BERKALA SAINSTEK 2021 9(1): 35-44
doi: 10.19184/bst.v9i1.20361
https://jurnal.unej.ac.id/index.php/BST/article/view/20361

RESEARCH ARTICLE

Information System Security Audit Based on the DSS05 Framework Cobit 5 at Higher Education XX

(Audit Keamanan Sistem Informasi Berbasis DSS05 Framework Cobit 5 Pada Perguruan Tinggi XX)

Rudolf Sinaga[1*)], Samsinar[2], Renny Afriany[2]
[1]Fakultas Ilmu Komputer, Program Studi Sistem Informasi, UNAMA, Jambi, Indonesia
[2] Program Studi D-3 Keperawatan, STIKES Garuda Putih, Jambi, Indonesia

ABSTRACT

Currently, information has become a commodity or basic need, it can even be said that we are already in an "information-based social" era. It is undeniable that the ability to access and ensure the availability of information quickly and accurately has become a very essential component for an organization, whether in the form of social or commercial organizations, educational institutions such as universities, government agencies, and individuals. Various channels were created to regulate access rights to information, to prevent unauthorized people from accessing it, to minimize losses for the owner of the information. Based on the results of interviews with the research object of XX college, there are still frequent disruptions to information system security such as attacks on servers that result in server downtime, attacks on institutional e-mails that result in being unable to receive or even send e-mails, and other disturbances. This certainly harms information services at the tertiary institution, therefore an information system security audit is required. This study aims to measure the level of information system security capabilities using the Cobit 5 framework in the APO13 and DSS05 domains. Based on the results of the audit, it was found that the GAP value was 3.6 for the APO13 domain or at level 1 while 3.4 for the GAP DSS05 value or at level 2, it can be concluded that the information system security maturity level is still very low so that it needs improvement. It is recommended to make SOPs and documentation of maintenance, control, and periodic security evaluation, install an antivirus that has high and up to date protection accuracy, and make regular maintenance reports both on software and hardware.

Saat ini informasi sudah menjadi sebuah komoditi atau kebutuhan pokok, bahkan boleh dikatakan kita sudah berada di masa "sosial berbasis informasi". Sudah tidak dapat dipungkiri, bahwa kemampuan untuk mengakses dan menjamin ketersediaan informasi secara cepat dan akurat sudah menjadi komponen yang sangat esensial bagi sebuah organisasi, baik yang berupa organisasi sosial maupun komersial, lembaga pendidikan seperti perguruan tinggi, instansi pemerintahan, maupun pribadi. Berbagai kanal diciptakan untuk mengatur hak akses informasi, untuk menjaga agar tidak dapat diakses oleh orang yang tidak berhak, yang bertujuan meminimalisir kerugian bagi pemilik informasi tersebut. Berdasarkan hasil wawancara pada objek penelitian perguruan tinggi XX, masih sering ditemukan adanya gangguan terhadap keamanan sistem informasi seperti serangan terhadap server yang mengakibatkan server *down*, serangan terhadap email institusi yang mengakibatkan tidak dapat menerima bahkan mengirim email serta gangguan lainnya. Hal ini tentu berdampak buruk terhadap layanan informasi pada perguruan tinggi tersebut, oleh sebab itu diperlukan kegiatan audit keamanan sistem informasi. Penelitian ini bertujuan untuk mengukur tingkat kapabilitas keamanan sistem informasi dengan menggunakan framework Cobit 5 pada domain APO13 dan DSS05. Berdasarkan hasil audit yang dilakukan didapatkan nilai GAP 3,6 untuk domain APO13 atau berada di level 1 sedangkan 3,4 untuk nilai GAP DSS05 atau berada di level 2, dapat disimpulkan bahwa tingkat kematangan keamanan sistem informasi masih sangat rendah sehingga diperlukan perbaikan. Direkomendasikan untuk membuat SOP dan pendokumentasian terhadap pemeliharaan, control dan evaluasi keamanan secara berkala, memasang antivirus yang memiliki akurasi proteksi yang tinggi dan uptodate serta membuat pelaporan maintanance secara berkala baik pada software maupun hardware.

Keywords: information system security audits, security evaluation, protection.

*)Corresponding author:
Rudolf Sinaga
E-mail: rudolfverdinan@gmail.com

PENDAHULUAN

Saat ini Internet telah menjadi media yang paling ekonomis untuk digunakan sebagai basis sistem informasi. Develover perangkat lunak pun semakin banyak bermunculan, sehingga akses terhadap perangkat lunak pun semakin banyak yang tersedia secara murah, bahkan ada yang bisa diakses secara gratis. Alasan-alasan ini pula yang menyebabkan Internet menjadi media elektronik yang paling populer untuk menjalankan bisnis. Persaingan pun semakin ketat, upaya untuk membangun layanan yang mampu menyediakan informasi secara cepat dan akurat pun menjadi komponen yang sangat esensial bagi sebuah organisasi, baik yang berupa perusahaan atau organisasi komersial, lembaga pendidikan seperti perguruan tinggi, lembaga pemerintahan, maupun pribadi. Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi internal penting ke pihak lain (misalnya pihak kompetitor) tentu dapat menimbulkan kerugian bagi para pemilik informasi [1].

