View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by E-Journal Universitas Teknokrat Indonesia

Jurnal TEKNOINFO, Vol. 12, No.1, 2018, 16-22. ISSN 1693-0010 (print)

AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN *FRAMEWORK* COBIT 5 (STUDI KASUS: BALAI BESAR PERIKANAN BUDIDAYA LAUT LAMPUNG)

Ryan Randy Suryono [1)], Dedi Darwis [2)], Surya Indra Gunawan [3)]

[1),3)]Prodi S1 Sistem Informasi, Universitas Teknokrat Indonesia
[2)] Prodi D3 Sistem Informasi, Universitas Teknokrat Indonesia
Jl. H. Z. A. Pagaralam, No 9-11, Labuhanratu, Bandarlampung
Email : ryan.dataku@gmail.com [1)], darwisdedi@teknokrat.ac.id [2)], suryaindra326@gmail.com [3)]

Abstrak

Balai Besar Pengembangan Budidaya Laut Lampung (BBPBL) adalah Unit Pelaksana Teknis (UPT) di bidang pengembangan budidaya laut yang berada di bawah dan bertanggungjawab kepada Direktorat Jendral Perikanan Budidaya. Balai Besar Pengembangan Budidaya Laut Lampung merupakan telah menggunakan sistem e-SKP (elektronik Sasaran Kinerja Pegawai). Saat ini kegiatan tata kelola keamanan informasi belum dilakukan secara maksimal. Untuk mengantisipasi terjadinya kendala seperti sumber daya manusia yang kurang memahami aplikasi e-SKP sehingga berpotensi terjadinya error pada aplikasi, maka dilakukan metode pengelolaan teknologi informasi menggunakan kerangka kerja COBIT. Proses yang digunakan dalam penelitian ini adalah EDM03, APO13, APO12, BAI06, DSS01, DSS02, DSS03, DSS05, MEA01, MEA02. Analisis data menggunakan Maturity Level dan Analisis Kesenjangan untuk menentukan tingkat kematangan. Dari hasil nilai aktual dan nilai ekspektasi yang ditentukan, penulis mendapatkan gap dari analisis kesenjangan di atas.

Kata kunci : *Tata Kelola Keamanan Informasi, Maturity Level, Analisis Kesenjangan, e-SKP, COBIT 5*

1. PENDAHULUAN

A. Latar Belakang

Dengan semakin berkembangnya teknologi, khususnya teknologi informasi dan komputer, maka banyak perusahaan yang mengadopsi sistem informasi berbasis komputer sebagai bagian penting dari kelancaran kegiatan operasi perusahaan tidak terkecuali pemerintahan. Balai Besar Perikanan Budidaya Laut Lampung merupakan salah satu balai yang telah menerapkan teknologi informasi (*TI*) dalam bidang Sasaran Kinerja Pegawai (SKP) yaitu dengan menggunakan sistem e-SKP (elektronik Sasaran Kinerja Pegawai). Saat ini kegiatan tata kelola keamanan informasi belum dilakukan secara maksimal. Untuk mengantisipasi terjadinya kendala seperti sumber daya manusia yang kurang memahami aplikasi e-SKP sehingga berpotensi terjadinya *error* pada aplikasi, kemudian e-SKP masih menghadapi persoalan berkaitan dengan sering terjadi kehilangan data e-SKP dan belum ada solusi terkait masalah kehilangan data tersebut, maka perlu adanya audit tata kelola keamanan informasi untuk peningkatan keamanan data dan informasi pada Balai Besar Perikanan Budidaya Laut Lampung khususnya pada sistem e-SKP.

Dalam bidang tata kelola teknologi informasi, terdapat sebuah kerangka kerja COBIT untuk mengukur kematangan pemanfaatan IT di sebuah organisasi. Kerangka COBIT 5 membagi proses teknologi informasi menjadi 5 domain, yaitu EDM (*Evaluate, Direct and Monitor*), APO (*Align, Plan and Organise*), BAI (*Build, Acquire and Implement*), DSS (*Deliver, Service, and Support*), MEA (*Monitor, Evaluate and Assess*) dengan keseluruhan 37 proses yang ada didalamnya. COBIT berfungsi untuk mempertemukan semua kebutuhan control dan isu-isu teknik, selain itu COBIT juga dirancang menjadi alat bantu untuk memecahkan permasalahan pada IT *Governance* dalam memahami dan mengelola resiko serta keuntungan yang berhubungan dengan sumber daya informasi.[14]. Dengan dilakukannya audit tata kelola keamanan informasi menggunakan *framework* COBIT 5 akan memberikan informasi kepada Balai Besar Perikanan Budidaya Laut Lampung mengenai hasil analisis yang akan digunakan untuk melakukan peningkatan terhadap sistem e-SKP (*Elektronik Sasaran Kinerja Pegawai*).

