ANALISIS KEAMANAN SISTEM INFORMASI PADA *EMAIL CORPORATE* UNIVERSITAS TEKNOLOGI SUMBAWA UNTUK IMPLEMENTASI SISTEM KERJA *PAPERLESS* (INOVASI *SMART CAMPUS*)

Ahmad Juliansyah[1], Houri Sobirin[2], Shinta Esabella[3]

*[1]Magister Manajemen Inovasi, Sekolah Pasca Sarjana Universitas Teknologi Sumbawa
[2]Magister Manajemen Inovasi, Sekolah Pasca Sarjana Universitas Teknologi Sumbawa
[3]Teknik Informatika,Fakultas Rekayasa Sistem Universitas Teknologi Sumbawa

*Corresponding Author email :[1]*ahmad.juliansyah@uts.ac.id*, [2]*houari.sabirin@uts.ac.id*, [3]*shinta.esabella@uts.ac.id*

Diterima :
Bulan September 2021

Diterbitkan :
Bulan Oktober 2021

Keyword :
Email Corporate[1],COBIT[1], Kemananan[1]

Abstrak

Universitas adalah satuan pendidikan yang berperan menyelenggarakan Pendidikan Tinggi dalam memajukan ilmu pengetahuan dan teknologi. Guna mewujudkan peran tersebut, Universitas harus memiliki pusat data yang memadai. penelitian ini bertujuan untuk menganalisa keamanan sistem informasi pada *email corporate*, guna menerapkan sistem kerja berbasis paperless di Universitas Teknologi Sumbawa, dalam mewujudkan inovasi Smart Campus oleh seluruh civitas akademika Universitas Teknologi Sumbawa. Penelitian ini menggunakan tipe penelitian deskriptif kualitatif. Dengan melakukan observasi langsung tentang audit keamanan sistem informasi menggunakan COBIT 4.1. Hasil dari penelitian berupa '*Term of Agreement*' pakta integritas aturan email korporat dan implementasi inovasi sistem kerja *paperless* universitas.

PENDAHULUAN

Universitas Teknologi Sumbawa (UTS) merupakan salah satu Perguruan Tinggi Swasta yang ada di Kabupaten Sumbawa, Provinsi Nusa Tenggara Barat. UTS berdiri sejak tanggal 13 Maret 2013 berdasarkan keputusan Menteri Pendidikan dan Kebudayaan Republik Indonesia No: 65/E/O/2013, berlokasi di Jalan Raya Olat Maras, Dusun Batu Alang, Desa Leseng, Kecamatan Moyo Hulu. Memiliki sarana teknologi informasi *data center* yang memadai, diantaranya *Google Suite* untuk *Email Corporate* , dengan spesifikasi *Google Drive Unlimited* & *Share Drive*.

Sarana teknologi informasi sangat memadai untuk mendukung sistem kerja yang efektif dan efisien, akan tetapi di Universitas Teknologi Sumbawa, *Google Suite* hanya digunakan sebagai formalitas *Email Corporate* kampus , dikarenakan terdapat fitur 'domain korporasi', seperti contoh: 'ahmad@uts.ac.id'. penerapan *paperless* belum sepenuhnya diimplementasikan, Kegiatan surat menyurat, masih dilakukan secara manual, seperti kertas yang dibagikan ke masing-masing unit atau melalui *platform messenger* "*WhatsApp*", begitu juga dengan berkas-berkas milik unit bersama, masih dikerjakan manual secara personal melalui perangkat masing-masing.

Masalah yang melatarbelakangi penggunaan tersebut adalah adanya rasa ragu dari setiap unit terhadap fasilitas keamanan sistem di *platform Email Corporate* kampus, dikarenakan pernah terjadi kehilangan data secara serentak di seluruh unit melalui serangan virus *ransomware* dan *blackmail* dengan media *email corporate*, dan juga masing-masing pengguna *email corporate* dapat dengan mudah meng *upload*, *download*, dan mengirim file dengan *extensi* asing "mencurigakan" menggunakan media tersebut. dikarenakan tidak adanya standar '*Term of Agreement*' untuk keamanan sistem pada *Email Corporate* Universitas Teknologi Sumbawa.

Solusi dan Inovasi yang ditawarkan pada penelitian ini adalah untuk Menganalisa keamanan sistem informasi pada *email corporate*, guna menerapkan sistem kerja berbasis *paperless* di .Universitas Teknologi Sumbawa, dalam mewujudkan inovasi *Smart Campus* oleh seluruh civitas akademika Universitas Teknologi Sumbawa.

LANDASAN TEORI

Keamanan sistem informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi resiko-resiko yang terjadi, mengoptimalkan pengembalian investasi (*return on investment*). Semakin banyak informasi perusahaan yang disimpan, dikelola dan diabaikan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau tereksposnya data ke pihak eksternal yang tidak diinginkan. (Sarno dan iffano : 2009).

Aspek yang penting dalam keamanan email adalah, kerahasiaan (*Confidentiality*), keaslian (*Authentication*), integritas (*Integrity*), anti penyangkalan (*Non-repudiation*) (Stallings, 2011). Surat elektronik atau email itu sendiri bagaikan surat

ISSN 2527-970X | E-ISSN 2621- 542x

konvensional, jalur yang dilalui dari pengirim ke penerima sangat panjang melalui beberapa kantor pos cabang, pusat dan dibawa oleh beberapa petugas pengirim surat. Email juga demikian, jalur yang dilalui dari pengirim ke penerima melalui beberapa router, mail servers, dan beberapa jaringan komputer. Email sangat rentan dengan serangan baik pasif maupun aktif.

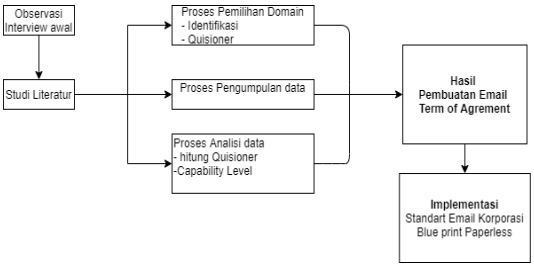
COBIT (*Control Objectives for Information and Related Technology*) adalah kerangka kerja tata kelola IT (*IT Governance Framework*) dan kumpulan perangkat yang mendukung dan memungkinkan para manager untuk menjembatani jarak (gap) yang ada antara kebutuhan yang dikendalikan (*control requirement*), masalah teknis (*technical issues*) dan resiko bisnis (*business risk*). COBIT mempermudah perkembangan peraturan yang jelas (*clear policy development*) dan praktik baik (*good practice*) untuk mengendalikan IT dalam organisasi. COBIT menekankan keputusan terhadap peraturan, membantu organisasi untuk meningkatkan nilai yang ingin dicapai dengan penggunaan IT, memungkinkan untuk menyelaraskan dan menyederhanakan penerapan dari kerangka COBIT. COBIT muncul pertama kali pada tahun 1996 yaitu COBIT versi 1 yang menekankan pada bidang audit, COBIT versi 2 pada tahun 1998 yang menekankan pada tahap control, COBIT versi 3 pada tahun 2000 yang berorientasi kepada manajemen, COBIT versi 4 yang lebih mengarah pada IT *Governance*, dan terakhir dirilis adalah COBIT versi 5 pada tahun 2012 yang mengarah pada tata kelola dan manajemen untuk aset-aset perusahaan IT. COBIT terdiri atas 4 domain, yaitu :

1) *Planning and Organizing*,
2) *Acquisition and Implementation*,
3) *Delivery and Support*,
4) *Monitoring and Evaluation*

Dalam COBIT mempunyai model kematangan (*maturity models*) untuk mengontrol proses-proses TI dengan menggunakan metode penilaian (*scoring*) sehingga suatu organisasi dapat menilai proses-proses TI yang dimilikinya dari skala nonexistent sampai dengan optimised (dari 0 sampai 5). 0 - Non Existent Perusahaan sama sekali tidak peduli akan pentingnya teknologi informasi untuk dikelola secara baik oleh pihak manajemen.