Walaupun sangat sering terlihat sebagai besaran yang tidak dapat langsung diukur dengan uang (*intangible*), keamanan sebuah sistem informasi sebenarnya dapat diukur dengan besaran yang dapat diukur dengan uang (*tangible*). Kerugian yang ditimbulkan dampaknya tidak dirasakan langsung misalnya kehilangan data yang menyebabkan diharuskan mencari data, untuk mengembalikan data diperlukan waktu bahkan data tersebut tidak dapat diambil kembali karena waktu yang sudah berlalu meskipun bersedia mengeluarkan biaya [2]. Maka dari itu diperlukan keamanan yang handal dari sistem informasi agar resiko kehilangan data dan pengontoral keamanaan dapat terlihat secara berkala. Untuk mengukur keberhasilan keamanan tersebut dapat dilakukan audit sistem informasi [3]. Dalam pelaksanaan audit tersebut perlu adanya standar yang baik sehingga ada perbandingan bagaimana keamanan yang sudah sesuai standar [3,4].

Perguruan Tinggi XX sudah memiliki sistem informasi yang terintegrasi antara sistem informasi akademik, *Digital Library*, *Open Journal System* (OJS), Portal Website dengan pelaporan PDDikti. Dari hasil wawancara terhadap pengelola unit IT, ditemukan masih sering adanya gangguan terhadap keamanan sistem informasi seperti serangan terhadap server yang mengakibatkan server *down*. Kegagalan akses pernah terjadi yang mengakibatkan tidak dapat menerima bahkan mengirim email serta gangguan lainnya. Hal ini menimbulkan kendala pada layanan informasi maupun terhadap proses pelaksanaan pelaporan, selain itu adanya kerusakan pada perangkat keras yang digunakan karena tidak sesuai dengan standar yang ditetapkan sehingga membutuhkan biaya yang lebih besar dari yang diharapkan. Agar kegagalan akses tersebut tidak terjadi lagi maka diperlukan audit system informasi agar terlihat pada bagian mana yang membutuhkan perbaikan dan peningkatan kualitas keamanan.

COBIT 5 merupakan kerangka kerja untuk manajemen, yang mampu mencakup aspek teknis maupun non teknis, mengelola semua yang berkaitan dengan teknologi informasi mulai dari pemenuhan kebutuhan para *stakeholder* terhadap teknologi informasi. COBIT 5 memiliki prinsip dasar untuk tata kelola dan manajemen TI.

Pada tingkat international kerangka kerja Cobit.5 telah diakui cukup baik. Bukan hanya diperoleh hasil evaluasi terhadap keamanan system namun juga diperoleh masukan untuk rekomendasi yang dapat digunakan dimasa mendatang [5,6,7]. Pada penelitian berfokus pada domain APO 13 (*Align, Plan dan Organise*) dan DSS 05 (*Delivery and Support System*). Apo 13 adalah proses pendefinisian, implementasi dan pengontrolan system yang diterapkan untuk menjaga resiko keamanan system informasi yang tidak diperbolehkan melebihi resiko yang telah ditentukan [4,8,9]. DSS adalah domain yang berfokus pada proses pelayanan TI dan dukungan teknisnya pada area keamanan system yang berkesinambungan dalam pengelolaan data yang sudah diterapkan [9,4].

METODE PENELITIAN

Kajian Pustaka

A. Penelitian Terdahulu

Penelitian yang dilakukan oleh Dewi Ciptaningrum, dkk tentang pelaksanaan audit keamanan sistem informasi pada Pemerintah Kota Yogyakarta menggunakan kerangka COBIT 5 untuk mengukur Keamanan Informasi. Pemilihan proses diukur melalui pemetaan tujuan kaskade yang menghasilkan lima (5) proses dalam COBIT 5, Hasil pengukuran kapabilitas keamanan SI yang dilakukan pada instansi Pemerintah Kota Yogyakarta

menunjukkan dari kelima proses yang diukur, tidak ada yang mampu mencapai level yang ditargetkan, yaitu level 3. Bahkan dari kelima proses itu hanya bisa mencapai level 1 [10].

Penelitian berikutnya yang dilakukan oleh Rifki Dimas Krisdiyawan, dkk., adalah audit keamanan sistem informasi pada RS MATA DR.YAP Yogyakarta menggunakan framework Cobit 5. Penelitian tersebut bertujuan untuk mengukur tingkat kemapanan keamanan dari sistem informasi yang sedang berjalan. Hasil penelitian menunjukkan bahwa pengelolaan keamanan pada Sistem lnformasi sudah hampir memenuhi keseluruhan aspek dalam domain APO 13 (*Manage Security*) dan DSS 05 (*Manage Security Services*) COBIT 5 Framework yang dibuktikan dengan tingkat kapabilitas yang dicapai pada domain APO 13 yaitu 2,59 berada pada level 3 (*Established Process*). Artinya hasil tersebut menunjukan bahwa pengelolaan keamanan sistem informasi telah dikelola dengan baik, namun demikian masih terus dikembangkan agar semakin mapan [4].

Selanjutnya pada penelitian yang dilakukan oleh Bagus Puji Santoso, dkk., yaitu penilaian tata kelola keamanan informasi perpustakaan dengan framework Cobit 5. Tujuan penelitian dilakukan untuk menilai tata kelola keamanan teknologi informasi perpustakaan yang sedang berjalan. Analisis dilakukan dengan alat bantu pengukuran tata kelola keamanan informasi meliputi penurunan tujuan organisasi dan TI, pemetaan proses tata kelola terhadap proses mengacu pada COBIT 5. Sementara itu, hasil dari penelitian tersebut ditemukan skala rating kapabilitas APO13 dan DSS05 berada di level P (*Partially Achieved*) yang berarti ada beberapa bukti dari aktivitas yang dijalankan dan beberapa pencapaian atribut yang didefinisikan dalam penilaian proses. Sedangkan level kapabilitas berada di level 1 (*performed process*) yang artinya ada proses dilaksanakan namun pencapaian tiap prosesnya belum terpenuhi semuanya dan belum mencapai tujuan proses yang diharapkan. Hasil analisis penelitian menemukan gap pada sub domain APO13 dan DSS05 hanya mampu memperoleh nilai rata-rata 1.0 [11].

