Information Security Audit *Analysis on Cloud Providers Using* ISO/IEC 27017:2015 *at* PT.XYZ

1st Falea Amira Nafisa
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
faleanafisa@student.telkomuniversity.ac.id

2nd Rahmat Yasirandi
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
rahmat.yasirandi@telkomuniversity.ac.id

3rd Rio Guntur Utomo
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
riogunturutomo@telkomuniversity.ac.id

Abstrak—Meningkatnya penggunaan cloud menyebabkan cloud service provider (CPS) untuk memiliki keamanan informasi yang tinggi. Karena kemudahan akses yang diberikan pada penyimpanan cloud sangatlah rentan karena semua data berada di internet. Saat ini pada studi kasus yaitu perusahaan swasta yang bergerak dibidang cloud service provider (CPS) tentulah memerlukan standar khusus untuk sistem keamanan cloud juga dalam mengambil keputusan baik data ataupun informasi yang ada, karena akan berdampak fatal bagi instansi/perusahaan. Saat ini studi kasus sudah memiliki standar keamanan, akan tetapi diperlukannya keamanan informasi dan regulasi baik pada pihak penyedia dan pengguna layanan cloud dengan dilakukannya analisis dan audit keamanan informasi pada cloud di PT.XYZ. Serta membuat hasil rekomendasi dari hasil evaluasi audit.

Kata Kunci—ISO 27017, Cloud Service Provider, Cloud Computing, CPS

Abstract—*The increasing use of cloud computing causes cloud service providers (CPS) to have high information security. Because of the ease of access given to cloud storage, it is very vulnerable because all data is on the internet. Currently, a private company engaged in cloud service provider (CPS), as the study case, requires particular standards for cloud security systems and in making data along with informed decisions because it will have a fatal impact on the agency/company. Currently, the case studies already have security standards. However, information security controls and regulations are needed both on the part of providers and users of cloud services by conducting analysis and auditing of information security on the cloud at PT.XYZ. Furthermore, make recommendations based on the results of the audit evaluation.*

Keyword—ISO 27017, Cloud Service Provider, Cloud Computing, CPS

I. PENDAHULUAN

Penggunaan teknologi cloud computing merupakan salah satu inovasi paling menarik dan menantang di bidang teknologi informasi, karena penyediaan elastis, fleksibel juga metode penyimpanannya sesuai dengan permintaan dan menyediakan layanan komputasi pada pelanggan [1]. CAGR atau tingkat pertumbuhan per tahun selama 2021 – 2028 dari market size serta pendapatan bersama dari permintaan cloud computing secara global adalah sebesar 15,80% yang menandakan akan adanya peningkatan penggunaan cloud computing [1]. Sedangkan market size & shared revenue cloud computing di Indonesia diperkirakan meningkat dengan tingkat pertumbuhan per tahun selama 2021 – 2028 sebesar 28-33% [2].

GAMBAR 1.1
MARKET SIZE CLOUD COMPUTING DI INDONESIA

Hal tersebut menandakan bahwa adopsi cloud computing meningkat tiap tahunnya berdasarkan hasil forecast global dan di Indonesia. Pernyataan ini dikuatkan dengan kehadiran banyaknya Cloud Service Provider (CSP) di Indonesia seperti Telkomsigma, Zettagrid Indonesia, CBN Cloud dan masih banyak CSP lainnya.

Ketua Asosiasi Cloud Computing Indonesia (ACCI) Alex Budiyanto mengatakan, sebanyak 32 persen responden tidak mengadopsi sistem komputasi awan karena mereka beralasan masih khawatir mengenai akses, kontrol data dan keamanan data [3]. Isu seperti keamanan data, kebocoran informasi, hak akses, privasi dan hal terkait menjadi sorotan dalam keamanan informasi yang menjadi kekhawatiran pelanggan layanan cloud/cloud service customer (CSC)[4].