Tujuan penelitian ini adalah untuk mengaudit keamanan informasi pada sistem e-SKP dengan menggunakan *framework* COBIT 5 dengan domain *Evaluate Direct and Monitor* (EDM), *Align Plan and Organise* (APO), *Build Acquire and Implement* (BAI), *Deliver Service and Support* (DSS), dan *Monitor Evaluate and Assure* (MEA) guna mengetahui tingkat keamanan informasi pada sistem e-SKP di Balai Besar Perikanan Budidaya Laut Lampung. Selain itu dilakukan pengujian terhadap sistem menggunakan aplikasi Nessus Scanner dan Apache Jmeter.

B. Landasan Teori

1. Definisi Audit

Audit pada dasarnya adalah proses sistematis dan obyektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan ekonomi, guna memberikan asersi/pernyataan dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kriteria yang berlaku dan mengkomunikasikan hasilnya kepada pihak terkait[10].

2. Tata Kelola Teknologi Informasi (TI)

Tata kelola TI adalah :

"Tata kelola TI sebagai tanggungjawab eksekutif dan dewan direksi, sebagai bagian dari tata kelola bisnis terdiri atas kepemimpinan, struktur dan proses-proses organisasi, yang akan memastikan bahwa TI organisasi tersebut bisa mendukung dan menyampaikan tujuan strategis organisasi". [10] Pentingnya Tata Kelola Teknologi yaitu :

1. Adanya perubahan peran TI, dari peran efisiensi ke peran strategic yang harus ditangani level korporat.
2. Banyak proyek TI strategic yang penting namun gagal dalam pelaksanaanya karena hanya ditangani oleh teknisi TI.
3. Keputusan TI di dewan direksi sering bersifat ad hoc atau tidak terencana dengan baik.
4. TI merupakan pendorong utama proses transformasi bisnis yang member imbas penting bagi organisasi dalam pencapaian misi, visi, dan tujuan strategic.
5. Kesukaan pelaksanaan TI harus dapat terukur melalui metric tata kelola TI.

3. Tata Kelola Teknologi Informasi dan Manajemen Teknologi Informasi

Tata Kelola Teknologi Informasi dan Manajemen Teknologi Informasi [14] memastikan bahwa tujuan perusahaan tercapai dengan mengevaluasi pemangku kepentingan, kebutuhan, kondisi dan pilihan. Menetapkan arah memalui prioritas dan pengambilan keputusan, pemantauan kinerja, kepatuhan dan kemajuan terhadap arah dan tujuan.

Salah satu kunci fokus tata kelola teknologi informasi [15] adalah untuk menyelaraskan teknologi informasi dengan tujuan bisnis. Sebagai penjelasan dapat dikatakan bahwa tata kelola teknologi informasi adalah perpaduan antara tata keloa perusahaan dan manajemen teknologi informasi.

4. COBIT 5

COBIT 5 (*Control Objektives For Information and Related Technology*) merupakan generasi terbaru dari panduan ISACA dibuat berdasarkan pengalaman penggunaan COBIT selama lebih dari 15 tahun oleh banyak perusahaan dan penggunaan dari bidang bisnis, komunitas, *IT*, risiko, asuransi, dan keamanan[14]. COBIT 5 mendefinisikan dan menjelaskan secara rinci sejumlah tata kelola dan manajemen proses. COBIT 5 menyediakan kerangka kerja yang komprehensif yang membantu perusahaan dalam mencapai tujuan mereka untuk tata kelola dan manajemen aset informasi perusahaan dan teknologi (*IT*). Secara sederhana, membantu perusahaan menciptakan nilai yang optimal dari *IT* dengan menjaga keseimbangan antara mewujudkan manfaat dan mengoptimalkan tingkat resiko dan penggunaan sumber daya. COBIT 5 menggunakan praktik tata kelola dan manajemen untuk menjelaskan tindakan praktik yang baik untuk efek tata kelola dan manajemen lebih perusahaan *IT*. COBIT 5 tidak dimaksudkan untuk menggantikan salah satu kerangka kerja atau standar lainnya, tetapi untuk menekankan tata kelola dan manajemen serta mengintegrasikan praktik pengelolaan terbaik pada perusahaan [14]. COBIT 5, memiliki kriteria informasi asli yaitu : Efisiensi, Efektivitas, Kerahasiaan, Integritas, Ketersediaan, Kepatuhan, dan Kehandalan.