Dari beberapa penelitian terkait tersebut, menunjukkan bahwa framework Cobit 5 sangat baik digunakan dalam membantu suatu organisasi dalam mengaudit tingkat kematangan keamanan sistem informasi. Namun pada penelitian tersebut tidak dilakukan perbandingan antara nilai yang diharapkan atau tingkat kematangan yang diharapkan oleh organisasi terhadap nilai kesenjangan (GAP), sehingga tidak cukup data yang digunakan untuk mengukur dan menyimpulkan tingkat kematangan keamanan yang dimaksud, sedangkan pada penelitian yang kami lakukan adalah selain menghitung tingkat kematangan berdasarkan domain APO13 dan DSS05, juga dilakukan penghitungan nilai GAP yang selanjutnya dibandingkan dengan nilai maturity masing-masing domain. Sehingga lebih memperkuat dalam penyusunan rekomendasi terhadap perbaikan dan peningkatan kapabilitas keamanan sistem informasi dikemudian hari.

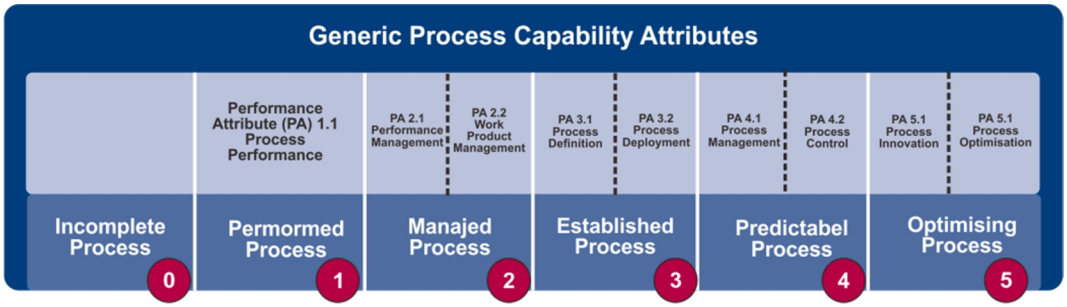
B. Dasar Teori

COBIT (*Control Objectives for Information and Related Technology*) merupakan sebuah kerangka kerja untuk tata kelola TI (*IT Governance*) yang dikembangkan oleh ISACA (*Information System and Control Association*) pada tahun 1992. COBIT dapat membantu perusahaan dalam mencapai tujuan dengan tata kelola dan manajemen TI. Saat ini ISACA mengeluarkan versi terakhir COBIT yaitu COBIT 5. COBIT 5 memberikan kerangka kerja yang mencakup 5 domain pada area governance yaitu memastikan bahwa kebutuhan, kondisi dan pilihan pemangku kepentingan dievaluasi untuk menentukan tujuan perusahaan yang seimbang dan disepakati yang akan dicapai, menetapkan arah melalui prioritas dan pengambilan keputusan seta memantau kinerja dan kepatuhan terhadap arah dan tujuan yang disepakati khusus untuk domain EDM (*Evaluate, Direct, and Monitor*) dan pada area management yaitu perencanaan, pembangunan, menjalankan dan pemantauan kegiatan yang selaras dengan arahan yang ditetapkan oleh badan tata kelola untuk mencapai tujuan perusahaan khusus domain APO (*Align, Plan, and Organize*), BAI (*Build, Acquire, and Implement*), DSS (*Deliver, Service, and Support*) dan MEA (*Monitor, Evaluate, and Assess*). [9]

COBIT 5 memberikan penilaian *capability levels* untuk setiap proses yang digolongkan menjadi 6 tingkatan, yaitu : a. Level 0 *Incomplete Process*, Proses tidak diimplementasikan atau gagal untuk mencapai prosesnya tujuan. Pada tingkat ini, hanya sedikit atau tidak ada bukti dari pencapaian proses yang sistematis tujuan. b. Level 1 *Performed Process* (satu atribut), Proses yang diimplementasikan mencapai tujuan prosesnya. c. Level 2 *Managed process* (dua atribut), Proses yang telah

dijelaskan sebelumnya sekarang diimplementasikan dengan cara yang dikelola (direncanakan, dipantau dan disesuaikan) dan produk kerjanya ditetapkan dengan tepat, dikendalikan dan terawat. d. Level 3 *Established Process* (dua atribut), Proses yang telah dijelaskan sebelumnya sekarang beroperasi dalam batasan yang ditetapkan untuk mencapai hasil prosesnya. e. Level 4 *Predictable process* (dua atribut), Proses yang telah dijelaskan sebelumnya sekarang beroperasi dalam batasan yang ditetapkan untuk mencapai hasil prosesnya. f. Level 5 *Optimized process* (dua atribut), Proses prediksi yang telah dijelaskan sebelumnya terus ditingkatkan untuk memenuhi tujuan bisnis saat ini dan yang diproyeksikan [1].