Kekhawatiran/keraguan dalam penggunaan cloud dapat menyebabkan ketidak percayaan terhadap kedua pihak baik CSC dan CSP yang mengimplementasikan cloud[5]. Hal tersebut dapat dihindari dengan meningkatkan kepercayaan CSC oleh CSP dengan mematuhi standar keamanan informasi ISO/IEC 27001: 2013[6]. Untuk memastikan ISO/IEC 27001 dipatuhi oleh CSP, panduan dalam mengimplementasi keamanan informasi disampaikan pada dokumen ISO/IEC 27002:2013. Peningkatan keamanan informasi pada cloud service provider dapat dilakukan dengan standar kendali keamanan ISO/IEC 27017:2015 yang merupakan standar keamanan tambahan pada layanan cloud yang menjadi referensi tambahan dari ISO/IEC 27001:2013 dan disampaikan dengan format yang sama dengan ISO/IEC 27002:2013.

Sehingga fokus pada penelitian ini adalah membantu perusahaan dalam meningkatkan keamanan informasi terhadap penyedia layanan cloud, dengan harapan dapat menyelesaikan isu keamanan informasi yang ditakutkan oleh pelanggan layanan cloud/calon pelanggan. Hal tersebut dapat dicapai dengan penerapan standar keamanan informasi menggunakan ISO/IEC 27017:2015, karena ini merupakan standar tambahan yang di khususkan untuk penyedia layanan cloud dari standar keamanan sebelumnya yaitu 27002.

Analisis audit keamanan informasi ini dilakukan pada studi kasus CSP PT. XYZ menggunakan ISO/IEC 27017:2015. Karena, perusahaan belum mengadopsi standar kendali keamanan tambahan untuk penyedia layanan cloud dan sebagai persiapan perusahaan untuk melakukan audit pada tahun 2023. Dalam analisis ini, peneliti juga menggunakan pengukuran Capability Maturity Model Integration (CMMI) serta mengetahui kesenjangan (gap) perusahaan dengan ISO/IEC 27017:2015.

A. Topik dan Batasannya

Berdasarkan latar belakang di atas, berikut merupakan rumusan masalah yang akan di evaluasi oleh penulis yaitu, bagaimana menganalisis keamanan informasi cloud yang diterapkan oleh PT.XYZ dan menganalisis gap berdasarkan ISO/IEC 27017:2015. Kemudian menentukan berapakah maturity level pada kebijakan keamanan informasi cloud yang diterapkan pada penyedia layanan cloud PT.XYZ. Selain itu peneliti juga menentukan bagaimana rekomendasi yang dapat diberikan dari hasil analisis audit yang sudah dilakukan pada penyedia layanan cloud PT. XYZ.

B. Tujuan

Mengacu terhadap rumusan masalah, tujuan dari penulisan ini yaitu menganalisis keamanan informasi dan gap yang ada agar sesuai dengan ISO/IEC 27017:2015, melakukan pengukuran dan menetukan tingkat maturity level dari keamanan informasi cloud yang dimiliki sehingga dapat memberikan rekomendasi dari keamanan informasi cloud yang dimiliki oleh PT. XYZ berdasarkan ISO/IEC 27017:2015 sehingga nantinya dapat digunakan untuk persiapan audit pada tahun 2023.

II. KAJIAN TEORI

A. ISO 27017

Merupakan salah satu bagian dari ISO 27000 standards family yang merupakan framework penerapan ISMS. Dokumen dengan judul *"Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services"* menjelaskan tentang aspek keamanan informasi dan rekomendasi penerapan kontrol keamanan informasi tambahan khusus untuk penyedia layanan *cloud*. [12]

Pada standar ini memberikan panduan berbasis keamanan informasi pada 37 kontrol dari ISO 27017 berasarkan lanjutan dari ISO 27002. Terdapat 2 (dua) kontrol baru serta 7 (tujuh) kontrol objektif baru yang membahas peran dan tanggung jawab bersama, pemantauan aktivitas layanan *cloud*, penyelarasan manajemen keamanan lingkungan jaringan *virtual* dan *cloud.*

B. Gap Analysis

Berdasarkan *Information Technology Infrastructure Library (ITIL), gap analysis* merupakan aktivitas membandingkan dua macam data dan identifikasi perbedaannya.

Menurut Pol dan Paturkar (2011), *Fit/Gap Analysis (FGA)* adalah metodologi yang digunakan untuk membandingkan proses bisnis dengan fungsi sistem dimana akan di lakukan evaluasi dan di urut kan prioritas nya untuk melihat pencapaian apakah terjadi kecocokan *(Fit)* dan kesenjangan *(Gap)*[13].