1. *Initial / Ad Hoc*
   Perusahaan secara reaktif melakukan penerapan dan implementasi teknologi informasi sesuai dengan kebutuhan-kebutuhan mendadak yang ada, tanpa didahului dengan perencanaan sebelumnya.
2. *Repeatable but Intuitive*
   Perusahaan telah memiliki pola yang berulang kali dilakukan dalam melakukan manajemen aktivitas terkait dengan tata kelola teknologi informasi, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidakkonsistenan.
3. *Defined*
   Perusahaan telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari.
4. *Managed and Measurable*
   Perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun objektif kinerja setiap penerapan aplikasi teknologi informasi yang ada
5. *Optimised*
   Perusahaan telah mengimplementasikan tata kelola teknologi informasi yang mengacu pada "*Best Practice*".

Kerangka pemikiran merupakan suatu uraian atau pernyataan tentang kerangka konsep pemecahan masalah yang telah diidentifikasi atau dirumuskan untuk mendapatkan sebuah kesimpulan berupa hipotesis. Dari teori yang telah dibahas diatas, maka dapat penulis menyimpulkan suatu kerangka pemikiran seperti berikut.



Gambar 2.1 Kerangka Pikir

Hipotesis adalah jawaban sementara terhadap masalah yang masih bersifat praduga karena harus dibuktikan kebenarannya. Hipotesis adalah pernyataan yang diterima secara sementara sebagai suatu kebenaran sebagaimana adanya, pada saat fenomena dikenal dan merupakan dasar kerja serta panduan dalam verifikasi. Terdapat beberapa hipotesis pada penelitian ini, antara lain:

a. Ketersediaan Pakta Integritas keamanan pengguna email korporasi kampus
b. Ketersediaan Standar skema penggunaan data melalui platform email korporasi

MATODE PENELITIAN

Desain Penelitian

Penelitian ini menggunakan tipe penelitian deskriptif kualitatif. Sifat dari penelitian ini adalah deskriptif, metode deskriptif digunakan sebagai prosedur memecahkan masalah yang diselidiki, dengan menggambarkan keadaan subyek atau obyek penelitian berdasarkan fakta yang terlihat. Data yang dikumpulkan berupa tulisan, gambar, dan bukan

ISSN 2527-970X | E-ISSN 2621- 542x

angka. Data tersebut berasal dari wawancara, catatan, observasi lapangan, foto, video, dokumen pribadi, dan dokumen resmi universitas.
Penelitian deskriptif ditujukan untuk :

1. Mengumpulkan informasi secara terperinci dan aktual tentang *email corporate*
2. Mengidentifikasikan masalah di UTS.
3. Membuat perbandingan atau evaluasi berdasarkan COBIT 4.1.
4. Menentukan yang akan dilakukan pengguna isistem lain, dalam menghadapi *problem solving* yang sama dan belajar dari pengalaman untuk menetapkan rencana serta keputusan di waktu yang akan datang.

Skala Pengukuran

Skala pengukuran yang akan dipakai dalam kuesioner pada penelitian ini adalah skala *maturity* yang mampu mengukur level pengembangan manajemen proses sistem informasi *email corporate* universitas. Seberapa bagus pengembangan sistem informasi atau kapabilitas manajemen sistem tergantung tercapainya tujuan COBIT. Jawaban setiap item instrumen yang menggunakan skala *maturity* berbentuk sebuah tanggapan responden terhadap pernyataan dalam kuesioner, adapun jawaban tersebut yaitu: *Optimized* (sempurna, TI berjalan dengan baik), *Managed and measurable* (dilakukan, ada proses), *Defined process* (dilakukan dan sudah baku), *Repeatable but intuitive* (dilakukan, tetapi belum baku), I*nitial / ad-hoc* (dilakukan, tetapi tidak ada prosedur), *Non-existent* (tidak ada proses TI). Penggunaan dari skala ini ditujukan untuk mengevaluasi kinerja yang paling relevan di bawah keadaan tertentu dalam universitas. Tujuannya untuk menguraikan secara efektif faktor yang penting bagi sistem informasi universitas teknologi sumbawa

Tabel 3.1 Skala Penilaian *Maturity*

Skor	Tingkatan	Keterangan
5	*Optimized*	Sempurna, TI berjalan dengan baik
4	*Managed & Measureable*	dilakukan, ada proses
3	*Defined Process*	dilakukan, dan sudah baku
2	*Repeatable but intuitive*	dilakukan, tetapi belum baku
1	*Initial*	dilakukan, tetapi tidak ada prosedure
0	*Non-Existent*	tidak ada proses TI

Tabel 3.2 Rentang Skala *Maturity*

Skor	Tingkatan
4,51 s/d 5,00	*Optimized*
3,51 s/d 4,50	*Managed & Measureable*
2,51 s/d 3,50	*Defined Process*
1,51 s/d 2,50	*Repeatable but intuitive*
0,51 s/d 1,50	*Initial*
0,00 s/d 0,50	*Non-Existent*

Sample dan Populasi

Untuk mendapatkan sebuah sampel yang dapat menggambarkan populasi pada penelitian ini, maka teknik sampling jenuh (sensus) sangat tepat digunakan dalam penentuan sampel bila semua anggota populasi digunakan sebagai sampel. Hal dilakukan apabila jumlah populasi relatif kecil atau kurang dari 30 orang agar penelitian dapat membuat generalisasi dengan kesalahan yang sangat kecil.

Populasi yang digunakan sebagai sampel data pada penelitian ini adalah pegawai yang memiliki otoritas memimpin serta berpotensi membentuk sistem kerja pada masing-masing divisinya di Universitas Teknologi Sumbawa yang berjumlah 12 orang, diantaranya terdapat warek, direktur, dekan dan kaprodi.

Metode Pengumpulan Data

Untuk mendapatkan data dan informasi untuk mendukung penelitian, maka metode yang akan digunakan dalam proses pengumpulan data adalah sebagai berikut :

1. Observasi

Dalam hal ini yang akan di observasi tentang audit keamanan sistem informasi pada *email corporate* di Universitas Teknologi Sumbawa menggunakan COBIT 4.1.

2. Studi Pustaka

Adalah metode yang dilakukan dengan cara mencari bahan yang mendukung dalam pendefinisian masalah melalui buku, internet, yang berkaitan dengan objek permasalahan.

3. Wawancara

Dengan melakukan tanya jawab langsung dengan pegawai yang dipilih oleh peneliti di Universitas Teknologi Sumbawa menggunakan COBIT 4.1.