Proses APO13 adalah proses pendefinisian, pengoperasian dan pengawasan sistem yang diterapkan suatu organisasi untuk mengelola keamanan pada sistem informasi yang dimiliki. Proses ini bertujuan untuk menjaga dan meminimalisir kejadian dan dampak atas gangguan keamanan informasi yang tidak boleh lebih dari level resiko yang ditentukan organisasi. Indikator kapabilitas proses adalah kemampuan proses dalam meraih tingkat kapabilitas yang dibentuk oleh proses. Bukti atas indikator kapabilitas proses akan mendukung penilaian atas pencapaian atribut proses. Dimensi kapabilitas dalam model penilaian proses mencakup enam tingkat kapabilitas sebagaimana ditunjukkan pada Gambar 1 [12].



Gambar 1. Model proses kapabilitas pada Cobit 5

DSS05 merupakan domain yang mencakup perlindungan informasi untuk mempertahankan tingkatan keamanan informasi sesuai dengan kebijakan keamanan sistem informasi pada sebuah organisasi atau perusahaan. Sub Proses pada DSS adalah sebagai berikut: 1. DSS05.1, Mengelola Jaringan dan Keamanan Konektifitas, 2. DSS05.2 mengelola keamanan *endpoint*, 3. DSS05.3, mengelola identitas User dan Akses logik, 4. DSS05.4, mengelola akses fisik terhadap aset TI, 5. DSS05.5, mengelola dokumen sensitif dan perangkat output. [12]

Tahapan Penelitian

Pada penelitian ini, metode yang digunakan untuk memperoleh hasil audit terhadap kinerja keamanan sistem informasi yang dimaksud adalah dengan tahapan sebagai berikut: 1. Memahami alur dari sistem informasi yang sedang berjalan, 2. Melakukan pengujian melalui kuiesioner berdasarkan Framework Cobit 5, selanjutnya diolah dan dibandingkan dengan tingkat maturity, melalui pengendalian proses yang menggunakan domain pada Cobit 5 yaitu meliputi APO (*Align, Plan and Organize*) dan DSS (*Service and Support*).

Gambar 2. Diagram alir penelitian

HASIL DAN PEMBAHASAN

Pada bagian ini akan dijelaskan hasil audit keamanan sistem informasi terhadap COBIT 5 untuk domain APO13 dan DSS05 untuk melihat apakah tingkat kematangan (*maturity level*) berdasarkan kedua standar tersebut sudah menunjukkan nilai memenuhi aspek keamanan sistem informasi.

Penyebaran Kuisioner

Sebelum melakukan penelitian telah dilakukan wawancara pada divisi TI yang berkaitan dengan security yang sudah berjalan. Kemudian dari hasil wawancara tersebut diperoleh data-data yang kemudian disusun kuisioner tentang keamanan TI berdasarkan Cobit 5. Responden divis TI yang diberikan kuisioner berjumlah 5 orang. 1 orang adalah kepala divisi IT, 2 orang bagian teknisi TI dan 2 orang lainnya adalah bagian pelaksana (admin) pada divisi TI. Dalam pengisian kuisioner tidak hanya berfokus pada pernyataan tapi juga dilakukan wawancara melihat sejauh mana pengisian kuisioner dengan bukti dokumen yang dimiliki oleh divisi teknologi maupun bagian pengguna system informasi tersebut. Skala penilaian pada kuisioner dengan tingkat persetujuan range 1 sampai dengan 5, yaitu tidak ada, ada ,ada belum lengkap, lengkap dan sangat lengkap.

Pengolahan Kuisioner

Penelitian ini berfokus pada evaluasi keamanan informasi yang ada pada Perguruan Tinggi XX. Sub kontrol yang diambil pada penelitian ini yaitu audit keamanan sistem untuk melihat tingkat risiko keamanan informasi yang dapat diterima oleh Perguruan Tinggi XX sesuai dengan kebijakan keamanan kemudian menetapkan dan mempertahankan peran keamanan informasi dan hak akes yang nantinya akan dilakukan pengontrolan dan rekomendasi perbaikan keamanan yang ada. Kerangka Cobit 5 pada domain APO 13 dan DSS 05. 5 Domain APO13 tersebut terdiri dari sub item yang terdapat pada Tabel 1, sedangkan domain DSS 05 pada Tabel 2.

Tabel 1. Kerangka Cobit.5 pada domain APO 13

Domain	*Manage Security*
APO13 01	*Establish and maintain an information security management system (ISMS)*
APO13 02	*Define and manage an information security risk treatment plan.*
APO13 03	*Monitor and review the ISMS*

Pada APO 13 berfokus pada perencanaan dan pelaksanaan *security* yang sudah berjalan. Pada APO 13 ini terdiri dari 5 pernyataan yang masing-masing memiliki skala 1 sampai dengan 5.

Tabel 2**.** Kerangka Cobit.5 pada domain DSS 05

Domain	Manage Operation
DSS 01	Manage network and connectivity security
DSS 02	Manage endpoint security
DSS 03	Manage user identity and logical access
DSS 04	Manage physical access to IT assets
DSS 05	Manage sensitive documents and output devices

Kuisioner DSS 05 yang berfokus pada menejemen control keamanan system informasi terdapat beberapa pernyataan, pada DSS 01 yaitu sub domain mengenai manajemen jaringan yang terdiri dari 9 pernyataan, pada DSS 02 sub domain mengenai informasi yang diproses ,disimpan dan dikirim oleh perangkat endpoint yang dilindungi yang terdiri dari 3 pernyataan, DSS 03 sub domain identifikasi hak akses yang terdiri dari 6 pernyataan, DSS 04 domain yang berisi tentang tindakan fisik yang telah diterapkan untuk informasi dari akses yang illegal terdiri dari 4 pernyataan, DSS 05 doamin mengenai data yang sensitive misalnya keuangan sudah diamankan dengan baik dan disimpan, dikirim atau dihancurkan 5 pernyataan.