5. Prinsip Dasar COBIT 5

COBIT 5 (*Control Objectivies Information and Related Technology*) secara umum memiliki 5 prinsip dasar yaitu [1]:

a. Meeting Stakeholder Needs

Terdapat usaha dari perusahaan untuk menciptakan nilai bagi para *stakeholder* dengan menjaga keseimbangan antara realisasi manfaat, optimalisasi risiko, dan penggunaan sumber daya.

b. Convering the Enterprise End-to-End

Bermanfaat untuk menintegrasikan tata kelola TI perusahaan kedalam tata kelola perusahaan. Sistem tata keloa TI yang digunakan COBIT 5 dapat menyatu dengan sistem tata kelola perusahaan dengan lancar. Prinsip kedua ini dibutuhkan untuk mengatur dan mengelola TI perusahaan dimanapun informasi diproses, baik layanan TI internal maupun eksternal.

c. Applying a Single Integrated Framework

Terdapat banyak standar yang berkaitan dengan IT, masing-masing memberikan panduan pada subset dari kegiatan IT. COBIT 5 sejalan dengan standar lain yang relevan dan kerangka pada tingkat tinggi. Dengan demikian, COBIT 5 dapat menjadi kerangka menyeluruh untuk tata kelola dan manajemen perusahaan.

d. Enalbling a Holistic Approach

Tata kelola dan manajemen perusahaan yang efektif dan efisien membutuhkan pendekatan holistic, dengan mempertimbangkan beberapa komponen yang saling berinteraksi.

e. Separating Governance From Management

COBIT membuat perbedaan yang cukup jelas antara tata kelola dan manajemen. Kedua hal tersebut mencakup berbagai kegiatan yang berbeda, memerlukan struktur organisasi yang berbeda, dan melayani untuk tujuan berbeda pula.

6. Domain COBIT 5

COBIT 5 *framework* dirancang dengan 5 domain yang masing-masing mencakup penjelasan rinci dan termasuk panduan secara luas dan bertujuan sebagai tata kelola dan manajemen TI perusahaan. Lima domain yang ada pad COBIT 5 adalah [14]:

a. EDM *(Evaluate, Direct and Monitor)*
b. APO *(Align, Plan and Organise)*
c. BAI *(Build, Acquire and Implement)*
d. DSS *(Deliver, Service, and Support)*
e. MEA *(Monitor, Evaluate and Assess)*

7. Pengukuran Tingkat Kematangan (*Maturity Level)*

Salah satu alat pengukur dari kinerja suatu sistem teknologi informasi adalah model kematangan (*maturity level*), model kematangan digunakan untuk mengontrol proses-proses teknologi informasi menggunakan *framework* COBIT dengan informasi menggunakan metode penilaian /*scoring* tujuannya adalah organisasi dapat mengetahui posisi kematangan teknologi informasi saat ini dan organisasi dapat terus menerus berkesinambungan berusaha meningkatkan *level*nya sampai tingkat tertinggi agar aspek *governance* terhadap teknologi informasi dapat berjalan dengan lancar. [14]

8. Audit *Software*

Audit *Softrware* merupakan jenis *software review* dimana satu atau lebih auditor yang bukan anggota dari pengembang perangkat, di luar organisasi yang melakukan pemeriksaan inependen dari produk perangkat lunak, proses *software* untuk menilai sesuai dengan spesifikasi, standar, perjanjian kontrak atau kriteria lainnya. Tujuan audit software adalah untuk memberikan evaluasi independen dari kesesuaian produk perangkat lunak dan proses ketentuan yang berlaku, standar, pedoman, dan rencana. Prinsip audit software adalah sebagai berikut :

a. Ketepatan waktu
b. *Open Source reflection*
c. *Bibliography*
d. *Referencing Innovations*
e. *Analysis of document*
f. *Scientific referencing and Learning*
g. *Continuous Review*
h. *Elaboration*

9. Apache Jmeter

Apahe Jmeter adalah sebuah perangkat lunak *open source*, aplikasi java murni yang dirancang untuk memuat prilaku fungsional tes dan menukur kinerja dan mengukur kinerja. Apache Jmeter pada awalnya dirancang untuk menguji aplikasi web tetapi sekaran sudah dipeluas untuk menguji fungsional lainnya. Secara umum Apache JMeter adalah sebuah *tools* yang memiliki fungsi sebagai berikut [17]:

a. Sebuah *Tool* atau alat yang digunakan untuk melakukan *performace test* pada sebuah software.
b. Apache JMeter dapat memberikan request dalam jumlah yang sangat banyak secara bersamaan dalam satu waktu pada server
c. Apache JMeter dapat memberikan analisa dan Laporan dari hasil pengujian
d. Berikut ini adalah requirement yang dibutuhkan untuk menjalankan Apache JMeter, yaitu :
e. JRE (*Java Runtime Enviroment*) >= 1.6
f. *Operating Systems* Unix (Solaris, Linux, etc), Windows (98, NT, XP, etc)

10. *Vulnerability scanner*

Vulnerability scanner adalah sebuah program komputer yang di desain untuk mencari dan memetakan system untuk kelemahan pada aplikasi, computer atau jaringan. Meningkatnya penggunaan internet membuat semakin banyaknya *website* yang bermunculan. Namun sangat disayangkan kejahatan internet terus meningkat seiring bermunculannya ragam artikel yang membahas masalah *hacking*. *Tools* yang digunakan untuk menganalisa kelemahan-kelemahan system adalah Nessus *scanner*. Nessus *scanner* merupakan kelompok *free scanner*. *Nessus* didistribusikan di bawah GNU *Public License* dari *Free Software Foundation*.