4. Quesioner

Pada metode ini kegiatan yang dilakukan adalah membuat beberapa pertanyaan berdasarkan framework COBIT 4.1 untuk melakukan audit keamanan sistem informasi pada email corporate di Universitas Teknologi Sumbawa.

Tahapan Pelaksanaan Audit

Adapun Tahapan audit keamanan teknologi informasi *email corporate* Universitas Teknologi Sumbawa meliputi:

1. Analisis Kondisi

ISSN 2527-970X | E-ISSN 2621- 542x

Tahapan analisis kondisi Audit Sistem Informasi dan Teknologi Informasi merupakan kegiatan meninjau kondisi kampus saat ini, terutama yang berkaitan dengan proses bisnis teknologi informasi pada *email corporate.*

2. Penentuan Tingkat Resiko

Adalah Tahapan pengklasifikasian bisnis proses yang tingkat resikonya tinggi (proses bisnis utama) maupun proses bisnis pendukung pada *email corporate.*.

3. Pelaksanaan Audit Sistem Informasi

Tahapan pelaksanaan audit mengacu kerangka kerja COBIT 4.1 dengan proses penentuan ruang lingkup serta tujuan audit berdasarkan hasil penentuan tingkat resiko pada pada *email corporate* di tahapan sebelumnya.

4. Penentuan Rekomendasi

Tahapan selanjutnya adalah pengkomunikasian hasil audit pada *email corporate* kepada pihak manajemen terkait. Alur tersebut menghasilkan kesepakatan dari hasil audit yang kemudian akan disusun dalam bentuk laporan audit.

Tahapan Implementasi

Tahapan implementasi keamanan sistem informasi email korporat Universitas Teknologi Sumbawa meliputi:

1. Pembuatan Dokumen Pakta Integritas '*Term of Agreement*'

Tahapan lebih mengacu pada pembuatan dokumen dari pernyataan atau janji kepada diri sendiri tentang komitmen penggunaan email korporasi dan peran sesuai dengan peraturan perundang-undangan serta kesanggupan untuk tidak menyalahgunakan fasilitas.

2. Implementasi Sistem kerja *'paperless'*

Setelah pembuatan '*Term of Agreement'* dilaksanakan, langkah selanjutnya adalah implementasi inovasi sistem kerja berbasis paperless, melalui media email korporasi, dengan merancang level email korporasi masing-masing unit, dan manajemen pengelolaan penyimpanan data serta akses penyimpanan bersama pada setiap unit di universitas teknologi sumbawa.

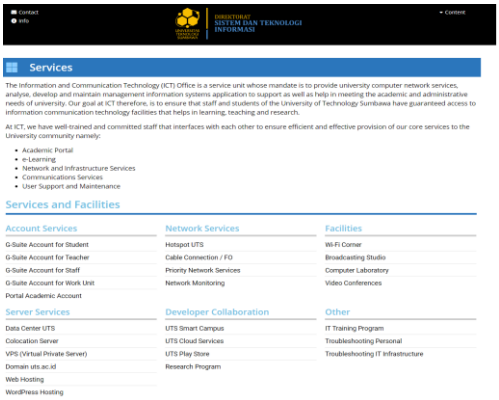
HASIL DAN PEMBAHASAN

Analisis Kondisi

Tahapan analisis kondisi dalam rencana audit keamanan sistem informasi pada Email korporat di Universitas Teknologi Sumbawa yang merupakan lembaga pendidikan ilmu pengetahuan dan teknologi, sampai dengan tahun 2021, telah dilakukan pembangunan ataupun pengembangan Sistem Informasi, baik itu menyangkut piranti lunak, dan piranti keras dan infrastruktur jaringan.

1. Standar

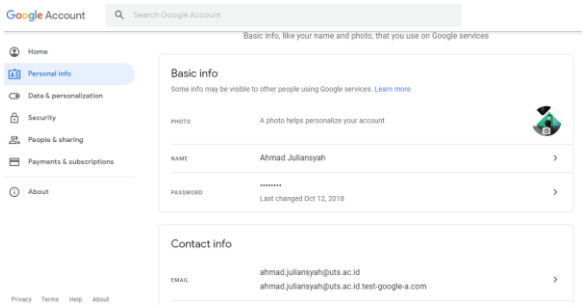
Untuk mensinergikan implementasi dan penerapan sistem informasi, Universitas Teknologi Sumbawa telah mempunyai arah pembangunan atau pengembangan sistem yang tercantum di dalamnya master plan Direktorat Sistem dan Teknologi Informasi (DSTI), dan integrasi satu pintu media email korporat universitas.



Gambar 4.1 *Service* DSTI

2. *Email Corporate* UTS

Untuk mensinergikan implementasi dan penerapan sistem informasi, Universitas Teknologi Sumbawa telah mempunyai arah pembangunan atau pengembangan sistem yang tercantum di dalamnya master plan Direktorat Sistem dan Teknologi Informasi (DSTI), dan integrasi satu pintu media email korporat universitas.



Gambar 4.2 *Email Corporate*

Penentuan Tingkat Resiko

Berdasarkan tahapan analisis kondisi yang telah dilakukan, maka penentuan tingkat resiko pada perangkat lunak terutama *email corporate*, agar tidak terjadi kendala yang serius ketika sistem yang ingin diterapkan, tidak berjalan semestinya seperti hacker atau *anonymous* (pihak yang tidak bertanggung jawab) ingin memasuki sistem tanpa mempunyai akses.

Perangkat keras menggunakan spesifikasi komputer standar dengan server *broadcast* yang diperuntukkan untuk monitoring jaringan internet dan *streaming* kegiatan seminar, belum adanya spesifikasi komputer untuk server pengelola administrator data penyimpanan dan *email corporate*. Infrastruktur jaringan internet telah diimplementasikan dan mampu mengakomodir seluruh area kampus, belum adanya tenaga ahli

ISSN 2527-970X | E-ISSN 2621- 542x

khusus untuk mengelolah sistem informasi *email corporate* yang ada di Universitas Teknologi Sumbawa.

Hasil Pelaksanaan Audit

Hasil dari pembahasan audit keamanan pada sistem informasi pada *email corporate* menggunakan Cobit 4.1. (*control objective for information and related technology*) di Universitas Teknologi Sumbawa. Kebutuhan untuk menjaga integritas informasi dan melindungi aset sistem informasi memerlukan proses manajemen keamanan. Proses ini meliputi penyusunan serta memelihara peranan keamanan (*security rules*) dan tanggung jawab, kebijakan, standar serta prosedur.

Adapun keberadaan tingkat keterkaitan langsung dalam upaya pengendalian terhadap kerentanan yang dapat memicu timbulnya ancaman yang berdampak serius terhadap pencapaian tujuan proses bisnis menggunakan. DS5 (*ensure system security*), dengan pertanyaan yang terdiri dari :

1). DS5.1 : Manajemen Keamanan TI (*Management Of IT Security*)

Manajemen keamanan sistem informasi pada level organisasi tertinggi sehingga tindakan manajemen keamanan selaras dengan kebutuhan bisnis. Menerjemahkan bisnis, risiko dan kepatuhan, ke dalam rencana keamanan sistem informasi secara keseluruhan dengan mempertimbangkan infrastruktur dan budaya keamanan.

