Dokumen Audit Keamanan Website Silaturahmi
Universitas Pembangunan Nasional "Veteran"
Jawa Timur
Menggunakan COBIT 2019

Dosen Pengampu

Afina Lina Nurlaili S.Kom., M.Kom

Disusun Oleh:

Niko Priyo Prakoso 22081010276

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR
2025

Abstrak

Website SILATURAHMI UPN “Veteran” Jawa Timur merupakan platform kolaborasi yang mendukung keterhubungan antara mahasiswa, alumni, sivitas akademika, dan mitra industri dalam rangka implementasi kebijakan Merdeka Belajar Kampus Merdeka (MBKM). Sebagai sistem yang mengelola data pribadi dan informasi penting pengguna, Website SILATURAHMI memiliki risiko keamanan informasi yang perlu dikelola secara sistematis dan terukur.

Penelitian ini bertujuan untuk menyusun dan melaksanakan audit keamanan sistem informasi pada Website SILATURAHMI menggunakan framework COBIT 2019. Audit difokuskan pada pemetaan Enterprise Goals (EG), IT-Related Goals (ITG), serta domain COBIT 2019 yang relevan, yaitu APO12 (Manage Risk), APO13 (Manage Security), DSS05 (Manage Security Services), dan MEA03 (Monitor Compliance). Metode audit dilakukan melalui penyusunan tujuan audit dan pertanyaan audit yang digunakan sebagai instrumen evaluasi terhadap pengelolaan keamanan, manajemen risiko, dan kepatuhan regulasi.

Hasil dari audit ini diharapkan mampu memberikan gambaran tingkat kapabilitas pengelolaan keamanan TI, mengidentifikasi potensi kelemahan (gap) dalam pengendalian keamanan, serta menghasilkan rekomendasi perbaikan yang dapat diterapkan untuk meningkatkan keamanan Website SILATURAHMI secara berkelanjutan. Dengan penerapan COBIT 2019, diharapkan tata kelola keamanan informasi dapat berjalan selaras dengan tujuan institusi dan standar internasional.

Kata kunci: Audit Keamanan, Sistem Informasi, COBIT 2019, Manajemen Risiko TI, Keamanan Website

BAB 1. Pendahuluan

1.1 Latar Belakang

Sistem Informasi SILATURAHMI merupakan platform kolaborasi yang dikembangkan oleh UPN "Veteran" Jawa Timur untuk mendukung keterhubungan antara mahasiswa, alumni, mitra industri, dan sivitas akademika. Website ini berperan penting dalam mendukung kebijakan Merdeka Belajar Kampus Merdeka (MBKM) serta mengelola data pribadi pengguna.

Seiring meningkatnya ketergantungan terhadap sistem berbasis web dan tingginya risiko kebocoran data, diperlukan evaluasi keamanan website secara terstruktur. Oleh karena itu, audit keamanan Website Silaturahmi dilakukan menggunakan framework COBIT 2019 guna memastikan tata kelola keamanan TI berjalan efektif, risiko dapat dikendalikan, dan kepatuhan terhadap regulasi terpenuhi.

Tujuan laporan ini adalah menyajikan proses audit keamanan website Silaturahmi secara runtut berdasarkan tahapan COBIT 2019, mulai dari penentuan enterprise goals hingga penyusunan instrumen audit berbasis kuesioner skala Likert.