Penghitungan Nilai Kematangan

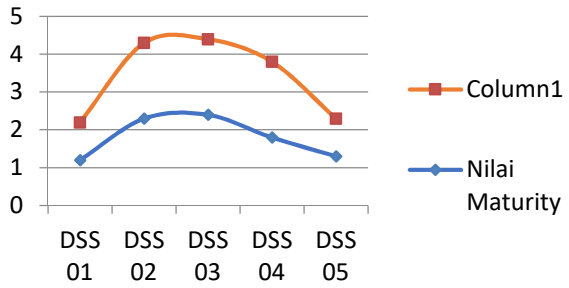
Nilai kematangan (*maturity level*) diperoleh dengan dengan menghitung setiap jawaban yang diberikan oleh responden dikalikan dengan setiap jawaban yang diberikan oleh responden dikalikan dengan setiap jawaban yang telah ditentukan kemudian dibagikan dengan total pertanyaan.

$$\text{Nilai Maturity} = \frac{\sum(\text{JawabanxBobot})}{\sum \text{Pertanyaan}} \qquad (1)$$

Dari hasil maturity tersebut kemudian diperoleh level dari system tersebut yaitu level 0 sampe dengan level 5. Hasil dari perhitungan kuisioner terdapat pada Tabel 3.

Tabel 3. Hasil pengolahan kuisioner pada domain APO

Hasil	Nilai Maturity	Level
APO13 1	1.2	1
APO13 2	2	2
APO13 3	1	1
Rata - rata	1.4	1

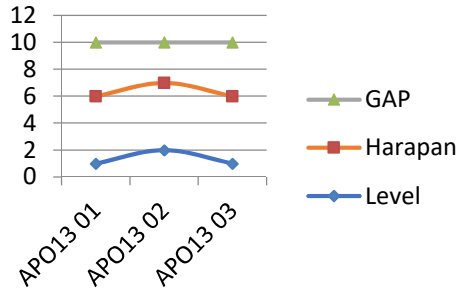


Gambar 3. Grafik nilai maturity APO

Dari Tabel 3 diperoleh hasil rata-rata nilai *maturity* pada domain APO13 yaitu 1.4, APO13 01, APO13 02 dan APO13 03 semua proses ini berada level 1 yaitu *Performed Process* dimana proses diimplementasikan untuk mencapai tujuan bisnisnya Yang artinya proses hanya sebatas dijalankan saja tetapi belum ada pendokumentasian, pengontrolan serta perbaikan.
APO13 01 membahas manajemen kemanan sistem informasi, APO13 02 domain yang menitikberatkan pada perencanaan security dan penanganan resiko IT. APO13 03 adalah domain yang membahas Adanya monitor dan review keamanan yang sedang berjalan. Sehingga dapat ditarik kesimpulan bahwa keamanan sistem informasi sudah memiliki manajemen, perencenaan *security*, tetapi belum ada antisipasi penanganan resiko dan belum adanya monitor dan review yang dilakukan.

Tabel 4. Hasil pengolahan kuisioner pada domain DSS 05

Domain	Nilai Maturity	Level
DSS 01	1.2	1
DSS 02	2.3	2
DSS 03	2.4	2
DSS 04	1.8	2
DSS 05	1.3	1
Rata-rata	1.8	1.6



Gambar 4. Grafik nilai *maturity* DSS05

Dari Tabel 4. diatas dapat dilihat bahwa secara keseluruhan rata-rata nilai *maturity*-nya adalah 1.8 yang berada dilevel 2. Skor tertinggi terdapat pada domain DSS 03 yaitu 2.4 yang termasuk pada level 2, kemudian pada DSS 02 nilai maturity nya 2.3 yang juga berda dilevel 2, DSS 04 dengan nilai maturity 1.8 berada pada level 2, pada DSS 05 diperoleh nilai maturity 1.3 berada dilevel 1, skor terendah pada DSS 01 yaitu 1.2 yang berada pada level 1. Berikut penjelasan secara rinci mengenai domain-domain dari nilai *maturity* dengan level yang tertinggi ke level yang terendah.

a. Pada DSS 03 domain mengenai hak ases yang berada pada level 2 (*managed process*) yang menunjukkan pada identifikasi hak akses yang sudah direncanakan, dominator dan disesuaikan hanya saja belum terlaksana secara optimal. Dalam hal ini hak akses sudah dibatasi untuk 1 orang hanya memilki 1 akun saja, jika terjadi kesalahan memasukkan password maka akan diblokir dan untuk membuka blokir user wajib membuat surat permohonan reset password, hanya saja dalam hal pengaksesan jaringan banyak yang masih melakukan akses diluar jam kerja. Mengingat Perguruan Tinggi XX ada institusi pendidikan yang jam kerja senin sampe dengan jum'at dengan *office hour* jam 7 sampe dengan jam 3 sore, masih terdapat pengguna yang mengkakses diluar dari jam tersebut.
b. DSS 02 domain mengenai informasi yang diproses ,disimpan dan dikirim oleh perangkat endpoint yang dilindungi memiliki nilai maturity 2.3 yang berada pada level 2 *Managed process* (dua atribut), Proses yang telah dijelaskan sebelumnya sekarang diimplementasikan dengan cara yang dikelola (direncanakan, dipantau dan disesuaikan) dan produk kerjanya ditetapkan dengan tepat, dikendalikan dan terawat sehingga dapat diambil kesimpulan bahwa perpindahan informasi baik dari segi penyimpanan ataupun pengiriman sudah dilakukan dengan baik yang sesuai dengan ketentuan hanya saja baru sekedar terlaksana namun belum ada pendokumentasian secara lengkap.
c. Pada DSS 04 juga berada pada level 2 *Managed process* yaitu proses tindakan fisik yang telah diterapkan untuk informasi dari akses yang ilegal tidak dibenarkan. Dalam hal ini hanya staf-staf tertentu yang dapat mangakses asset fisik TI