2). DS5.2: Rencana Keamanan TI (*IT Security Plan*)

Memastikan rencana dapat diterapkan dalam bentuk prosedur serta kebijakan keamanan bersama investasi yang tepat dalam layanan, personil, *hardware* dan *software*. Mengkomunikasikan kebijakan dan prosedur keamanan kepada user.

3). DS5.3 : Manajemen Identitas (*Identity Management*)

Memastikan semua pengguna (*user*) dan aktivitas mereka dalam sistem informasi secara unik teridentifikasi. Memudahkan pengguna (*user*) dalam mengidentifikasi melalui mekanisme otentikasi. Konfirmasi setiap hak akses pengguna ke sistem informasi sesuai dengan yang ditetapkan, kebutuhan bisnis, dan kebutuhan kerja yang melekat pada identitas pengguna. Memastikan bahwa hak akses pengguna (*user*), disetujui oleh pemilik operator sistem dan diimplementasikan oleh penanggung jawab.

4). DS5.4: Manajemen Akun Pengguna (*User Account Management*)

Menempatkan permintaan, penyusunan, penerbitan, penangguhan. Modifikasi (*custom*) dan penutupan akun pengguna serta hak akses yang berkaitan dengan rangkaian prosedur manajemen akun pengguna. Termasuk prosedur persetujuan yang menguraikan (editor) data atau pembagian hak akses. Prosedur ini harus berlaku untuk semua pengguna termasuk administrator, pengguna internal.

5). DS5.5: Penjagaan, Pemantauan dan Uji Coba Keamanan (*Surveillance monitoring and Security Testing,*)

Menguji, menjaga dan memantau implementasi keamanan sistem informasi dalam langkah yang proaktif. Keamanan seharusnya ditinjau secara berkala untuk memastikan landasan keamanan informasi organisasi yang disetujui dan dipelihara. *Login* serta fungsi pemantauan keamanan sistem informasi akan memudahkan dalam pencegahan, pendeteksian dini dan untuk melaporkan aktivitas yang tidak seperti biasanya perlu diperhatikan.

6). DS5.6: Definisi Insiden Keamanan (*Security Incident Definition*)

Mendefinisikan serta mengkomunikasikan karakteristik dari insiden keamanan yang berpotensi, sehingga dapat diklasifikasi dan diperlakukan dengan baik oleh peristiwa dan proses manajemen masalah.

7). DS5.7: Proteksi Teknologi Keamanan (*Protection of Security Technology*)

Membuat teknologi keamanan sistem informasi yang tahan terhadap gangguan, serta tidak mengungkapkan dokumentasi keamanan yang tidak perlu.

8). DS5.8: Manajemen Kunci Kriptografi (*Cryptographic Key Management*)

Menentukan kebijakan dan prosedur telah sesuai untuk mengatur perubahan, pembatalan, penghancuran, distribusi, sertifikasi, penyimpanan, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan *decrypter* yang tidak sah.

9). DS5.9: Pencegahan Aplikasi Berbahaya, Deteksi dan Perbaikan (*Malicious Software Prevention, Detection and Correction*)

Memasang pendeteksi, pencegahan dan langkah-langkah perbaikan yang sesuai (terutama patch keamanan yang *up-to-date* dan pengendalian virus) di seluruh organisasi untuk melindungi sistem informasi dan teknologi dari malware (seperti virus, worm, spyware dan spam).

10). DS5.10 Keamanan Jaringan (*Network Security*)

Menggunakan teknik serta prosedur manajemen keamanan seperti firewall, peralatan keamanan, segmentasi jaringan, instruksi deteksi, untuk otorisasi akses serta kontrol informasi mengalir dari dan ke jaringan.

10) DS5.11: Pertukaran Data Sensitif (*Exchange of Sensitive Data*)

Transaksi pertukaran data sensitif yang melalui jalur terpercaya dan media dengan kontrol untuk menyediakan keaslian konten, bukti pengiriman dan bukti penerimaan.

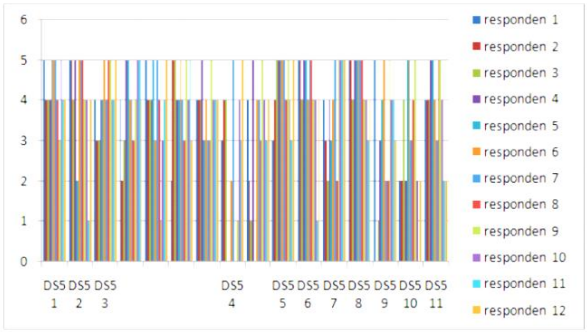
Berikut hasil wawancara berupa kuesioner untuk domain DS5 (*ensure system security*), yang telah disebarkan kepada pegawai yang memiliki otoritas terhadap sistem kerja pada masing - masing unitnya, yang berjumlah 12 orang pimpinan terdiri

ISSN 2527-970X | E-ISSN 2621- 542x

dari warek, dekan, direktorat, prodi pada Universitas Teknologi Sumbawa yaitu :

Tabel 4.1 DS5 *(Ensure System Security)*

Pertanyaan DS5	Responden												Rata - Rata	Rata - rata perproses
	1	2	3	4	5	6	7	8	9	10	11	12		
DS5 1	5	4	4	4	5	5	5	4	3	5	4	4	4,33	3,84
DS5 2	5	5	4	5	2	5	5	5	4	4	1	4	4,08	
DS5 3	4	3	3	4	4	5	4	5	5	4	4	5	4,17	
	4	2	3	5	5	4	4	3	4	5	5	4	4,00	
	5	4	4	4	5	3	5	4	1	3	4	5	3,92	
	2	5	5	4	4	5	4	3	5	4	5	3	4,08	
	4	4	4	5	3	4	3	3	5	4	4	4	3,92	
DS5 4	3	4	4	0	0	2	5	0	1	4	3	5	2,58	
	4	2	1	5	0	4	4	3	5	4	3	4	3,25	
DS5 5	3	4	5	5	5	5	5	4	5	4	3	5	4,42	
DS5 6	5	5	4	5	5	4	5	5	4	4	1	4	4,25	
DS5 7	4	3	2	4	3	4	5	2	5	5	5	5	3,92	
DS5 8	5	5	4	5	5	5	5	5	4	4	3	4	4,50	
DS5 9	5	0	1	3	4	5	2	2	5	4	4	3	3,17	
DS5 10	2	2	4	2	5	5	3	4	5	2	0	2	3,00	
DS5 11	4	4	4	5	5	4	3	5	5	4	3	2	3,92	



Gambar 4.3 Grafik DS5 (*Ensure System Security*)

Berdasarkan data grafik diatas bahwa, proses pengawasan dan evaluasi terhadap kinerja teknologi informasi pada *email corporate* berdasarkan *maturity* model sudah berjalan baik yaitu berada pada skala 4 yaitu 3.84 menurut responden, sudah berfungsi dengan baik dan penempatannya sudah sesuai dengan aturan, penggunaan teknologi informasi *email corporate* selalu mendapat pengawasan dari pimpinan sehingga tugas dapat diselesaikan tepat waktu. Namun kegiatan *training* penggunaan *email corporate* untuk pegawai belum secara keseluruhan.