1.2 Identifikasi Masalah

Berdasarkan latar belakang tersebut, dapat diidentifikasi bahwa Website SILATURAHMI memiliki potensi risiko keamanan informasi yang perlu dievaluasi lebih lanjut. Pengelolaan risiko dan keamanan sistem informasi belum diketahui tingkat kematangannya secara pasti berdasarkan standar tata kelola TI yang diakui secara internasional. Selain itu, diperlukan penilaian terhadap penerapan kebijakan keamanan, layanan keamanan operasional, serta kepatuhan sistem terhadap regulasi perlindungan data dan kebijakan internal institusi.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah yang telah diuraikan, permasalahan utama dalam penelitian ini adalah bagaimana tingkat pengelolaan risiko dan keamanan sistem informasi pada Website SILATURAHMI jika ditinjau menggunakan framework COBIT 2019. Selain itu, perlu dikaji sejauh mana penerapan domain COBIT 2019 yang relevan dalam mendukung keamanan sistem informasi serta bagaimana tingkat kepatuhan Website SILATURAHMI terhadap regulasi dan standar keamanan informasi yang berlaku.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk melakukan audit keamanan sistem informasi pada Website SILATURAHMI UPN “Veteran” Jawa Timur dengan menggunakan framework COBIT 2019. Melalui audit ini, diharapkan dapat diketahui tingkat kapabilitas pengelolaan risiko dan keamanan TI, mengevaluasi kesesuaian penerapan proses keamanan dengan domain COBIT 2019 yang relevan, serta menyusun rekomendasi perbaikan guna meningkatkan keamanan dan tata kelola sistem informasi secara berkelanjutan.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini diharapkan dapat memberikan kontribusi baik secara teoretis maupun praktis. Secara teoretis, penelitian ini dapat menambah referensi dan wawasan akademik mengenai penerapan COBIT 2019 dalam audit keamanan sistem informasi, khususnya di lingkungan perguruan tinggi. Secara praktis, hasil penelitian ini dapat menjadi bahan evaluasi dan pertimbangan bagi pengelola Website SILATURAHMI dalam meningkatkan pengelolaan keamanan, manajemen risiko, serta kepatuhan terhadap regulasi yang berlaku. Selain itu, penelitian ini juga diharapkan dapat mendukung institusi dalam memperkuat tata kelola teknologi informasi dan meningkatkan kepercayaan pengguna terhadap sistem informasi yang disediakan.

BAB 2. METODOLOGI

Metodologi audit keamanan Website Silaturahmi disusun berdasarkan pendekatan COBIT 2019, yang menekankan keterkaitan antara tujuan bisnis organisasi dengan pengelolaan dan pengendalian teknologi informasi. Runtutan ini bertujuan agar audit tidak hanya bersifat teknis, tetapi juga selaras dengan kebutuhan dan risiko organisasi.

2.1 Identifikasi Objek dan Fokus Audit

Tahap awal dalam metodologi audit adalah mengidentifikasi objek dan fokus audit secara jelas. Objek audit dalam penelitian ini adalah Website Silaturahmi UPN "Veteran" Jawa Timur, yaitu sebuah sistem informasi berbasis web yang digunakan sebagai platform kolaborasi antara mahasiswa, alumni, mitra industri, dan sivitas akademika.

Fokus audit diarahkan pada keamanan website, khususnya pada aspek perlindungan data, pengelolaan risiko keamanan, serta kepatuhan terhadap regulasi. Penetapan fokus ini didasarkan pada beberapa pertimbangan utama, antara lain:

- Website Silaturahmi mengelola data pribadi pengguna, seperti identitas dan informasi akademik.
- Website beroperasi secara daring dan terbuka terhadap berbagai potensi ancaman keamanan siber.
- Keamanan website berpengaruh langsung terhadap kepercayaan pengguna dan reputasi institusi.

Dengan demikian, audit tidak mencakup seluruh fungsi TI, melainkan dipusatkan pada proses-proses COBIT 2019 yang berhubungan langsung dengan keamanan informasi dan pengelolaan risiko TI.

2.2 Identifikasi Tujuan Bisnis Organisasi

Setelah objek dan fokus audit ditetapkan, tahap selanjutnya adalah mengidentifikasi tujuan bisnis organisasi yang didukung oleh Website Silaturahmi. Identifikasi tujuan bisnis ini penting karena COBIT 2019 menekankan bahwa tata kelola TI harus memberikan nilai dan mendukung pencapaian tujuan organisasi.

Berdasarkan fungsi dan peran Website Silaturahmi, tujuan bisnis yang relevan dapat dirumuskan sebagai berikut:

- Menyediakan layanan digital yang aman, andal, dan berkelanjutan.
- Melindungi data pribadi dan informasi pengguna dari ancaman keamanan.
- Menjaga kepercayaan sivitas akademika dan mitra eksternal terhadap layanan digital kampus.
- Memastikan operasional website berjalan sesuai dengan ketentuan hukum dan regulasi yang berlaku.