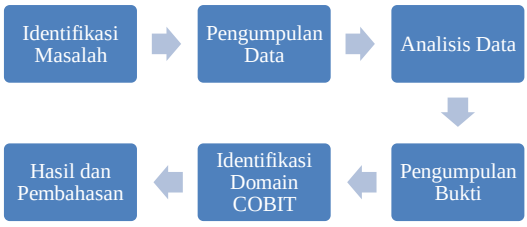
Nessus scanner merupakan *remote security* scanning tool yang digunakan untuk melakukan testing secara otomatis dalam masalah keamanan, khususnya untuk menemukan kerentanan-kerentanan yang memungkinkan seseorang hacker mendapakan akses pada suatu host yang terkoneksi dalam suatu jaringan [7] Kelebihan yang diberikan oleh *Nessus scanner* adalah :

a. *Intelligent Scannig*. Nessus tidak berasumsi bahwa *service* yang diberikan berjalan pada port yang tetap. Hal ini berarti jika menjalankan webserver pada port 1234 maka Nessus tetap akan mendeteksi dan menguji keamanannya secara tepat.
b. *Modular Architecture*. Arsitektur *client/server* menyediakan fleksibilitas sehingga Nessus dapat digunakan oleh banyak client melalui *web server*
c. *Complete reports*. Nessus tidak hanya akan memberitahukan kerentanan keamanan pada jaringan dan level resiko, tetapi juga menawarkan solusi untuk menagatasinya
d. *Full* SSL/TLS Support. Nessus juga mempunyai kemampuan untuk melakukan penguian dan *service* yang dijalankan melalui SSL seperti HTTPS, SMTPS, IMAPS dan lain sebagainya

2. METODE PENELITIAN

A. Tahapan Penelitian

Berikut tahapan penelitian yang digunakan, dapat dilihat pada gambar 1 berikut:



Gambar 1. *Tahapan Penelitian*

B. Identifikasi Masalah

Identifikasi masalah adalah tahapan selanjutnya setelah menentukan topik penelitian dari beberapa pilihan topik yang telah disediakan. Tahapan ini dilakukan untuk mendapatkan informasi mengenai permasalahan yang terjadi di Balai Besar Perikanan

Budidaya Laut Lampung terkait audit tata kelola sistem informasi.

C. Pengumpulan Data

Penelitian ini dilakukan melalui studi kasus di mana lokasi penelitian ini di Balai Besar Perikanan Budiday Laut Lampung. Studi ini mengukur kematangan mengendalikan proses teknologi informasi yang terjadi di lembaga-lembaga dalam rangka mencapai tujuan institusional didasarkan pada COBIT framework versi 5. Penelitian ini merupakan penelitian deskriptif, penelitian ini terdiri dari data primer dan sekunder. Data primer diperoleh dari wawancara dan sistem operator yang didasarkan pada instrumen penelitian dengan menggunakan kuisioner, survei dan observasi pada implementasikan teknologi informasi.

D. Analisis Data

Setelah dilakukan pengumpulan data, penulis melakukan analisis data. Analisis data yang dilakukan terdiri dari analsisi tingkat kematangan dan analsisi kesenjangan. Pengolahan dan dana analsisi hasil penelitian dilakukan dengan sistem komputerisasi *Microsoft Excel* 2010.

1. Analisis Tingkat Kematangan saat ini

Dari hasil jawaban kuisioner dan hasil wawancara dari narasumber pada instansi balai yang diperoleh saat melakukan analisis tersebut. Analisis yang dilakukan pada tahap ini adalah untuk menilai tingkat kematangan tata kelola teknologi informasi saat ini, akan tersedia jawaban dengan nilai 0-5.

2. Analisis Tingkat Kematangan yang diharapkan

Setelah melakukan analisis kematangan saat ini, penilis melakukan analisis tingkat kematangan yang diharapkan