Analisis Kesenjangan (*Gap*)

Merupakan tahapan dari sekumpulan perangkat yang mendukung ser memungkinkan para manajer untuk menjembatani jarak (*gap*) yang ada antara kebutuhan yang dikendalikan. Berdasarkan analisis keamanan sistem informasi pada *Email corporate* Universitas Teknologi Sumbawa yang sedang berjalan (*as-is*), maka dapat diketahui bahwa tingkat kematangan tersebut diidentifikasikan berada pada level 4. Sedangkan tingkat kematangan yang ditetapkan sebagai acuan (*to-be*) atau sistem untuk kedepan dalam tata kelola teknologi informasi pada pengelolaan data *Email corporate* di Universitas Teknologi Sumbawa diidentifikasikan pada level 5.

Pembahasan

Maturity model merupakan (*tools*) alat ukur untuk mengetahui kondisi proses Sistem Informasi pada *Email Corporate* di Universitas Teknologi Sumbawa. *Maturity* model akan menghasilkan kondisi sekarang tentang penilaian dari proses DS5 (*Ensure System Security*), terdiri dari :

a. DS5.1: Manajemen Keamanan TI (*Management Of IT Security*)
b. DS5.2: Rencana Keamanan TI (*IT Security Plan*)
c. DS5.3: Manajemen Identitas (*Identity Management*)
d. DS5.4: Manajemen Akun Pengguna (*User Account Management*)
e. DS5.5: Penjagaan, Pemantauan dan Uji Coba Keamanan (*Surveillance monitoring and Security Testing*)
f. DS5.6: Definisi Insiden Keamanan (*Security Incident Definition*)
g. DS5.7:Proteksi Teknologi Keamanan (*Protection of Security Technology*)
h. DS5.8:Manajemen Kunci Kriptografi (*Cryptographic Key Management*)
i. DS5.9: Pencegahan Software Berbahaya, Deteksi dan Perbaikan (*Malicious Software Prevention, Detection and Correction*)
j. DS5.10: Keamanan Jaringan (*Network Security*)
k. DS5.11: Pertukaran Data Sensitif (*Exchange of Sensitive Data*)

Pada *Maturity model* ,pengukuran digunakan pengambilan data melalui kuesioner. Responden yang dilibatkan adalah kepala divisi dengan otoritas implementasi sistem kerja dari masing - masing unit tersebut.

Tabel 4.2 Skala Pembuatan Indeks

Skala Pembuatan	Tingkat *Model Maturity*
4,51 - 5,00	5 - *Optimized*
3,51 - 4,50	4 - *Managed & Measureable*
2,51 - 3,50	3 - *Defined Process*
1,51 - 2,50	2 - *Repeatable but intuitive*
0,51 - 1,50	1 - *Initial*
0,00 - 0,50	0 - *Non-Existent*

Untuk mendukung audit tata kelola sistem informasi *email corporate* menggunakan Cobit 4.1. (*control objective for information and related technology*) di Universitas Teknologi Sumbawa, data yang diperoleh dari kuesioner akan diolah dan dilakukan :

1. Melakukan perhitungan rata-rata terhadap masing-masing atribut isian dari semua responden.
2. Penilaian tingkat maturity, proses tersebut diperoleh dengan melakukan perhitungan rata-rata semua attribut.
3. Representasi kondisi teknologi informasi yang ada.

ISSN 2527-970X | E-ISSN 2621- 542x

Tahap selanjutnya adalah menggunakan formula matematika untu merelasikan antara tingkatan nilai serta nilai absolut yang dilakukan dengan perhitungan dalam bentuk indeks, Persamaan matematika untuk menentukan nilai indeks adalah sebagai berikut:

$$\text{Indeks} = \frac{\Sigma\ DS5.1 + DS5.2 + DS5.3 + DS5.4 + DS5.5 + DS5.6 + DS5.7 + DS5.8 + DS5.9 + DS5.10 + DS5.11}{\Sigma \text{ pertanyaan kuesioner}}$$

$$\text{Indeks} = \frac{\Sigma\ 4.33 + 4.08 + 4.17 + 4,00 + 3,92 + 4,08 + 3,92 + 2.58 + 3,25 + 4.42 + 4.25 + 3.92 + 4.50 + 3.17 + 3.00 + 3.92}{\Sigma\ 16} = 3.84$$

Tingkat kematangan secara keseluruhan untuk domain DS5 (*Ensure System Security*) pada Universitas Teknologi Sumbawa adalah terdapat pada tingkat 3.85.

Tabel 4.3
Hasil Pengukuran Tingkat Kematangan Setiap Proses TI *email corporate* pada Domain DS5 (*Ensure System Security*)

Kontrol Proses Teknologi Informasi *Email Corporate*	Kondisi Saat ini	Tingkat *Model Maturity*
	Rata- Rata Per Proses	
DS5.1 : Manajemen Keamanan TI (*Management Of IT Security*)	4,33	*Managed & Measureable*
DS5.2: Rencana Keamanan TI (*IT Security Plan*)	4,08	*Managed & Measureable*
DS5.3 : Manajemen Identitas (*Identity Management*)	4,02	*Managed & Measureable*
DS5.4: Manajemen Akun Pengguna (*User Account Management*)	2,92	*Defined Process*
DS5.5: Uji Coba Keamanan, Penjagaan dan Pemantauan (*Security Testing, Surveillance and monitoring*)	4,42	*Managed & Measureable*
DS5.6: Definisi Insiden Keamanan (*Security Incident Definition*)	4,25	*Managed & Measureable*
DS5.7: Proteksi Teknologi Keamanan (*Protection of Security Technology*)	3,92	*Managed & Measureable*
DS5.8: Manajemen Kunci Kriptografi (*Cryptographic Key Management*)	4,50	*Managed & Measureable*
DS5.9: Pencegahan Software Berbahaya, Deteksi dan Perbaikan (*Malicious Software Prevention, Detection and Correction*)	3,17	*Managed & Measureable*
DS5.10: Keamanan Jaringan (*Network Security*)	3,00	*Defined Process*
DS5.11: Pertukaran Data Sensitif (*Exchange of Sensitive Data*)	3,92	*Managed & Measureable*

Skala hasil audit tata kelola sistem informasi pada email *corporate* di Universitas Teknologi Sumbawa menggunakan metode Cobit 4.1 yaitu :

a. DS5.1: Manajemen Keamanan TI (*Management Of IT Security*) dengan nilai rata-rata 4,33
b. DS5.2:Rencana Keamanan TI (*IT Security Plan*) dengan nilai rata-rata 4,08
c. DS5.3:Manajemen Identitas (*Identity Management*) dengan nilai rata-rata 4,02
d. DS5.4: Manajemen Akun Pengguna (*User Account Management*) dengan nilai rata-rata 2,92
e. DS5.5: Penjagaan Pemantauan dan Uji Coba Keamanan, (*Surveillance, monitoring and Security Testing,*) dengan nilai rata-rata 4,42
f. DS5.6: Definisi Insiden Keamanan (*Security Incident Definition*) dengan nilai rata-rata 4,25
g. DS5.7: Proteksi Teknologi Keamanan (*Protection of Security Technology*) dengan nilai rata-rata 3,92
h. DS5.8: Manajemen Kunci Kriptografi (*Cryptographic Key Management*) dengan nilai rata-rata 4,50
i. DS5.9: Pencegahan Software Berbahaya, Deteksi dan Perbaikan (*Malicious Software Prevention, Detection and Correction*) dengan nilai rata-rata 3,17
j. DS5.10: Keamanan Jaringan (*Network Security*) dengan nilai rata-rata 3,00
k. DS5.11: Pertukaran Data Sensitif (*Exchange of Sensitive Data*) dengan nilai rata-rata 3,92