misalnya mengecek server, melakukan maintenance maupun melakukan perbikan harus melalui pihak terkait, tidak dibenarkan divisi yang tidak berkaitan untuk masuk atau mengecek fasilitas IT terutama server, namun untuk proses pengecekan siapa yang terakhir mengecek belum *terecord* atau belum ada pendokumentasian akun mana yang login terakhir sehingga tidak bisa dilacak.

d. Pada DSS 05 berada pada level 1 *Performed Process* (satu atribut), Proses yang diimplementasikan mencapai tujuan prosesnya dengan nilai *maturity* 1,3. Informasi ini menunjukkan bahwa informasi elektronik bisa diakses, dikirim dan diamankan sesuai dengan tujuan hanya saja baru sampai pada tahap terlaksanan belum ada pembuatan standarisasi bagaimana proses yang benar dan pengukuran informasi tersebut sudah valid atau tidak. Penyimpanan sudah disesuaikan dengan tahun namun belum ada pelaporan secara rinci mengenai jumlah dokumen dan setiap berapa tahun diadakan penghancuran, serta belum adanya ketetapan pembaharuan database setiap tahunnya.

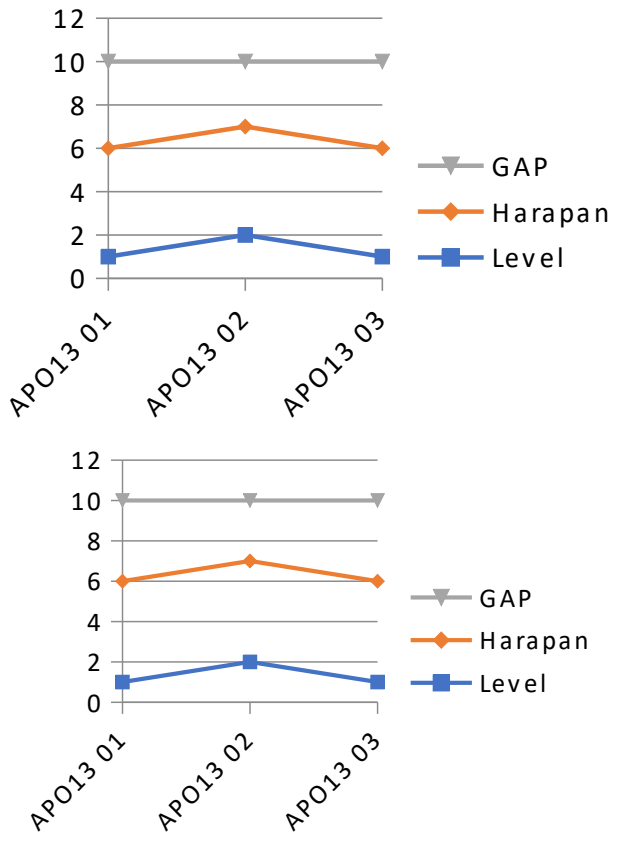
e. Skor terendah diperoleh dari hasil DSS 01 tentang kebutuhan jaringan komunikasi yang juga berada pada level 1 Performed Process. Pada domain DSS 01 terlihat bahwa sistem sudah memiliki antivirus hanya saja pendeteksian virus yang masih belum optimal, belum terlihat apakah anti virus yang digunakan sudah mampu mengatasi virus yang ada , anti virus yang belum ter *up to date* secara otomatis, belum terdapat SOP pengelolaan jaringan secara rinci, sehingga ketika ada data yang hilang belum ada solusi agar bisa mengembalikan data tersebut dalam waktu singkat , belum tersedia *back up* secara otomatis.

Analisis Nilai Kesenjangan

Dalam peneltian ini setelah didapat nilai *maturity* selanjutnya akan dianalisis dengan melihat nilai kesenjangan. Nilai kesenjangan adalah perbandingan nilai yang diperoleh dengan nilai yang diharapkan. Hasil dari nilai kesenjangan (GAP) terlihat pada Tabel 5 pada domain APO13 dan Tabel 6 pada domain DSS 05.

Tabel 5. Hasil pengolahan kuisioner pada domain APO

Domain	Level	Harapan	GAP
APO13 01	1	5	4
APO13 02	2	5	3
APO13 03	1	5	4
Rata-rata	1.3	5	3.6



Gambar 5. Grafik nilai GAP APO

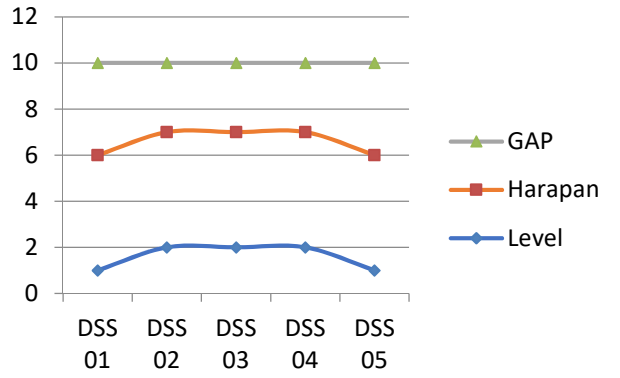
Dari Table 5. diperoleh hasil rata-rata yaitu 1.3 yang artinya hasil dari nilai maturity berada pada level 1 Performed Process dengan nilai harapan berada pada level 5 sehingga diperoleh nilai kesenjangan atau GAP 4. Rentang nilai ini menunjukkan bahwa nilai saat ini dan nilai yang diharapkan masih sangat jauh, sehingga dapat ditarik kesimpulan bahwa proses keamanan yang dilakukan masih sangat kurang dan perlu perbaikan.