Tujuan bisnis ini menjadi dasar dalam menentukan enterprise goals COBIT 2019 yang paling relevan dengan kondisi dan kebutuhan organisasi.

2.3 Penentuan Enterprise Goals (EG)

Penentuan **Enterprise Goals (EG)** dilakukan dengan mencocokkan tujuan bisnis organisasi dan fokus audit keamanan dengan daftar enterprise goals yang telah distandarkan dalam COBIT 2019. Enterprise goals menggambarkan sasaran strategis organisasi yang ingin dicapai melalui pemanfaatan TI secara optimal.

Berdasarkan hasil analisis, enterprise goals yang dipilih dalam audit ini adalah:

NO	KODE EG	Enterprise Goal
1	EG02	Managed Business Risk
2	EG03	Managed IT-Related Risk
3	EG09	IT Compliance with External Laws and Regulations

1. Enterprise goal ini dipilih karena keamanan website berkaitan langsung dengan risiko bisnis organisasi. Kegagalan dalam mengelola risiko keamanan dapat menyebabkan kebocoran data, gangguan layanan, serta penurunan reputasi institusi.
2. Enterprise goal ini relevan karena risiko utama yang dihadapi Website Silaturahmi berasal dari penggunaan teknologi informasi, seperti serangan siber, kelemahan sistem, dan kesalahan pengelolaan keamanan TI.
3. Enterprise goal ini dipilih untuk memastikan bahwa pengelolaan website mematuhi peraturan perundang-undangan yang berlaku, khususnya terkait perlindungan data pribadi dan keamanan informasi.

Pemilihan enterprise goals ini memastikan bahwa audit keamanan Website Silaturahmi tidak hanya berorientasi pada aspek teknis, tetapi juga mendukung tujuan strategis organisasi serta kepatuhan terhadap regulasi.

2.4 Penentuan IT-Related Goals (ITG)

Setelah enterprise goals (EG) ditetapkan, tahap selanjutnya dalam runtutan COBIT 2019 adalah menentukan IT-Related Goals (ITG). IT-related goals merepresentasikan tujuan TI yang secara langsung mendukung pencapaian enterprise goals organisasi. Tahap ini merupakan inti dari mekanisme Goals Cascade COBIT 2019, yaitu proses penurunan tujuan strategis organisasi ke tujuan TI yang lebih operasional dan terukur.

Penentuan IT-related goals dilakukan dengan memetakan setiap enterprise goal yang telah dipilih ke IT-related goals yang tersedia dalam COBIT 2019. Pemetaan ini memastikan bahwa pengelolaan dan pengendalian TI, khususnya dalam aspek keamanan website, benar-benar berkontribusi terhadap pencapaian tujuan organisasi.

2.5 Pemetaan Enterprise Goals ke IT-Related Goals

Berdasarkan tabel Goals Cascade COBIT 2019, pemetaan enterprise goals ke IT-related goals pada audit keamanan Website Silaturahmi adalah sebagai berikut:

Enterprise Goal	IT Realated Goal	Deskripsi
EG02 – Managed Business Risk	ITG03 – Managed IT-Related Risk	Pengelolaan risiko TI diperlukan untuk menekan risiko bisnis akibat ancaman keamanan website.
EG03 – Managed IT-Related Risk	ITG04 – Security of Information and Infrastructure	Perlindungan informasi dan infrastruktur TI menjadi kunci dalam mengurangi risiko keamanan sistem.
EG09 – IT Compliance with External Laws and Regulations	ITG09 – Compliance with External Laws	Kepatuhan TI diperlukan untuk memastikan website memenuhi regulasi perlindungan data dan keamanan.

Pemetaan ini menunjukkan hubungan sebab-akibat yang jelas antara tujuan bisnis organisasi dan tujuan TI yang harus dicapai.