Tingkat *maturity* skala 4 yaitu *managed and measurable*, pada tingkat ini

1. Kondisi dimana ukuran kuantitatif yang dijadikan sebagai sasaran maupun objektif terhadap kinerja proses teknologi informasi atau universitas telah memiliki sejumlah indikator atau
2. Terdapat fasilitas untuk mengukur prosedur dan memonitor yang sudah berjalan, dapat mengambil tindakan jika terdapat proses yang diindikasikan tidak efektif.
3. Proses dibandingkan dengan praktik-praktik terbaik dan diperbaiki terus menerus.
4. Terdapat otomatisasi untuk pengawasan proses dan perangkat bantu.

Tingkat model *maturity* skala 3 yaitu :

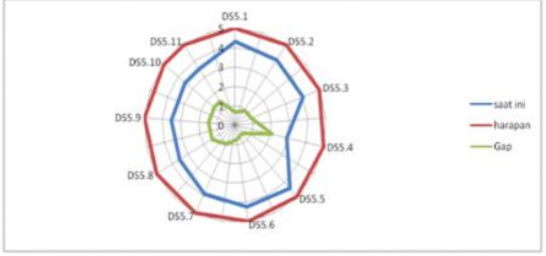
a. DS5.10 Keamanan Jaringan (*Network Security*) dengan nilai rata-rata 3,00
b. DS5.4: Manajemen Akun Pengguna (*User Account Management*) dengan nilai rata-rata 2,92

Maturity model skala 3 yaitu *defined process*, pada tingkat ini

a. Kondisi di mana universitas memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke seluruh civitas akademika dan tenaga pendidik untuk dipatuhi dan dikerjakan.
b. Memungkinkan terjadinya banyak penyimpangan dikarenakan tidak adanya pengawasan untuk menjalankan prosedur.

Grafik hasil pengukuran tingkat kematangan proses audit sistem informasi pada *email corporate* menggunakan COBIT 4.1. (*control objective for information and related technology*) di Universitas Teknologi Sumbawa seperti grafik dibawah ini.

	DS5.1	DS5.2	DS5.3	DS5.4	DS5.5	DS5.6	DS5.7	DS5.8	DS5.9	DS5.10	DS5.11
saat ini	4,33	4,08	4,02	2,92	4,42	4,25	3,92	3,53	3,53	3,53	3,53
Harapan	5	5	5	5	5	5	5	5	5	5	5
Gap	0,67	0,92	0,98	2,08	0,58	0,75	1,08	1,47	1,47	1,47	1,47



Gambar 4.4 Grafik Penilaian Kuisioner

ISSN 2527-970X | E-ISSN 2621- 542x

Adapun seluruh hasil dari tingkat *maturity* model penelitian sistem informasi pada *email corporate* menggunakan COBIT 4.1. (*control objective for information and related technology*) di Universitas Teknologi Sumbawa yaitu skala 4 (*Managed and Measurable*), kampus sudah menggunakan teknologi informasi yang ada. Prosedur telah distandarisasi tapi belum dan didokumentasikan, tetapi belum adanya Pakta Integritas '*term of agreement*' yang mengikat penggunaan e*mail corporate* serta implementasi sistem kerja berbasis paperless. Hal ini dinyatakan bahwa proses harus diikuti, namun tidak mungkin bahwa penyimpangan akan terdeteksi. Prosedur sendiri tidak canggih tetapi formalisasi praktek yang ada.

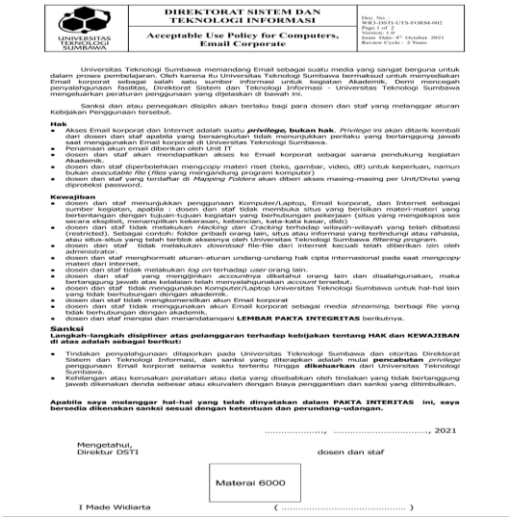
Temuan dari analisis keamanan sistem informasi pada *email corporate* di Universitas Teknologi Sumbawa sudah distandarisasi, terdokumentasi, dan dikomunikasikan melalui pelatihan tetapi implementasi inovasi sistem kerja paperless pada penyimpanan online melalui email corporate masih belum terlaksana dan belum tersedia Pakta Integritas '*Term of Agreement*' *email corporate* serta masih tergantung pada pegawai apakah mau mengikuti prosedur tersebut atau tidak. Prosedur yang dibuat tersebut tidak rumit, hanya merupakan formalitas yang sudah ada.

Implementasi

Berdasarkan hasil temuan dari analisis keamanan sistem informasi pada *email corporate* diatas, maka pada bagian ini akan dilakukan tahap implementasi dari aturan hukum penggunaan *email corporate* dan implementasi sistem kerja berbasis *paperless* melalui media manajemen penyimpanan *email corporate* di Universitas Teknologi Sumbawa

1. Pakta Integritas '*Term of Agreement*'

Berikut adalah hasil dari pembuatan Pakta Integritas '*Term of Agreement*' atau aturan hukum penggunaan *email corporate* di Universitas Teknologi Sumbawa.



DIREKTORAT SISTEM DAN TEKNOLOGI INFORMASI

Acceptable Use Policy for Computers, Email Corporate

Universitas Teknologi Sumbawa memandang Email sebagai suatu media yang sangat berguna untuk dalam proses pembelajaran. Oleh karena itu Universitas Teknologi Sumbawa bermaksud untuk menyediakan Email korporat sebagai salah satu sumber informasi untuk kegiatan Akademik. Demi mencegah penyalahgunaan fasilitas, Direktorat Sistem dan Teknologi Informasi - Universitas Teknologi Sumbawa mengeluarkan peraturan penggunaan yang dijelaskan di bawah ini.

Sanksi dan atau penegakan disiplin akan berlaku bagi para dosen dan staf yang melanggar aturan Kebijakan Penggunaan tersebut.

Hak

- Akses Email korporat dan Internet adalah suatu ***privilege*, bukan hak**. *Privilege* ini akan ditarik kembali dari dosen dan staf apabila yang bersangkutan tidak menunjukkan perilaku yang bertanggung jawab saat menggunakan Email korporat di Universitas Teknologi Sumbawa.
- Penamaan akun email diberikan oleh Unit IT
- Dosen dan staf akan mendapatkan akses ke Email korporat sebagai sarana pendukung kegiatan Akademik.
- dosen dan staf diperbolehkan *mengcopy* materi riset (teks, gambar, video, dll) untuk keperluan, namun bukan *executable file* (*files* yang mengandung program komputer)
- dosen dan staf yang terdaftar di *Mapping Folders* akan diberi akses masing-masing per Unit/Divisi yang diprotekasi password.