3. Analisis Kesenjangan (*GAP*)

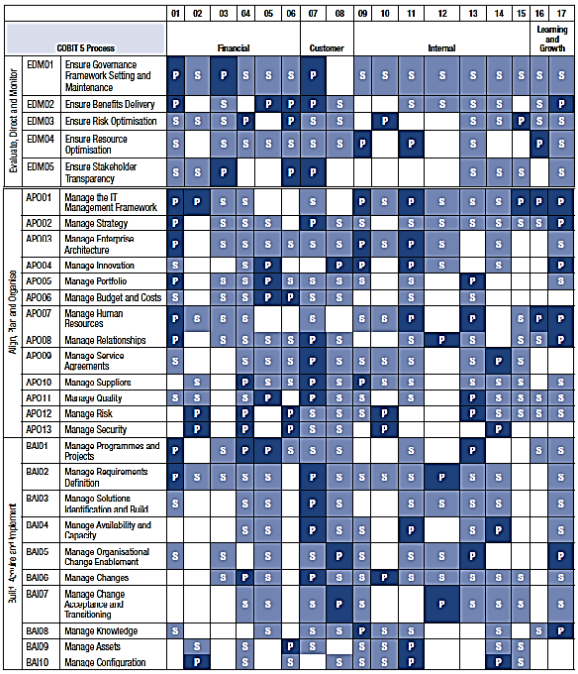
Setelah tingkat kematangan saat ini dan tingkat kematangan yang diharapkan diperoleh, penulis akan melakukan analisis kesenjangan terhadap tingkat kematangan tersebut.

4. Pengumpulan Bukti

Pada tahap ini peneliti melakukan pengumpulan bukti untuk menunjukkan adanya kekurangan di dalam sistem e-SKP, pengumpulan bukti ini dilakukan dengan bantuan *tools audit* yaitu Nessus 6.1 dan *tools testing* adalah Apache Jmeter. Tools Nessus berfungsi sebagai alata untuk mengaudit kerentanan sebuah sistem aplikasi berbasis website. Nessus memberikan secara detail kerentanan yang bisa terjadi di sebuah sistem dan memberikan solusi terhadap kerentanan tersebut. *Tools testing* Apache Jmeter merupakan merupakan kependekan dari *Web Application Load, Stress, and Performance Testing)* atau berarti aplikasi untuk melakukan test *load*, stress, dan performa pada sebuah alat aplikasi website. Hasil output berupa daftar table dan grafik yang menunjukkan tingkat peforma, tingkat stress, tingkat error dari sebuah aplikasi website.

5. Identifikasi Domain dan Proses COBIT 5

Berdasarkan *IT Related Goals* selanjutnya melakukan pemilihan terhadap 5 Domain dan 37 Proses COBIT 5 berdasarkan matriks berikut ini:



Gambar 2. *Matrik Domain COBIT 5 dan IT Related Goals*

Dari matrik tersebut dapat disimpulkan domain dan proses COBIT 5 yang akan digunakan ialah:

Tabel 1. *Daftar Proses COBIT 5*

No	Domain	Keterangan
1	APO10	Mengelola Penyedia
2	APO12	Mengelola Risiko
3	APO13	Mengelola Keamanan
4	BAI01	Mengelola Program dan Proyek
5	BAI06	Mengelola Perubahan
6	DSS01	Mengelola Operasi
7	DSS02	Mengelola Permintaan Layanan dan Insiden
8	DSS03	Mengelola Masalah
9	DSS04	Mengelola Kelangsungan
10	DSS05	Mengelola Layanan Keamanan
11	DSS06	Mengelola Kendali Proses Bisnis
12	EDM03	Memastikan Optimasi Risiko
13	MEA01	Memantau, Melakukan Evaluasi dan Menilai Kinerja dan Kesesuaian
14	MEA02	Memantau, Melakukan Evaluasi dan Menilai Sistem dari Kendali Internal
15	MEA03	Memantau, Melakukan Evaluasi dan Menilai Kepatuhan dengan

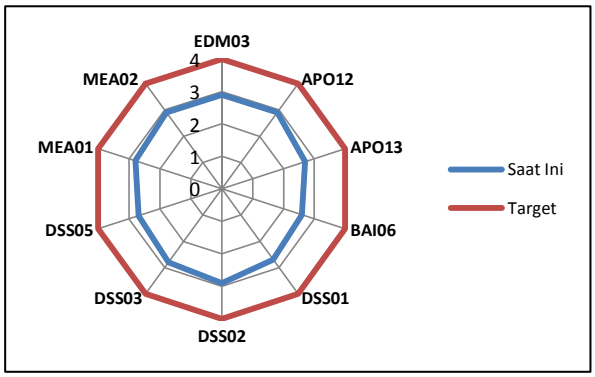
		Persyaratan Eksternal

3. HASIL DAN PEMBAHASAN

A. Analisis Kesenjangan

Tabel 2. *Analisis GAP*

Proses	Tingkat Kematangan		
	Saat Ini	Diharapkan	*GAP*
EDM03	2,9	4	4,0 – 2,9 = 1,1
APO12	2,9	4	4,0 – 2,9 = 1,1
APO13	2,7	4	4,0 – 2,7 = 1,3
BAI06	2,6	4	4,0 – 2,6 = 1,4
DSS01	2,7	4	4,0 – 2,7 = 1,3
DSS02	2,8	4	4,0 – 2,8 = 1,2
DSS03	2,8	4	4,0 – 2,8 = 1,2
DSS05	2,7	4	4,0 – 2,7 = 1,3
MEA01	2,8	4	4,0 – 2,8 = 1,2
MEA02	2,9	4	4,0 – 2,9 = 1,1
Rata-rata			**1,2**



Gambar 3. *Kesenjangan Masing-masing Proses*

Dari grafik diatas dapat dilihat kesenjangan dari masing-masing proses, kesimpulan dari *spider chart* diatas adalah kesepuluh proses COBIT 5 belum ada yang sesuai dengan target yaitu 4,0. dari sepuluh proses belum ada satu proses pun yang masuk kedalam kategori.