Sehingga dapat disimpulkan bahwa *gap analysis* digunakan untuk evaluasi kinerja pengelolaan manajemen internal perusahaan dan sebagai alat bantu mengukur kualitas perusahaan. Dalam penelitian ini gap analysis digunakan untuk mengidentifikasi kesenjangan antara kondisi perusahaan saat ini dengan standar keamanan yang ingin dicapai serta standar keamanan yang ingin diadopsi yaitu ISO/IEC 27017.

C. Capability Maturity Model Integration (CMMI)

COBIT 2019 CMMI mendefinisikan 6 level kapabilitas yang dapat diterapkan oleh organisasi untuk model tingkat kapabilitas dan kematangan mulai dari level 0 *(incomplete)* hingga *level 5 (optimizing).* Tingkat kapabilitas digunakan untuk mengukur seberapa baik suatu proses di implementasi kan dan kinerjanya. Sedangkan tingkat kematangan digunakan untuk mengetahui keberadaan pencapaian yang ada dan memberikan informasi peningkatan[15]. Penjelasan terkait setiap *level* CMMI [16], dijelaskan pada Tabel 2.1 berikut :

TABEL 2.1
KETERANGAN MATURITY LEVEL

Maturity Level	Keterangan
0 – Incomplete	Tidak ditemukan bukti bahwa perusahaan mengetahui adanya permasalahan yang perlu diatasi
1 – Initial	Terdapat bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Bagaimanapun juga tidak terdapat proses standar, namun menggunakan pendekatan ad hoc yang cenderung diperlakukan secara individu/per kasus. Secara umum pendekatan proses tidak terorganisir.
2 – Managed	Proses dikembangkan kedalam tahapan dimana proses sudah direncanakan, didokumentasikan dan bersifat reaktif. prosedur serupa diikuti oleh pihak-pihak yang berbeda untuk pekerjaan yang sama. Tidak terdapat pelatihan formal/mengomunikasikan prosedur, standar, dan tanggung jawab diserahkan kepada individu masing-masing. Terdapat tingkat kepercayaan yang tinggi terhadap individu sehingga memungkinkan terjadinya error yang besar.
3 – Defined	Prosedur distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan. Kemudian diamanatkan bahwa proses-proses tersebut harus diikuti. Tetapi penyimpanan tidak dapat terdeteksi. Prosedur sendiri tidak lengkap namun sudah memformalkan praktek yang berjalan.
4 – Quantitively Managed	Manajemen mengawasi dan mengukur kepatuhan terhadap prosedur dan mengambil tindakan jika proses tidak dapat dikerjakan secara efektif. Proses berada di bawah peningkatan yang konstan dan penyediaan praktek yang baik. Otomatisasi dan perangkat digunakan dalam batasan tertentu
5 – Optimizing	Proses sudah pada tingkat praktek yang baik, dan pada peningkatan perusahaan. Perusahaan sudah menggunakan hasil perbaikan untuk peningkatan kualitas dan efektivitas serta membuat perusahaan cepat beradaptasi.

III. METODE

Penelitian ini menggunakan metode kualitatif juga teknik triangulasi untuk mengumpulkan data untuk penelitian yang berasal dari wawancara, observasi dan dokumentasi. Analisis yang dilakukan menggunakan work paper gap analysis untuk menentukan gap pada penerapan ISO/IEC 27017 pada PT.XYZ dan mengukur *maturity level* pada perusahaan dengan *work paper maturity level.*

