan *business architecture*-nya adalah sebagai berikut :

Tabel 6. Analisis Kesenjangan *Business Architecture*

Kondisi Saat Ini	Target Masa Depan
Dalam menjalankan bisnis, Puslit Telimek belum menggunakan TI /SI sebagai kebutuhan utama khususnya yang menangani *Intellectual Property Assets*	Puslit Telimek memiliki rancangan arsitektur TI/SI

b. Usulan Perancangan Pengelolaan Aset

Untuk usulan perancangan pengelolaan *Intellectual Property Assets* sebagai berikut :



Gambar 2. Usulan Perancangan Pengelolaan Aset

4. *Information Systems Architectures*

Tahapan ini terdiri dari dua garis besar yaitu informasi dan sistem aplikasi yang digunakan untuk proses kerja.

a. Analisis Kesenjangan *Information Systems Architectures*

Daftar analisis kesenjangan *information systems architectures*-nya pada tabel 7 :

Tabel 7. Analisis Kesenjangan *Information Systems Architectures*

No	Kondisi Saat Ini	Target Masa Depan
1	Belum adanya database khusus yang terkait dengan *Intellectual Property Assets*	Tersedia database *Intellectual Property Assets*
2	Data belum ter-*backup*	*Backup* data terpenuhi secara rutin dan *backup* otomatis
3	Belum adanya aplikasi khusus yang menangani *Intellectual Property Assets* yang terintegrasi	Tersedia aplikasi *Intellectual Property Assets* yang terintegrasi
4	Belum adanya informasi untuk manajemen tingkat atas (Kepala Puslit Telimek). Informasi *Intellectual Property Assets* masih didapatkan secara manual	Tersedia sistem informasi untuk tingkat manajemen sehingga manajemen dapat dengan cepat mengetahui tentang hasil penelitian yang berupa *Intellectual Property Assets* secara *realtime dan uptodate*

No	Kondisi Saat Ini	Target Masa Depan
5	Belum adanya standar kebijakan keamanan untuk *Information Systems Architectures*	Memiliki standar kebijakan keamanan untuk *Information Systems Architectures*

b. Analisis Kelas-Kelas Data

Berikut ini kelas-kelas data yang berkaitan dengan *Intellectual Property Assets* :

Tabel 8. Daftar Kelas Data Pada Arsitektur Data

Kandidat Kelas	Kelas Data
Peneliti	Peneliti Utama/ Madya/ Muda Perekayasa Utama/ Madya Teknisi Litkayasa Pelakasana Pranata Humas Madya Pranata Humas Pelaksana Lanjutan Arsiparis Penyelia Arsiparis Pelakasana Lanjutan
Hasil Kegiatan Penelitian	Hak kekayaan Intelektual (HKI) Publikasi Ilmiah Produk
Jenis Program	Tematik Kompetitif Penugasan Khusus Pengembangan Kelembagaan Peningkatan kemapuan individu
Jenis Promosi	Pameran Publikasi Media Cetak Publikasi Media elektronik / TV

c. Usulan Perancangan Arsitektur Aplikasi

Pada tahapan ini mendefinisikan aplikasi-aplikasi yang diperlukan untuk mengelola *Intellectual Property Assets*.

Tabel 9. Arsitektur Aplikasi Yang Diusulkan

No. App	Nama	Deskripsi
APL-1	Aplikasi data peneliti	Aplikasi ini untuk mengelola data peneliti baik yang baru maupun lama
APL-2	Aplikasi data penelitian	Aplikasi ini untuk mengelola *Intellectual Property Assets,* mulai dari pengajuan proposal penelitian, pelaksanaan penelitian, dan laporan hasil penelitian.
APL-3	Aplikasi data promosi	Aplikasi ini untuk mengelola keikutsertaan promosi di berbagai media.
APL-4	Aplikasi penghargaan	Aplikasi ini untuk mengelola penghargaan terhadap prestasi peneliti atau hasil penelitian yang dilakukan.

Untuk kebijakan keamanan mengenai aplikasi yang merujuk kepada ISO/IEC 17799 :2005 yaitu :

1) Pemberian hak akses yang tingkatannya tinggi hanya diberikan kepada karyawan yang benar-benar kompeten.
2) Hak akses pengguna diberikan berdasarkan tugas pokok dan fungsi pengguna.

3) Hak akses pengguna yang menjalani mutasi atau tidak lagi bekerja harus segera di non-aktifkan maksimum 7 (hari) setelah tanggal yang ditetapkan.
4) Hak akses tidak boleh dipinjamkan kepada pengguna lain.
5) Tingkat akses atau kompleksitas yang sesuai : menggunakan beberapa tingkat akses yang membutuhkan beberapa kata sandi.