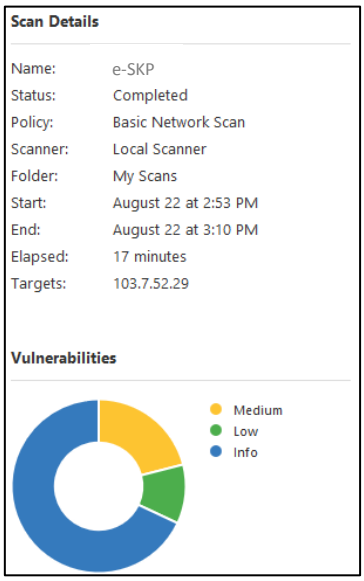
Hasil evaluasi menunjukan adanya permasalahan pada proses pengamanan sistem informasi terutama pada sistem e-SKP yaitu pada EDM03 masalah pada bagian ini adalah Balai Besar Perikanan Budidaya Laut Lampung belum secara rutin melakukan pembahasan mengenai permasalahan-permasalahan yang terjadi. Penanggulangan permasalahan hanya dilakukan dengan menunggu solusi dari pihak terkait seperti kementrian kelautan dan perikanan. Laporan permasalahan yang diterima oleh kepala balai hanya sebatas pelaporan permasalahan, bukan untuk pengembangan solusi. Untuk proses APO12 yaitu tidak ada perkiraan frekuensi kerugian yang berkaitan dengan risiko TI. Tidak ada pelaporan secara khusus ke bagian-bagian yang mengalami dampak dari permasalahan. Sedangkan untuk BAI06 yaitu Tidak melakukan pelaporan secara rinci terhadap permasalahan dan perubahan yang ada. Permasalahan pada APO13yaitu *User* e-SKP saat ini di pegang oleh dua, dua orang tersebut memiliki hak akses penuh terhadap sistem sistem e-SKP, permasalahan muncul ketika dua *user* tersebut akunnya dimiliki oleh semua pegawai. Ini yang menjadi permasalahan utama yang dihadapi oleh balai besar perikanan budidaya laut lampung karena dengan tersebarnya akun maka siapa saja dapat mengaakses dengan mudah dan dapat merusak, dan menghapus data e-SKP yang telah di inputkan oleh pegawai. Sedangkan untuk BAI06 yaitu Tidak melakukan pelaporan secara rinci terhadap permasalahan dan perubahan yang ada.

Permasalahan pada proses DSS01 Kurangnya perlindungan terhadap bencana alam maupun buatan manusia. Tidak ada prosedur khusus untuk melakukan pengecekan history.. Ruang server yang tidak ada batasan, sehingga banyak orang lain yang dapat mengakses server. Untuk DSS02 masalah yang muncul yaitu tidak melakukan pemeriksaan dengan pengguna untuk mengetahui apakah layanan telah memenuhi persyaratan untuk menyelesaikan permasalahan. DSS03 masalah yang dihadapi adalah Belum memantau dampak berkelanjutan dari masalah dan kesalahan yang dikenal pada layanan Dan pada DSS05 adalah Belum melakukan filter, seperti email dan download, untuk melindungi informasi yang tidak diminta (misalnya, spyware, phishing email). Tidak melakukan pelatihan berkala tentang malware di email dan internet penggunaan. Informasi tidak Encrypt hanya dilakukan penyimpanan di folder komputer. Tidak melaksanakan pengujian berkala dari sistem keamanan untuk menentukan kesiapan sistem. Tidak menetapkan prosedur untuk mengatur penerimaan, penggunaan, pemindahan dan pembuangan bentuk khusus dan perangkat output ke dalam, di dalam dan keluar dari perusahaan. Tidak menghancurkan informasi sensitif dan melindungi perangkat output.

Sedangkan untuk proses MEA01 masalah yang sering terjadi adalah tidak melakukan pelacakan terhadap permasalahan yang terjadi sehingga ketika masalah terulang perlu melakukan prosedure baru untuk menyelesaikan permasalahan. Dan untuk proses MEA02 adalah belum pernah melakukan audit baik itu secara internal maupun secara eksternal mengenai aplikasi e-SKP. Tidak ada kegiatan assurance dan memastikan kerja yang dilakukan selesai, memenuhi tujuan dan kualitas yang dapat diterima.