TABEL 3.1
WORKPAPER GAP *ANALYSIS*

ANNEX A	KONTROL	KONDISI	EVALUASI	KEPEMILIKAN	REKOMENDASI	NILAI KONTROL OBJEKTIF
10	CRYPTOGRAPHY					
10.1	CRYPTOGRAPHIC CONTROLS					
	OBJECTIVE *To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.*					
10.1.1	Policy on the use of cryptographic controls **KONTROL** A policy on the use of cryptographic controls for protection of information should be developed and implemented.	**KONDISI** Perusahaan belum memiliki kebijakan formal secara khusus terkait penggunaan kriptografi, pada pengimplementasiannya perusahaan belum menerapkan kriptografi pada layanan. Saat ini acuan kebijakan berada pada kebiajakn keamanan informasi **SEBAB** Perusahaan tidak menerapkan teknik kriptografi dalam pengamanan informasi layanan atau perusahaan	**GAP** Berdasarkan annex 10 kontrol objektif 10.1.1, seharusnya terdapat kebijakan terkait penggunaan kendali kriptografi untuk perlindungan informasi dikembangkan diimplementasi. Selain itu perusahaan perlu menyediakan dokumen terkait penggunaan kriptografi yang disampaikan kepada pengguna layanan **DAMPAK** -Apabila nantinya perusahaan menggunakan kriptografi dan belum adanya kendali kriptografi yang dapat dijadikan acuan maka teknik tersebut tidak optimal dipakai untuk meminimalisir risiko akibat dari insiden keamanan informasi	DIVISI *OPERATION* DAN *CYBERSECURITY*	- Apabila nantinya perusahaan menggunakan kriptografi untuk mengamankan informasi perusahaan dan layanan maka perlunya kebijakan/prosedur kendali kriptografi - Perusahaan perlu menyediakan kendali kriptografi apasaja yang diterapkan pada layanan yang diserahkan kepada CSC	1

Kemudian dari hasil Tabel 3.1, dapat dilakukan penilain menggunakan maturity level yang menggunakan cara seperti Tabel 3.2 dibawah ini.

TABEL 3.2
PENILAIAN *MATURITY* LEVEL

ANNEX A	KONTROL	PERTANYAAN	YES	NO	NILAI INDEX/KONTROL OBJEKTIF	RATA-RATA INDEX/KONTROL	RATA-RATA NILAI KLAUSUL & MATURITY LEVEL
10	CRYPTOGRAPHY						
10.1	CRYPTOGRAPHIC CONTROLS						
	OBJECTIVE *To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.*						
10.1.1	Policy on the use of cryptographic controls	Apakah kebijakan terhadap penggunaan kendali kriptografi untuk perlindungan informasi sudah dikembangkan dan diimplementasikan ?		✓	1	1	1
10.1.2	Key management	Apakah kebijakan terhadap penggunaan, perlindungan dan masa hidup kunci kriptografi sudah dikembangkan dan diimplementasikan dalam keseluruhan siklus hidupnya/life cyclenya ?		✓	1		

IV. HASIL DAN PEMBAHASAN

A. Penilaian Maturity Level

Berdasarkan hasil analisis yang digunakan *maturity level tiap annex dijelaskan pada Tabel 4.1 berikut :*

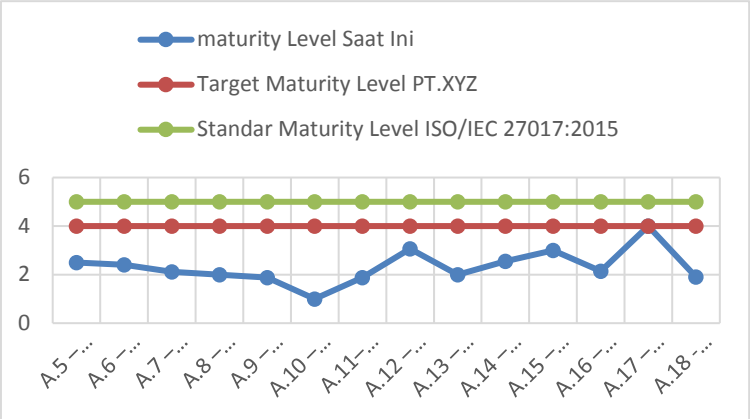
TABEL 4.1
HASIL MATURITY LEVEL TIAP ANNEX

Klausul	Level	Keterangan
5 – Kebijakan Keamanan Informasi	2,5	Managed
6 – Organisasi Keamanan Informasi	2,4	Managed
7 – Keamanan Sumber Daya Manusia	2,11	Managed
8 – Manajemen Aset	2	Managed
9 – Kendali Akses	1,88	Initial
10 – Kriptografi	1	Initial
11– Keamanan Fisik dan Lingkungan	1,88	Initial
12 – Keamanan Operasi	3,07	Defined
13 – Keamanan Komunikasi	2	Managed
14 – Akuisisi, Pengembangan dan Perawatan Sistem	2,55	Managed
15 – Hubungan Pemasok	3	Defined
16 – Manajemen Insiden keamanan Informasi	2,14	Managed
17 – Aspek Keamanan Informasi dari Manajemen Keberlangsungan Bisnis	4	Quantitively Managed
18 - Kesesuaian	1,9	Initial
Rata-Rata	**2,317**	**Managed**