5. *Technology Architecture*

Tahapan *technology architecture* meliputi perangkat lunak dan perangkat keras serta kebijakan untuk keamanan dalam penggunaan teknologi dengan menggunakan kebijakan ISO/IEC 17799:2005 yaitu klausa keenam "Manajemen Komunikasi Dan Operasi".

a. Analisis Kesenjangan *Technology Architecture*

Daftar analisis kesenjangan *technology architecture*-nya adalah sebagai berikut :

Tabel 10. Analisis Kesenjangan *Techology Architecture*

No	Kondisi Saat Ini	Target Masa Depan
1	Belum adanya server untuk *Intellectual Property Assets*	Tersedia server untuk *Intellectual Property Assets*
2	Belum adanya standar kebijakan keamanan untuk *techology architecture*	Memiliki standar kebijakan keamanan untuk *techology architecture*

b. Usulan Perancangan Teknologi Perangkat Lunak

Tahapan ini menjabarkan tentang usulan perancangan teknologi perangkat lunak yang akan digunakan, yaitu :

1) Teknologi Aplikasi
2) Kriptografi – MD5 (*Message Digest* versi 5)
3) Teknologi Sistem Operasi
4) *Office Software*
5) *Antivirus*

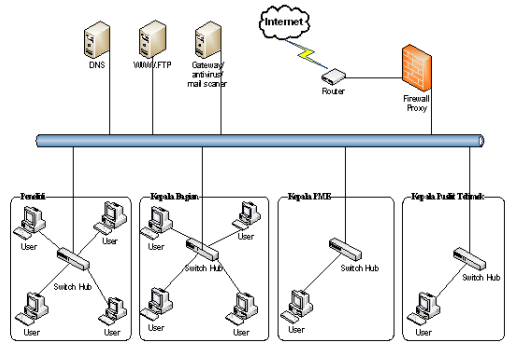
c. Usulan Perancangan Teknologi Perangkat Keras

Tahapan ini memberikan usulan perancangan teknologi perangkat keras yang akan digunakan. Adapun rinciannya adalah sebagai berikut :

1) *Personal computer*
2) Laptop
3) Server

d. Usulan Perancangan Teknologi Jaringan

Usulan arsitektur jaringannya seperti yang diilustrasikan pada gambar di bawah ini :



Gambar 3. Usulan Perancangan Teknologi Jaringan

Kebijakan keamanan jaringan yaitu :

1) *Router*

Prosedur yang harus dilakukan dalam pengamanan akses pada *router* yaitu :

a) Membuat akses pengguna dan kata sandi bagi administrator *router* yang diberikan hanya kepada karyawan yang berwenang di masing-masing lokasi sistem informasi.
b) Membuat *control access-list*
c) Mengaktifkan *encryption key* pada administrator *password router* baik pada akses *console* maupun akses telnet.

2) *Switch Hub*

Prosedur yang harus dilakukan dalam pengamanan akses pada *switch hub* yaitu :

a) Mengakatifkan *encryption key* pada administrator *switch hub* baik pada akses *console* maupun akses telnet.
b) Membatasi waktu dengan *automatic logout* bila administrator login tanpa aktifitas.

3) *Firewall*

Firewall berfungsi sebagai penyaring atau penghalang yang membatasi aliran data ke dan dari perusahaan tersebut dan internet.

6. *Opportunities and Solutions*

Pada tahapan ini lebih menekan pada usulan solusi. Adapun usulan solusinya adalah sebagai berikut :

Fase	Kondisi Saat ini	Usulan Solusi
Business Architecture	Dalam menjalankan bisnis, Puslit Telimek belum menggunakan TI /SI sebagai kebutuhan utama khususnya yang menangani *Intellectual Property Assets*	Merancang penererapan TI/ SI pada proses bisnis
Information Systems Architecture	Belum adanya database khusus yang terkait dengan *Intellectual Property Assets*	Merancang database untuk *Intellectual Property Assets*
	Data belum ter-*backup.*	Menjadwalkan *backup database* secara berkala
	Belum adanya aplikasi khusus yang menangani *Intellectual Property Assets* yang terintegrasi	Pengembangan aplikasi untuk menangani *Intellectual Property Assets* yang terintegrasi
	Belum adanya informasi untuk manajemen tingkat atas (Kepala Puslit Telimek). Informasi *Intellectual Property Assets* masih didapatkan secara manual.	Merancang aplikasi untuk manajemen report.
	Belum adanya standar kebijakan keamanan untuk *Information Systems Architectures*	Menggunakan standar kebijakan ISO/IEC 17799:2005 yaitu klausa ketujuh untuk keamanan *Information Systems Architectures*

KESIMPULAN DAN SARAN

Dari hasil penelitian yang dilakukan dapat diberi kesimpulan dan saran sebagai berikut :

1. Kesimpulan

a. Dengan adanya arsitektur aset di Puslit Telimek yang meliputi *Architecture Vision, Business Architecture, Information Systems Architectures, Technology Architecture, Opportunities and Solution* dapat membantu mempermudah dalam mengelola, menelusuri *Intellectual Property Assets.*
b. Dengan menerapkan kebijakan dari ISO/IEC 17799:2005 sebagai standar sistem manajemen keamanan informasi khususnya untuk *Intellectual Property Assets* sehingga dapat meminimalisir resiko terjadinya ancaman baik dari internal maupun eksternal seperti penggunaan dan modifikasi yang tidak terotorisasi.

2. Saran

Adapun sarannya yaitu menggunakan keseluruhan klausa yang terdapat pada kerangka kerja ISO/IEC 17799:2005 sehingga dapat meminimalisir risiko dari ancaman-ancaman keseluruhan aspek yang mendukung keberlangsungan proses bisnis di Puslit Telimek.

DAFTAR PUSTAKA

[1] Mcleod,R. dan G.P. Schell, 2009, Sistem Informasi Manajemen, Salemba Empat, Jakarta.

[2] Weil, P. dan J.W. Ross, 2004, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results,* Harvard Business School Press.

[3] ISO/IEC, 2005, *Information Technology-Security Techniques-Code Of Practice For Information security Management*, Switzerland.

[4] Harrison, R, 2009, TOGAF™ *Version 9 Foundation Study Guide*, Van Haren Publishing, Zaltbommel.