2.6 Penjelasan IT-Related Goals yang Dipilih

2.6.1 ITG03 – Managed IT-Related Risk

IT-related goal ini berfokus pada kemampuan organisasi dalam mengidentifikasi, menganalisis, dan mengendalikan risiko yang berasal dari pemanfaatan teknologi informasi. Dalam konteks Website Silaturahmi, ITG03 berkaitan dengan pengelolaan risiko keamanan seperti serangan siber, kebocoran data, dan gangguan layanan.

Pencapaian ITG03 memastikan bahwa risiko keamanan website tidak hanya dikenali, tetapi juga dimitigasi secara sistematis melalui kebijakan, prosedur, dan pengendalian yang memadai.

2.6.2 ITG04 – Security of Information and Infrastructure

ITG04 menekankan pentingnya perlindungan terhadap informasi dan infrastruktur TI. Tujuan ini relevan karena Website Silaturahmi menyimpan dan memproses data pribadi pengguna yang harus dijaga kerahasiaan, integritas, dan ketersediaannya.

Pencapaian ITG04 mencerminkan bahwa organisasi telah menerapkan kontrol keamanan yang memadai, baik dari sisi teknis maupun non-teknis, untuk melindungi sistem dari ancaman internal maupun eksternal.

2.6.3 ITG09 – Compliance with External Laws

ITG09 berfokus pada kepatuhan teknologi informasi terhadap hukum dan regulasi eksternal. Dalam audit ini, ITG09 digunakan untuk menilai sejauh mana Website Silaturahmi mematuhi peraturan terkait perlindungan data pribadi dan keamanan informasi.

Pencapaian ITG09 menunjukkan bahwa pengelolaan TI tidak hanya berorientasi pada operasional, tetapi juga memperhatikan aspek hukum dan tata kelola yang baik.

BAB 3. Penentuan Domain dan Proses COBIT 2019

Setelah IT-Related Goals (ITG) ditetapkan, tahap berikutnya dalam metodologi COBIT 2019 adalah menentukan domain dan proses COBIT 2019 yang akan menjadi ruang lingkup audit. Tahap ini berfungsi sebagai penghubung antara tujuan TI yang bersifat strategis dengan aktivitas pengelolaan dan operasional TI yang dapat diukur dan dievaluasi.

Pemilihan domain dan proses dilakukan secara selektif dengan mempertimbangkan fokus audit keamanan website, risiko yang dihadapi, serta dampaknya terhadap pencapaian tujuan organisasi. Oleh karena itu, tidak seluruh proses COBIT 2019 dijadikan objek audit, melainkan hanya proses-proses yang paling relevan dan memiliki kontribusi langsung terhadap keamanan Website Silaturahmi.

Penentuan domain dan proses ini juga mengikuti prinsip alignment, yaitu keselarasan antara IT-related goals dengan proses-proses COBIT 2019 yang mendukung pencapaiannya. Hasil dari tahap ini adalah penetapan proses COBIT 2019 yang digunakan sebagai dasar evaluasi keamanan Website Silaturahmi.

3.1 Pemetaan IT-Related Goals ke Proses COBIT 2019

Pemetaan dilakukan untuk memastikan bahwa setiap proses yang dipilih memiliki keterkaitan langsung dengan IT-related goals yang telah ditetapkan sebelumnya. Hasil pemetaan ditunjukkan pada tabel berikut:

IT-Related Goal	Domain	Proses COBIT 2019	Fokus Audit
ITG03 – Managed IT-Related Risk	APO	APO12 – Manage Risk	Pengelolaan risiko keamanan website
ITG04 – Security of Information and Infrastructure	APO	APO13 – Manage Security	Kebijakan dan kontrol keamanan informasi
ITG04 – Security of Information and Infrastructure	DSS	DSS05 – Manage Security Services	Operasional layanan keamanan TI
ITG09 – Compliance with External Laws	MEA	MEA03 – Monitor, Evaluate and Assess Compliance	Kepatuhan terhadap regulasi dan standar

3.2 Domain APO (Align, Plan, and Organize)

Domain APO (Align, Plan, and Organize) berfokus pada perencanaan dan pengelolaan TI agar selaras dengan strategi organisasi. Domain ini dipilih karena menjadi fondasi utama dalam pengelolaan risiko dan keamanan TI.