B. Hasil Analisis dan Rekomendasi Perbaikan

Berdasarkan hasil analisis yang sudah dilakukan terhadap gap dan maturity level maka peneliti dapat menggambarkan sejauh mana cloud service provider (CSP) sudah menerapkan keamanan informasi berdasarkan ISO/IEC 27017:2015 pada Tabel 4.5. Hasil dari analisis dan penilaian ini akan digambarkan dengan grafik, sekaligus memberikan rekomendasi perbaikan sehingga perusahaan dapat mengadopsi standar keamanan informasi yang ditunjukkan untuk cloud provider.

Grafik ini digunakan untuk membandingkan antara maturity level perusahaan saat ini dengan maturity level yang ingin dicapai dan Standar ISO 27017:2015 oleh CSP PT.XYZ. Berdasarkan komalasari dan perdana (2014), perusahaan pada umumnya mempunyai keamanan informasi dengan maturity level 3. Pada saat melakukan wawancara dengan perwakilan karyawan perusahaan, cloud service provider (CSP) ingin memiliki nilai maturity level 4. Dengan begitu grafik maturity level ini dapat menunjukan posisi gap antara maturity level perusahaan dengan standar keamanan dan target yang akan dicapai.



GAMBAR 4.1
GRAFIK MATURITY LEVEL SETIAP ANNEX

Gambar 4.1 menjelaskan bahwa maturity level dari setiap annex yang didapat dibandingkan dengan standar tingkat maturity level dari ISO/IEC 27017:2015 (level 5), tingkat maturity level yang diinginkan perusahaan (level 4), dan maturity level perusahaan saat ini (level 2).

V. KESIMPULAN

Hasil analisis menggunakan ISO/IEC 27017:2015 dan maturity level yang dilakukan terhadap CSP PT. XYZ, maka dapat disimpulkan sebagai berikut:

1. Pada CSP PT. XYZ keamanan informasi yang diterapkan sudah sesuai dengan standar ISO/IEC 27017:2015. Dari 121 kontrol objektif, PT. XYZ sudah menerapkan 97 objektif kontrol atau sebesar 80,16% dengan level maturity level 2 (Managed).
2. Proses pada perusahaan sudah direncanakan, didokumentasikan tetapi bersifat reaktif. Prosedur juga sudah diikuti oleh pihak-pihak yang berbeda untuk pekerjaan yang sama. Tidak terdapat pelatihan formal/sosialisasi prosedur/standar, dan tanggung jawab diserahkan kepada individu masing-masing.
3. Berdasarkan hasil maturity level dan gap pada keamanan informasi cloud service provider (CSP) PT. XYZ dapat disimpulkan:
   a. Keamanan Informasi pada CSP PT. XYZ dengan nilai annex yang kecil, yaitu:
      A.5-A.16 dan A.18.
      Prosedur tidak lengkap dan hilang walaupun implementasi sudah hampir sesuai.
   b. Keamanan Informasi pada CSP PT. XYZ dengan nilai annex yang besar, yaitu:
      a) A.17–Aspek Keamanan Informasi dari Manajemen Keberlangsungan Bisnis, level 4 (Quantitively Managed)

REFERENSI

[1] Facts & Factors, “Demand for Global Cloud Computing Market Size & Share to Surpass USD 1025.7 Bn by 2028, Exhibit a CAGR of 15.80% | Cloud Computing Industry Trends, Dynamics, Growth, Value, Analysis & Forecast Report by Facts & Factors,” 2022. [Online]. Available: https://www.globenewswire.com/en/news-release/2022/06/22/2467017/0/en/Demand-for-Global-Cloud-Computing-Market-Size-Share-to-Surpass-USD-1025-7-Bn-by-2028-Exhibit-a-CAGR-of-15-80-Cloud-Computing-Industry-Trends-Dynamics-Growth-Value-Analysis-Forecast.html

[2] G. Research, “Indonesia Cloud Computing Market Share, Size, Growth & Industry Report, 2021-2028,” 2021, [Online]. Available: https://www.gmiresearch.com/report/indonesia-cloud-computing-market-share-size-growth-industry/#:~:text=Introduction of the Indonesia Cloud,period (2021-2028).