Kewajiban

- dosen dan staf menunjukkan penggunaan Komputer/Laptop, Email korporat, dan Internet sebagai sumber kegiatan, apabila : dosen dan staf tidak membuka situs yang berisikan materi-materi yang bertentangan dengan tujuan-tujuan kegiatan yang berhubungan pekerjaan (situs yang mengekspos sex secara eksplisit, menampilkan kekerasan, kebencian, kata-kata kasar, dlsb)
- dosen dan staf tidak melakukan *Hacking dan Cracking* terhadap wilayah-wilayah yang telah dibatasi (restricted). Sebagai contoh: folder pribadi orang lain, situs atau informasi yang terlindungi atau rahasia, situs atau data yang telah terblok akseanya oleh Universitas Teknologi Sumbawa *filtering program*.
- dosen dan staf tidak melakukan *download* file-file dari internet kecuali telah diberikan izin oleh administrator.
- dosen dan staf menghormati aturan-aturan undang-undang hak cipta internasional pada saat *mengcopy* materi dari internet.
- dosen dan staf tidak melakukan *log on* terhadap *user* orang lain.
- dosen dan staf yang menggunakan *accountnya* dikatahui orang lain dan disalahgunakan, maka bertanggung jawab atas kelalaian telah menyalahgunakan *account* tersebut.
- dosen dan staf tidak menggunakan Komputer/Laptop Universitas Teknologi Sumbawa untuk hal-hal lain yang tidak berhubungan dengan akademik.
- dosen dan staf tidak mengkomersilkan akun Email korporat
- dosen dan staf tidak menggunakan akun Email korporat sebagai media *streaming*, berbagi file yang tidak berhubungan dengan akademik.
- dosen dan staf menjaga dan menandatangani **LEMBAR PAKTA INTEGRITAS** berikutnya.

Sanksi

Langkah-langkah disipliner atas pelanggaran terhadap kebijakan tentang HAK dan KEWAJIBAN di atas adalah sebagai berikut:

- Tindakan penyalahgunaan dilaporkan pada Universitas Teknologi Sumbawa dan otoritas Direktorat Sistem dan Teknologi Informasi, dan sanksi yang diterapkan adalah mulai **pencabutan** *privilege* penggunaan Email korporat selama waktu tertentu hingga **dikeluarkan** dari Universitas Teknologi Sumbawa.
- Kerusakan atau kerusakan peralatan atau data yang disebabkan oleh tindakan yang tidak bertanggung jawab dikenakan denda sebesar atau ekuivalen dengan biaya penggantian dan sanksi yang ditimbulkan.

Apabila saya melanggar hal-hal yang telah dinyatakan dalam PAKTA INTERITAS ini, saya bersedia dikenakan sanksi sesuai dengan ketentuan dan perundang-udangan.

....., ..., 2021

Mengetahui,
Direktur DSTI

dosen dan staf

Materai 6000

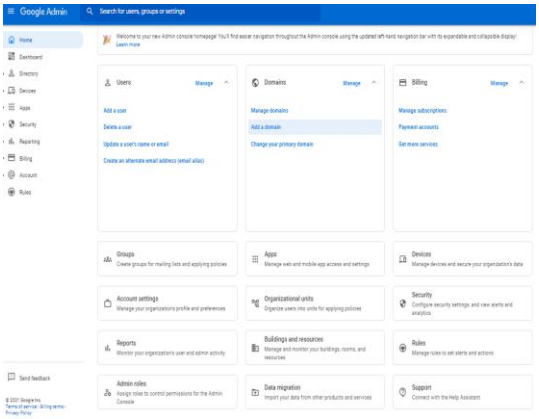
I Made Widiarta

(.....)

2. Paperless work system

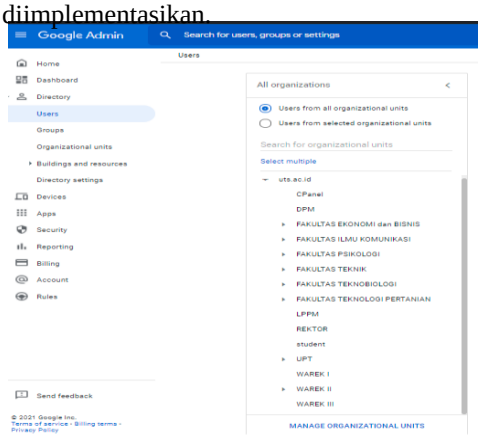
Berikut merupakan tahapan penerapan sistem kerja berbasis *paperless* melalui manajemen penyimpanan *email corporate* di Universitas Teknologi Sumbawa

a. Gambar berikut merupakan dashboard dari implementasi *paperless working system* ,menggunakan media *email corporate* universitas, pada *dashboard* utama terdapat beberapa fitur konfigurasi *email corporate* yang akan diimplementasikan adalah *management drive*, *user*, *group*, dan *file.*



Gambar 4.6 *Dashboard Email Corporate*

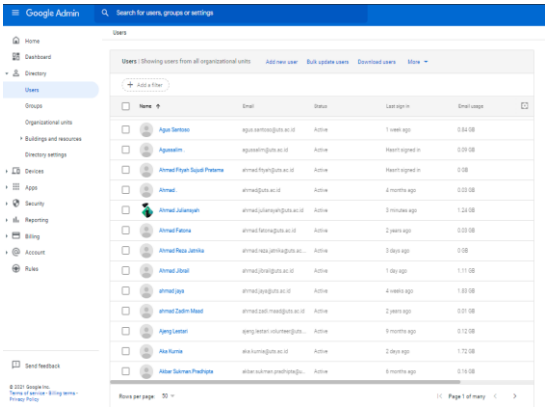
b. Gambar berikut merupakan *management drive* ,serta konfigurasi dari implementasi *paperless working system* ,menggunakan media drive email corporate universitas, pada *management drive* terdapat beberapa konfigurasi drive bersama , drive unit , *grouping drive* unit, management rule drive *'create*, *edit*, *view'* yang diimplementasikan.



Gambar 4.7 *Drive Email Corporate*

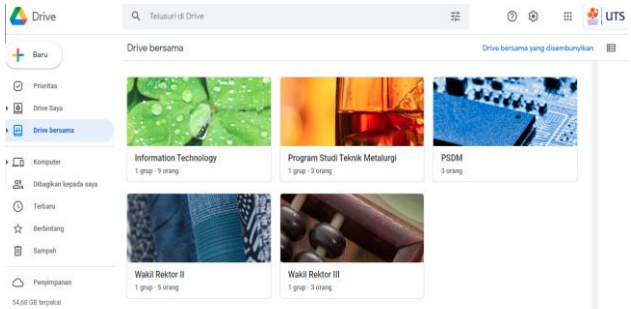
c. Gambar berikut adalah dashboard user ,serta konfigurasi dari implementasi *paperless working system* ,menggunakan media *user email corporate* universitas, pada dashboard user terdapat beberapa konfigurasi *user email corporate* yang wajib dibuat menggunakan nama lengkap, untuk memudahkan *paperless* surat menyurat, dll yang diimplementasikan.