Pada APO13 menunjukkan keamanan sistem informasi seharusnya mempunya standarisasi atau

penetapan, pemeliharaan, manajemen keamanan (ISMS), namun dalam hal ini standarisasi tersebut belum terlihat sehingga dalam pelaksanaannya ketika terjadi resiko dalam hal keamanan belum ada *treatment plan* yang bias dilakukan, selain tidak ada standarisasi tentunya belum dilakukan monitoring dan evaluasi system keamanan tersebut.

Tabel 6. Nilai Kenjangan pada domain DSS 05

Domain	Level	Harapan	GAP
DSS 01	1	5	4
DSS 02	2	5	3
DSS 03	2	5	3
DSS 04	2	5	3
DSS 05	1	5	4
Rata – rata	1.6	5	3.4



Gambar 6. Grafik nilai GAP DSS05

Pada table 6. diperoleh level rata-rata pada domain DSS adalah 1.6 yang artinya berada pada level 2 sedangkan nilai yang diharapkan yaitu berada pada level 5 , sehingga diperoleh nilai kesenjangan 3. Nilai GAP ini memberikan gambaran bahwa pelaksanaan sesuai dengan standar Cobit 5 pada domain DSS masih jauh dari yang diharapkan bahkan belum mencapai nilai 50 % terlaksana.

Pada DSS05 1 yaitu pengelolaan jaringan dan keamanan konektifitas sudah terlaksana namun bandwit yang tersedia masih belum optimal yang mengakibatkan kegagalan akses. Pada domain DSS05 2 pengelolaan keamanan endpoint belum diterapkan belum ada jaminan bahwa dengan system keamanan yang ada semua data dapat tersimpan dan terbebas dari virus.

Pada domain DSS05 3 pengelolaan identitas user dan Akses logic sudah ada namun ketersediaan layanan yang berkelanjutan belum ada, contohnya akses yang seharusnya hanya berlaku dijam kerja namun pada prakteknya akses dapat dilakukan 24 jam selama meskipun diluar jam kerja.

DSS05 4 pengelolaan akses fisik terhadap asset TI juga masih jauh dari target, dalam cobit 5 seharunya adanya *maintenance* secara berkala baik *maintenance* software maupun *maintenance* infrastruktur teknologi, belum adanya prosedur untuk memberikan, membatasi, dan mencabut hak akses dalam gedung dan area sesuai dengan kebutuhan termasuk antipasti dalam keadaan darurat. Domain DSS05 5 pengelolaan dokumen sensitif dan perangkat output belum dibedakan belum terlihat pengklasifikasian dokumen rahasia maupun dokumen biasa, yang seharusnya jika terdapat dokumen rahasia memilki tempat khusu dan harus dilakukan penghancuran dalam kurun waktu tertentu.

Menyusun Rekomendasi

Hasil perhitungan maturity level, kemudian analisis kematangan , sehingga diperoleh nilai kesenjangan atau GAP. Perolehan nilai kesenjangan (GAP) pada domain APO yang terdapat pada Table 5, dan perolehan nilai kesenjangan pada domain DSS yang terdapat pada Table 6 diatas diperoleh rekomendasi sebagai berikut:

a. Adanya pedoman standarisasi atau penetapan, pemeliharaan, manajemen keamanan (ISMS), sehingga dengan pedoman tersebut dapat dilakukan treatmen plan atau antisipasi jika terjadi resiko yang selanjutnya dapat menjadi laporan monitoring dan evaluasi sistem keamanan.
b. Dibuatkan pelaporan berkala tentang pelaksanaan keamanan informasi, perpindahan informasi dan penggunaan hak akses sehingga lebih jelas bagian mana yang berhak mengakses dan melakukan perpindahan.
c. Dibuatkan tempat penyimpanan dokumen kerahasiaan yang terintegrasi sehingga data yang sudah tidak dibutuhkan dapat dimusnahkan dan dibuatkan berita acara pemusnahan setiap dokumen yang bersifat rahasia.
d. System keamanan memiliki anti virus yang mumpuni yang selalu ter update secara otomatis.
e. Dibuatkan SOP pengontrolan dan evaluasi keamanan sistem sehingga dapat terlihat sisi mana yang sudah tercapai dan yang belum

tercapai. Dilakukan pengecekan secara berkala baik ketika ada kendala maupun tidak.

f. Dibuatkan laporan *maintenance* secara berkala baik *maintenance software* maupun maintenance infrastruktur teknologi.
g. Dibuatkan laporan *monitoring review* keamanan sistem yang sedang berjalan, sehingga dapat digunakan untuk pelaksanaan monitoring berikutnya.