[3] Mediana, “Pemanfaatan ”Cloud” Kian Marak, Layanan Diharapkan Semakin Baik,” 2022. https://www.kompas.id/baca/ekonomi/2022/02/16/pemanfaatan-cloud-kian-marak-layanan-diharapkan-semakin-baik?track_source=baca&track_medium=login-paywall&track_content=https%3A%2F%2Fwww.kompas.id%2Fbaca%2Fekonomi%2F2022%2F02%2F16%2Fpemanfaatan-cloud-kian-ma

[4] W. a. Pauley, “Cloud Provider Transparency,” Security, vol. 8, no. December, pp. 32–39, 2010, [Online]. Available: http://ieeexplore.ieee.org/iel5/8013/5655229/05551112.pdf?arnumber=5551112

[5] S. Majumdar et al., “Security compliance auditing of identity and access management in the cloud: Application to OpenStack,” Proceedings - IEEE 7th International Conference on Cloud Computing Technology and Science, CloudCom 2015, pp. 58–65, 2016, doi: 10.1109/CloudCom.2015.80.

[6] C. di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. Campbell, and M. N. Bashir, “IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers,” Proceedings - 2017 17th IEEE/ACM International Symposium on Cluster,

Cloud and Grid Computing, CCGRID 2017, pp. 1090–1099, 2017, doi: 10.1109/CCGRID.2017.137.
[7] S. Manvi and G. K. Shyam, “Cloud Computing; Concepts and Technologies.”
[8] IEEE, “IEEE Cloud Computing”.
[9] C. Surianarayanan and P. R. Chelliah, Essentials of Cloud Computing: A Holistic Perspective. 2019.
[10] Michael E. Whitman and H. J. Mattord, Management of Information Security, 3rd Edition. 2010.
[11] I. Sarno, Riyanto ; iffano, Sistem Manajemen Keamanan Informasi. ITS Press, 2009.
[12] “Information technology-Security techniques-Code of practice for information security controls based on ISO/IEC 27002 for cloud services.”
[13] M. . Pol, Prakash; Paturkar, “Methods of Fit Gap Analysis in SAP ERP Projects,” 2011.
[14] P. D. Syafitri, “Penilaian kualitas pengembangan sistem informasi pada perusahaan distributor,” IQRA`: Jurnal Ilmu Perpustakaan dan Informasi (e-Journal), vol. 10, no. 1, pp. 15–27, 2016, [Online]. Available: http://jurnal.uinsu.ac.id/index.php/iqra/article/view/124
[15] C. Emeka Elue, CISA, “Effective Capability and Maturity Assessment Using COBIT 2019,” 2020. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2020/effective-capability-and-maturity-assessment-using-cobit-2019#4
[16] CMMI, “CMMI Levels of Capability and Performance.” [Online]. Available: https://cmmiinstitute.com/learning/appraisals/levels
[17] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta, 2007.
[18] Nana Syaodih Sukmadinata, Metode Penelitian Pendidikan. Bandung: PT Remaja Rosdakarya, 2017.
[19] R. Mita, “Wawancara Sebuah Interaksi Komunikasi Dalam Penelitian Kualitatif,” Jurnal Ilmu Budaya, vol. 11, no. 2. pp. 71–79, 2015. [Online]. Available: https://media.neliti.com/media/publications/100164-ID-wawancara-sebuah-interaksi-komunikasi-da.pdf
[20] A. Z. Maingak, “Asesmen Keamanan Informasi Menggunakan Standar ISO/IEC 27001:2013 Pada Institusi Pemerintah X”.
[21] Luis Gorgona, “Building a Maturity Model for COBIT 2019 Based on CMMI,” vol. 6, pp. 2019–2021, 2021, [Online]. Available: https://www.isaca.org/resources/cobit