ISSN 2527-970X | E-ISSN 2621- 542x



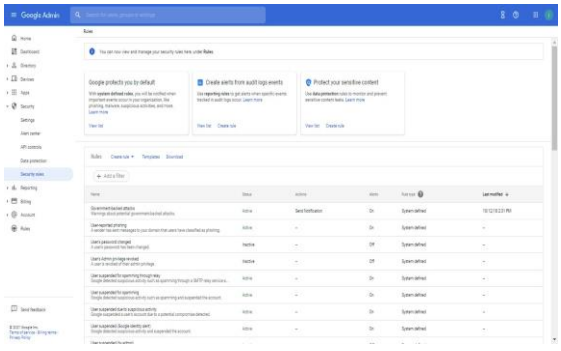
Gambar 4.8 *User Email Corporate*

d. Gambar berikut adalah *drive* dan *user* yang diterapkan pada seluruh unit dari implementasi *paperless working system*, menggunakan media *email corporate* universitas, pada implementasi tersebut terdapat beberapa hasil yang sukses diterapkan, yaitu manajemen penyimpanan bersama satu universitas dan masing-masing unit, serta aturan (*edit, view, create*) pada seluruh file dengan *extensi* document, excel, *pdf*, dan *powerpoint* di drive menggunakan media *email corporate*, serta surat menyurat yang tidak lagi menggunakan kertas.



Gambar 4.9 *User* dan *drive* implementasi

e. Gambar berikut merupakan *dashboard security* pada implementasi '*Policy Security*' dari *paperless working system* ,menggunakan media *email corporate* universitas, pada dashboard security utama terdapat beberapa fitur konfigurasi *email corporate* yang akan diimplementasikan adalah *management security user* , *file extensi*, *synchronize* , dan *device policy*.

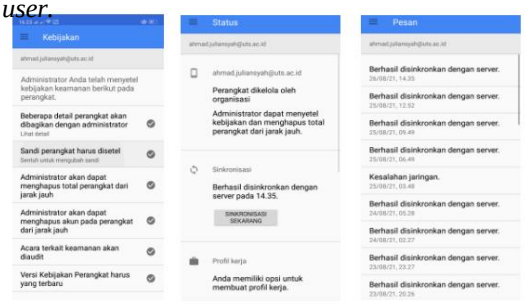


Gambar 4.10 *Dashboard Security*

f. *Dashboard security user* terdapat beberapa fitur konfigurasi *email corporate* yang telah diimplementasikan melalui *dashboard security* utama, jika ingin menggunakan *email corporate* universitas di perangkat ponsel yaitu ; keamanan internal perangkat adalah *email corporate* tidak akan bisa digunakan atau diinstal pada perangkat ponsel, jika perangkat tidak memiliki keamanan seperti pola, *password* , *finger* dll. Aturan *sinkronisasi email* dan *drive*, keamanan internal perangkat melalui *device policy* perangkat .

Gambar 4.11 *Dashboard Security User*

g. Gambar berikut merupakan penerapan dari keamanan sistem informasi pada *email corporate* universitas yang telah diimplementasikan. '*Device policy*' yang telah dikonfigurasi tersebut, keamanan data universitas seperti *file extens*i asing serta serangan dari luar melalui *email corporate* dapat teratasi, dari penerapan *security paperless working system*, menggunakan media *email corporate* universitas, pada *dashboard security user*.



Gambar 4.12 *Device policy user*

PENUTUP

Kesimpulan

Berdasarkan hasil pembahasan dan audit yang telah dilakukan, dapat disimpulkan bahwa Analisis Keamanan Sistem Informasi pada Email Corporate UTS menggunakan COBIT 4.1 (*Control Objectives for Information and Related Technology*) mampu memberikan hasil audit keamanan sistem informasi yang lebih optimal pada *email corporate* untuk mendukung sistem kerja berbasis paperless,

ISSN 2527-970X | E-ISSN 2621- 542x

serta mampu mengimplementasikan Inovasi Smart Campus di Universitas Teknologi Sumbawa.

Saran

Analisis Keamanan Sistem Informasi pada *email corporate* yang dilakukan oleh peneliti, masih belum menyertakan metode integrated sistem yang berbasis SSO (*Single Sign On*). Diharapkan peneliti selanjutnya mampu merancang konfigurasi *system* pada *email corporate*, dengan tujuan mengintegrasikan seluruh sistem informasi yang masih berdiri sendiri (*stand alone*) di Universitas Teknologi Sumbawa dalam bentuk satu pintu dengan media *email corporate*

REFERENSI

Andrea Pederiva. (2018). The COBIT Maturity Model In Vendor Evaluation Case, Information System Control Journal, Vol 3, ISACA

Arikunto. (2019). Populasi dan Sampel .Prosedur Penelitian suatu Pendekatan Praktek. Rineka Cipta. Jakarta.

Budi Widjajanto, Nova Rijati, (2019). Analisis Maturity Level Tata Kelola Teknologi Informasi UDINUS Berdasarkan Domain DS dan ME COBIT 4.0, LP2M Universitas Dian Nuswantoro.

Cocca, P. (2014), Email Security Threats. Amerika : GIAC Security Essentials Certification (GSEC).

Darminto, Dwi Prastowo., dan Rifka Julianty. (2019). Analisa Laporan Keuangan: Konsep dan Manfaat. Yogyakarta. AMP-YKPN: halaman 52

ISACA, (2019), COBIT Student Book, IT Governance Institute

ISACA, (2018), Integrating COBIT into the IT Audit Process (Planning, Scope Development, Practise) , IT Governance Institute

IT Governance Institute, (2016), COBIT 4.0 Control Objectives, Management Guidelines, Maturity Models , IT Governance Institute

Santi. (2020). Metode Penelitian deskriptif kualitatif .Jurnal Tarbiyah al-Awlad, 4(1),. 345-357.

Haerudin, H. (2017). undefined. Jurnal Informatika Universitas Pamulang, 2(4), 174. https://doi.org/10.32493/informatika.v2i4.1437

Hamid, H. (2017). Analisis keamanan aplikasi email bawaan Android Dan Gmail pada jaringan nirkabel. Teknoin, 23(2).

Haula, Kinanti. (2018) "PERANCANGAN DATABASE MENGGUNAKAN GOOGLE SUITE UNTUK PENILAIAN PERFORMANCE INDICATOR MATA KULIAH BERSTANDAR ABET". Fakultas Teknik. UGM

Mustofa, A., & Supriatnoko, S. (2019). undefined. Epigram, 16(1). https://doi.org/10.32722/epi.v16i1.1424

Robert Hartono. (2015). Analisis dan perancangan sistem keamanan email menggunakan gnu privacy guard Pada linux ubuntu 12.04, 2016 UIB Repository(c)

Ula, M. (2019). Analisis metode pengamanan data pada layanan cloud computing. TECHSI - Jurnal Teknik Informatika, 11(1), 116

Yuliandesi, A., Sitompul, D. R., AJF, A. P., & Mhd.Arief. (2020). Implementasi algoritma md5 Dan rc4

ISSN 2527-970X | E-ISSN 2621- 542x