3.2.1 APO12 – Manage Risk

Proses APO12 – Manage Risk digunakan untuk menilai sejauh mana organisasi mampu mengidentifikasi, menganalisis, dan mengendalikan risiko keamanan website. Evaluasi difokuskan pada keberadaan manajemen risiko, dokumentasi risiko, serta penerapan mitigasi risiko keamanan.

3.2.2 APO13 – Manage Security

Proses APO13 – Manage Security digunakan untuk menilai pengelolaan keamanan informasi secara menyeluruh, termasuk kebijakan keamanan, pengendalian akses, dan perlindungan data pengguna website.

3.3 Domain DSS (Deliver, Service, and Support)

Domain DSS (Deliver, Service, and Support) berfokus pada implementasi dan operasional layanan TI. Domain ini dipilih karena keamanan website sangat dipengaruhi oleh penerapan layanan keamanan sehari-hari.

3.3.1 DSS05 – Manage Security Services

Proses DSS05 – Manage Security **Services** digunakan untuk mengevaluasi efektivitas layanan keamanan operasional, seperti perlindungan server, pemantauan keamanan, backup data, serta pembaruan sistem.

3.4 Domain MEA (Monitor, Evaluate, and Assess)

Domain MEA (Monitor, Evaluate, and Assess) berfokus pada pemantauan dan evaluasi kepatuhan TI terhadap regulasi dan kebijakan.

3.4.1 MEA03 – Monitor, Evaluate and Assess Compliance

Proses MEA03 – Monitor, Evaluate and Assess Compliance digunakan untuk menilai tingkat kepatuhan Website Silaturahmi terhadap peraturan perundang-undangan dan standar keamanan yang berlaku, serta tindak lanjut terhadap hasil audit sebelumnya.

3.5 Fokus Audit per Domain yang Diaudit

Untuk memastikan audit berjalan terarah dan mendalam, fokus audit ditetapkan secara spesifik pada setiap domain dan proses yang dipilih. Penetapan fokus ini membantu auditor memahami apa yang dinilai, mengapa dinilai, dan batasan penilaian pada masing-masing domain.

3.5.1 Fokus Audit Domain APO (APO12 & APO13)

Tujuan Umum Domain APO: Membangun fondasi tata kelola keamanan TI melalui perencanaan, kebijakan, dan pengelolaan risiko yang selaras dengan tujuan organisasi.

Ruang Lingkup Penilaian:

- Keberadaan kebijakan dan prosedur formal terkait manajemen risiko dan keamanan informasi.
- Mekanisme identifikasi, analisis, dan mitigasi risiko keamanan website.
- Penetapan peran dan tanggung jawab keamanan (roles & responsibilities).
- Keselarasan kebijakan keamanan dengan kebutuhan bisnis dan regulasi.

Batasan Audit: Audit tidak menilai perencanaan TI secara umum (mis. portofolio proyek TI), melainkan terbatas pada aspek yang berdampak langsung pada keamanan Website Silaturahmi.

3.5.2 Fokus Audit Domain DSS (DSS05)

Tujuan Umum Domain DSS: Menilai efektivitas implementasi dan operasional layanan keamanan TI dalam mendukung perlindungan website.

Ruang Lingkup Penilaian:

- Pengamanan infrastruktur server dan jaringan website.
- Proses pemantauan keamanan dan pencatatan insiden.
- Mekanisme backup dan pemulihan data.
- Pelaksanaan pembaruan dan patch keamanan.

Batasan Audit: Audit tidak mencakup seluruh layanan operasional TI, tetapi hanya layanan yang berhubungan langsung dengan keamanan operasional Website Silaturahmi.

3.5.3 Fokus Audit Domain MEA (MEA03)

Tujuan Umum Domain MEA: Memastikan pengelolaan keamanan website dipantau dan dievaluasi secara berkelanjutan serta mematuhi regulasi yang berlaku.