B. Pengujian *Vulnerability* terhdapat Sistem E-SKP

Hasil dari analisa *vulnerability* terhadap sistem e-SKP dapat diketahui beberapa kelemahan-kelemahan yang bisa menjadi pintu masuk bagi *attacker* untuk menguasai sistem e-SKP. Hasil yang ditunjukkan *Nessus Scanner* dapat diketahui terdapat 45 jenis kelemahan terdiri dari berbagai kategori yakni mediun dan info. Pada gambar 3 di bawah ini ditunjukkan hasil dari *Nessus Scanner*.



Gambar 4. *Detail Hasil Scanner Menggunakan Nessus*

Dari gambar 4 dapat diketahui jenis kelemahan dengan rincian sebagi berikut :

a. Kategori medium sebanyak 8 kelemahan
b. Kategori low sebanyak 4 kelemahan
c. Kategori info sebanyak 33 kelemahan

C. Hasil Pengujian sistem e-SKP menggunakan Apache Jmeter

Pengujian menggunakan Apache Jmeter terhadap sistem e-SKP. Apache Jmeter menguji sistem dengan cara menjalankan 50 *virtual user*. secara bertahap dengan jumlah perulangan 2 kali.

Dalam Test Ini didapat *throghput server* prestasikerja.kkp.go.id adalah 102.366/menit artinya server prestasikerja.kkp.go.id dapat menangani permintaan 102.366/menit. Deviasi prestasikerja.kkp.go.id adalah 3781 dibandingkan dengan devisasi server *google* yaitu (577) dengan nilai deviasi 3781 yang besar maka dapat disimpulkan peforma sistem e-SKP kurang baik dan perlu ditingkatkan kembali.

Hasil tersebut diperoleh dari 50 sampel user (Virtual) dengan rata-rata waktu respon yang dibutuhkan untuk mengakses sistem e-SKP adalah 797 ms, waktu respon yang paling cepat adalah 429 ms dan waktu respon paling lama adalah 5715 ms. Error yang ditemukan pada testing ini adalah 0%.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan maka dapat ditarik kesimpulan sebagai berikut:

1. Balai Besar Perikanan Budidaya Laut Lampung telah menerapkan proses pengamanan data dan informasi pada rata-rata level *Defined process.*
2. Hasil pengolahan kuesioner mendapati nilai rata-rata untuk domain MEA, APO, BAI, DSS, dan MEA adalah 2,8 dari rentang nilai 0 sampai 5. Balai Besar Perikanan Budidaya Laut Lampung telah melakukan proses pengamanan dan baku atau sudah mengikuti standar yang ada.
3. Hasil penelitian menemukan bahwa pada proses semua proses EDM03, APO12, APO13, BAI06, DSS01, DSS02, DSS03, DSS05, MEA01, MEA02. Ke sepuluh proses ini hanya mampu memperoleh nilai rata-rata 2,8 artinya masih pada level *Defined process*. Beberapa kelemahan yang paling fatal adalah belum memiliki prosedur yang baku dalam proses pengamanan data dan informasi, sehingga perlunya rekomendasi untuk mencapai tujuan yang diharapkan.
4. Hasil audit keamanan menggunakan aplikasi Nessus Scanner hasil yang didapat adalah pada aplikasi e-SKP terdapat kategori medium sebanyak 8 kelemahan, kategori low sebanyak 4 kelemahan, kategori info sebanyak 33 kelemahan. Hasil testing menggunakan aplikasi tester Apache Jmeter di dapat hasil sebagai berikut
   a. Peforma aplikasi hasilnya *throghput* adalah 102.366/menit dan Deviasi adalah 3781
   b. Respon Time sistem E-SKP adalah rata-rata 797 ms
5. Dengan hasil demikian aplikasi e-SKP perlu ditingkatkan dalam kemanan, *throghput* dan performa sehingga aplikasi dapat berjalan dengan maksimal, aman dan efisien.

5. DISKUSI

Dalam menjaga keamanan informasi dan perbaikan bagi Balai Besar Perikanan Budidaya Laut Lampung, maka terdapat saran bagi organisasi, yaitu:

1. Balai Besar Perikanan Budidaya Laut Lampung sebaiknya menerapkan rekomendasi-rekomendasi yang telah diberikan penulis untuk meningkatkan sistem keamanan terutama dalam pengamanan asset data dan informasi aplikasi e-SKP.
2. Mempersiapkan SDM yang memadai, melakukan pelatihan atau kursus mencakup bidang-bidang yang menggunakan teknologi informasi, memberikan pelatihan dalam pengelolaan risiko.
3. Mempersiapkan fasilitas yang memadai untuk pengamanan data seperti membuat ruang khusus, pembatasan hak akses ruangan, dan melakukan pemeriksaan secara rutin terhadap kemungkinan risiko-risiko yang muncul.
4. Melakukan penambahan *bandwidth* dan melakukan solusi-solusi yang direkomendasikan oleh aplikasi Nessus Scenner
5. Dilakukan pengauditan kembali dengan target nilai maturity sebesar 4 sehingga dapat memberikan rekomendasi untuk meningkatkan pengamanan data dan informasi pada Besar Perikanan Budidaya Laut Lampung

6. DAFTAR PUSTAKA

[1] Anggoro A D., 2014. *Analisis Kepatuhan Karyawan Terhadap Kebijakan Pengamanan Data pada PT XYZ dengan Standar COBIT 5*, Program Studi Teknik Informatika Universitas Bakrie, Jakarta.

[2] Handayaningsih S., 2013. *Perancangan Model Tata Kelola Teknologi Informasi Berbasis Cobit 4.1 pada Proses Mengelola Sumber Daya Manusia IT (Studi Kasus Bagian Pengelolaan Data Kab, Kendal),*Program Studi Teknik Informatika Universitas Ahmad Dahlan, Yoyakarta.

[3] Masykur Fauzan., 2015. *Analisis Vulnerability Web Based Application menggunakan Nessus*, Fakultas Teknik Universitas Purwokerto.

[4] Megawati.,2014. *Evaluasi Tingkat Kematangan Teknologi Informasi Dengan Menggunakan Model Maturity Level COBIT 4.1 di PT BRI Cabang Bangkinang*, Program Studi Sistem Informasi Universitas Islam Negeri Suska Riau Jalan HR. Soebrantas KM 115 Tampan Pekanbaru, Riau.

[5] Putra R., 2015. *Evaluasi Tata Kelola Teknologi Informasi Berbasis COBIT 5 dalam Pelayanan Sistem Informstasi Akademik di Universitas Pendidikan Ganesha*, Program Studi Magister Teknik Informatika Program Pascasarjana Universitas Atmajaya Yogyakarta, Yogyakarta.

[6] Rahmaani R A., 2014. *Audit Sistem Informasi Akademik UIN Sunan Kalijaga Yogyakarta Menggunakan COBIT Framework pada Domain Deliver and Support*, Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta, Yogyakarta.

[7] Ruslam Z R., 2013. *Audit Kepatuhan Keamanan Informasi Dengan Menggunakan Framework ISO 27001/ISMS* pada PT. XYZ, Universitas Indonesia, Fakultas Ilmu Komputer Program Studi Magister Teknologi Informasi, Jakarta.

[8] Sari S., 2014. *Penerapan framework Cobit 5 Pada Audit Tata Kelola Teknologi Informasi di Dinas Komunikasi dan Informatika Kabupaten OKU*, Universitas Bina Darma, alan A. Yani No. 12 Palembang, Sumatera Selatan.

[9] Sembiring W S., 2012. *Evaluasi Penerapan Teknologi Informasi Menggunakan Model COBIT Framework 4.1*, Program Studi Magister Teknik Informatika Program Pascasarjana Universitas Atma Jaya Yogyakarta, Yogyakarta.

[10] Syaroh S., 2011. *Audit Sistem Informasi Call Center Pada PT Arga Bangun Bangsa (ESQ Learship Center) dengan menggunakan framework COBIT*, Universitas Islam Negeri Syarif Hidayatullah Jakarta, Jakarta.

[11] Suharto A., 2014. *valuasi Tata Kelola Teknologi Informasi Dengan Framework COBIT 5 di Kementerian ESDM*, Program Studi Teknik Informatika Sekolah Tinggi Manajemen Infomatikadan Komputer Eresha, Jakarta.

[12] Suwarno R F., 2004. *Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus pada Proses Manage Relationship (APO08) Studi Kasus :PT OTO MULIARTHA*, Universitas Islam Negeri Syarif Hidayatullah Jakarta, Jakarta.

[13] Wardani S., 2014. *Audit Tata Kelola Teknologi nformasi Menggunakan Framework COBIT dengan Model Maturity Level (Studi Kasus Fakultas ABC).*

[14] ISACA 2012, *Kerangka COBIT 5, COBIT 4.1, BMI (Modeling Bussiness Information), Manajemen Tata Kelola, Jaminan Framework, Kerangka IT Risk*, Major ISACA.

[15] Romney, Steintbart., 2015. *Informasi Sistem Informasi*, Jakarta.

[16] Schiller M., 2011. The McGraw-Hill Compaines, *Audit TI menggunakan Kontrol untuk melindungi asset informasi*, Amerika Serikat.

[17] Apache Software Foundation. 2016. *Apache JMeter*. [online]. Tersedia : http://.apache.org/ [akses 14 oktober 2016]