KESIMPULAN

Berdasarkan analisis yang dilakukan menggunakan *framework* Cobit 5 diperoleh rata-rata nilai kematangan pada domain APO 13 yaitu 1,3 yang berada dilevel 1,dengan GAP 3,6 ini menunjukkan bahwa sistem keamanan pada Perguruan ini masih jauh dari target yang diharapkan. APO13 adalah bagian dari Cobit 5 yang memilki standarisasi adanya menajemen proses pada keamanan sistem informasi seharusnya memiliki *information security management system (ISMS)* namun pada Perguruan XX ini belum terdapat sistem keamanan yang optimal, direkomendasikan dibentuk ISMS , kemudian sistem keamanan tersebut dapat dibuat *treatmant plan*, selanjutnya dimonitor dan direview dengan review tersebut dapat dilakukan perbaikan untuk kedepannya. Begitu pula pada domain DSS05 diperoleh rata-rata nilai kematangan 1,6 yang berada pada level 2 dengan GAP 3,4.

Hal ini juga menunjukkan dari sisi *operation* manajemen yang baru berjalan kurang dari 50 %, sehingga pada domain ini juga perlu dilakukan perbaikan. Dari hasil analisis diperoleh rekomendasi untuk dipasang anti virus yang mumpuni yang selalu ter *update* secara otomatis, dengan sistem akses yang sudah terintegrasi perbidang pada divisi masing-masing yang dapat ter-*record* sehingga dalam melakukan perbaikan cukup pada divisi yang bermasalah saja. Perlu dilakukan *maintenance* secara berkala baik *hardware* maupun pada *software* sehingga jika terjadi resiko kegagalan IT tidak berakibat fatal yang dapat merugikan perguruan tinggi baik secara waktu maupun materi.

UCAPAN TERIMA KASIH

Terima kasih kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini. Dukungan dan kerja sama yang baik dari divisi TSI (teknologi Sistem Informasi) Perguruan Tinggi XX yang antusias dalam pengisian kuesioner, wawancara serta bersedia menyediakan waktunya dalam berbagi informasi mengenai Tata Kelola TI yang diterapkan pada Perguruan Tinggi XX. Terimakasih kepada seluruh tim redaksi Media Informatika Budidarma yang telah membantu dan mengarahkan hingga terbitnya artikel ini.

DAFTAR PUSTAKA

[1] C. Vehicles, "Jurnal Computer Science and Information Technology (CoSciTech)," vol. 1, no. 2, pp. 57–64, 2020.

[2] Y. Supit, S. S. Kusumawardani, and W. W. Winarno, "Kajian Framework Cobit 5 Untuk Pengukuran Keamanan," no. September, pp. 113–117, 2015.

[3] F. A. Gunadi, A. Wibowo, and I. Gunawan, "Audit Keamanan Sistem Informasi IT Di PT X," *J. Infra*, no. 031, 2015, [Online]. Available: http://publication.petra.ac.id/index.php/teknik-informatika/article/view/3257.

[4] R. D. Krisdiyawan and R. B. H. Kuswantoro, "Audit Keamanan Sistem Informasi Pada Rs Mata Dr. Yap Yogyakarta Menggunakan Framework Cobit 5, Vol. 1, no. September, 2017, [Online]. Available: http://ojs.mmtc.ac.id/index.php/jimik/article/view/44.

[5] E. Ekowansyah, Y. H. Chrisnanto, and P. N. Sabrina, "Audit Sistem Informasi Akademik Menggunakan COBIT 5 di Universitas Jenderal Achmad Yani," *Pros. Semin. Nas. Komput. dan Inform. 2017 (ISBN 978 - 602 - 60250 - 1 -2)*, vol. 2017, pp. 201–206, 2017, [Online]. Available: http://www.senaski.unikom.ac.id/prosiding-file/201-206 erdis ekowansyah dkk 6 hal.pdf.

[6] F. Febrianto and D. I. Sensuse, "Evaluasi keamanan informasi menggunakan ISO / IEC 27002 : studi kasus pada Stimik Tunas Bangsa Banjarnegara," *Infokam*, vol. 2, no. 2013, pp. 21–27, 2017.

[7] J. Teknik Komputer STMIK AMIK Bandung Jl Jakarta, "Penilaian Tata Kelola Keamanan Informasi Perpustakaan dengan Framework Cobit 5 Studi Kasus Dinas Perpustakaan dan Arsip Kota Bandung Yoki Muchsam," no. September, 2017, [Online]. Available: http://dispusip.bandung.go.id.

[8] I. J. Aritonang, E. D. Udayanti, and N. Iksan, "Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (Apo13)," *Inf. Technol. Eng. Journals*, vol. 03, no. 02, pp. 3–7, 2018.

[9] ISACA, *COBIT ® Process Assessment Model (PAM): Using COBIT ® 5*. 2013.

[10] Heru pratama, "Audit Keamanan Sistem Informasi Pada Kantor Samsat Di Kota Krui Menggunakan Cobit 5," vol. 2015, no. Sentika, 2018.
[11] B. P. Santoso, E. Hariyanti, and E. Wuryanto, "Penyusunan Panduan Pengelolaan Keamanan Informasi Untuk Firewall Configuration Berdasarkan Kerangka Kerja PCI DSS v.3.1 dan COBIT 5," *J. Inf. Syst. Eng. Bus. Intell.*, vol. 2, no. 2, p. 67, 2016.
[12] COBIT 5, "COBIT 5: Process Assessment Model (PAM)," *Isaca*, p. 144, 2013, [Online]. Available: https://drive.google.com/folderview?id=0B9yuuoKpwX3MczducjREdEhqdTA&usp=sharing.