Ruang Lingkup Penilaian:

- Kepatuhan terhadap peraturan perlindungan data pribadi dan kebijakan internal.
- Pelaksanaan audit atau evaluasi keamanan secara berkala.
- Mekanisme pelaporan dan tindak lanjut temuan audit.

Batasan Audit: Audit difokuskan pada aspek kepatuhan dan evaluasi keamanan website, tidak mencakup evaluasi kinerja TI secara menyeluruh.

Dengan penetapan fokus audit per domain ini, proses audit keamanan Website Silaturahmi menjadi lebih terarah, mendalam, dan relevan terhadap tujuan serta risiko yang dihadapi organisasi.

3.6 RACI Analisis

RACI Chart merupakan sebuah matriks manajemen tanggung jawab yang digunakan untuk mendefinisikan dan mengklarifikasi peran setiap pihak yang terlibat dalam suatu proses atau aktivitas. RACI merupakan singkatan dari Responsible, Accountable, Consulted, dan Informed yang masing-masing memiliki arti sebagai berikut:

- **Responsible (R)**
  Pihak yang bertanggung jawab secara langsung dalam melaksanakan suatu aktivitas atau proses. Pihak ini melakukan pekerjaan operasional dan memastikan aktivitas berjalan sesuai rencana.

- **Accountable (A)**
  Pihak yang memiliki tanggung jawab akhir terhadap hasil dari suatu aktivitas. Pihak ini berwenang mengambil keputusan dan memastikan bahwa aktivitas tersebut terlaksana dengan benar. Dalam setiap aktivitas, hanya terdapat satu pihak yang berperan sebagai Accountable.

- **Consulted (C)**
  Pihak yang memberikan masukan, saran, atau keahlian sebelum suatu keputusan atau aktivitas dijalankan. Komunikasi dengan pihak ini bersifat dua arah.

- **Informed (I)**
  Pihak yang perlu mendapatkan informasi terkait pelaksanaan atau hasil suatu aktivitas, namun tidak terlibat langsung dalam pengambilan keputusan maupun pelaksanaan. Komunikasi dengan pihak ini bersifat satu arah.

Penerapan RACI Chart dalam audit keamanan Website SILATURAHMI bertujuan untuk memastikan bahwa setiap proses COBIT 2019 yang diaudit memiliki pembagian peran yang jelas, sehingga tidak terjadi tumpang tindih tanggung jawab maupun kekosongan peran. Dengan adanya RACI Chart, koordinasi antar pihak yang terlibat dalam pengelolaan keamanan TI dapat berjalan lebih terstruktur, efektif, dan akuntabel sesuai dengan prinsip tata kelola COBIT 2019.

Proses COBIT 2019	**Pimpinan Unit**	**PJ MBKM**	**Dosbing**	**Mahasiswa**
APO12 – Manage Risk	A	R	C	I
APO12.01 Identifikasi Risiko	A	R	C	I
APO12.02 Analisis Risiko	A	R	C	I

APO12.03 Mitigasi Risiko	A	R	C	I
APO12.04 Monitoring Risiko	A	R	C	I
APO13 – Manage Security	A	R	C	I
APO13.01 Kebijakan Keamanan	A	R	C	I
APO13.02 Kontrol Akses	A	R	C	I
APO13.03 Perlindungan Data	A	R	C	I
DSS05 – Manage Security Services	A	R	R	I
DSS05.01 Keamanan Operasional	A	R	R	I
DSS05.02 Penanganan Insiden	A	R	R	I
DSS05.03 Backup & Recovery	A	R	R	I
MEA03 – Monitor, Evaluate & Assess Compliance	A	R	C	I
MEA03.01 Evaluasi Kepatuhan	A	R	C	I
MEA03.02 Audit Keamanan	A	R	C	I
MEA03.03 Tindak Lanjut Audit	A	R	C	I

BAB 4. Instrumen Audit Berbasis COBIT 2019 (Skala Likert)

Pilihan	Penjelasan	Skor
STS	Sangat Tidak Setuju / Belum Diterapkan	1
TS	Tidak Setuju / Jarang Diterapkan	2
N	Netral / Kadang Diterapkan	3
S	Setuju / Sebagian Besar Diterapkan	4
SS	Sangat Setuju / Diterapkan Sepenuhnya	5

4.1 Domain APO: Align, Plan, and Organize (Perencanaan & Keamanan)

Domain	Kode	Pertanyaan	Skor
APO12	12.01	Apakah penanggung jawab MBKM (Responsible) telah menyusun dan memperbarui daftar risiko keamanan secara rutin?	3
	12.02	Apakah Mahasiswa (Informed) menerima informasi atau peringatan dini mengenai potensi risiko keamanan yang berdampak pada akun mereka?	3
APO13	13.01	Apakah penanggung jawab MBKM (Responsible) telah mendokumentasikan kebijakan kontrol akses (hak administrator) dan mematuhinya secara ketat?	3
	13.02	Sejauh mana Mahasiswa (Informed) telah diinformasikan mengenai panduan menjaga keamanan data pribadi di website SILATURAHMI?	3

4.2 Domain DSS: Deliver, Service, and Support (Operasional Keamanan)

Domain	Kode	Pertanyaan	Skor
DSS05	05.01	Apakah terdapat prosedur penanganan insiden yang dijalankan oleh penanggung jawab MBKM (Responsible) saat terjadi gangguan layanan?	3
	05.02	Apakah Mahasiswa (Informed) mendapatkan pemberitahuan status ketika website sedang dalam pemeliharaan (maintenance)?	3

4.3 Domain MEA: Monitor, Evaluate, and Assess (Kepatuhan dan Evaluasi)

Domain	Kode	Pertanyaan	Skor
MEA03	03.01	Apakah penanggung jawab MBKM (Responsible) telah melakukan evaluasi berkala untuk memastikan sistem mematuhi regulasi perlindungan data?	3
	03.02	Sejauh mana Mahasiswa (Informed) merasa yakin bahwa data pribadi mereka dilindungi sesuai kebijakan yang diinformasikan?	3

4.4 Skor Rata-Rata Skala Likert

Setelah tahap mendata seluruh jawaban responden, maka tahap berikutnya adalah menghitung skor total memakai rumus yang sudah dijelaskan sebelumnya. Dari data yang dirapikan di tahap sebelumnya maka perhitungan skor total adalah sebagai berikut:

$$\text{Rata-rata} = \frac{\text{Skor Total}}{\text{Jumlah Responden}}$$

Domain	Proses COBIT 2019	Jumlah Pernyataan	Total Skor	Skor Rata-Rata	Skor Rata-Rata
APO12	Manage Risk	3	6	3.0	Netral / Kadang Diterapkan
APO13	Manage Security	2	6	3.0	Netral / Kadang Diterapkan

DSS05	Manage Security Services	2	6	3.0	Netral / Kadang Diterapkan
MEA03	Monitor, Evaluate & Asses Compliance	2	6	3.0	Netral / Kadang Diterapkan

4.5 Persentase Skor

Tahap perhitungan skala penilaian likert adalah menghitung skor dalam bentuk persentase. Berikut perhitungannya:

$$\text{Persentase} = \frac{\text{Skor yang Diperoleh}}{\text{Skor Maksimal}} \times 100\%$$

Domain	Proses COBIT 2019	Skor Rata-Rata	Skor Maksimal	Persentasi	Kategori
APO12	Manage Risk	3.0	5	60%	Cukup
APO13	Manage Security	3.0	5	60%	Cukup
DSS05	Manage Security Services	3.0	5	60%	Cukup
MEA03	Monitor, Evaluate & Asses Compliance	3.0	5	60%	Cukup

Persentase	Kategori
0% - 20%	Sangat Kurang
21% - 40%	Kurang
41% - 60%	Cukup
61% - 80%	Baik
81% - 100%	Sangat Baik

4.4 Gap Analysis

Gap analysis adalah proses perbandingan antara kondisi saat ini (as-is) dengan kondisi yang diinginkan (to-be) dalam kerangka kerja COBIT 2019. Hal ini dilakukan untuk mengidentifikasi gap atau kesenjangan antara kondisi yang ada dengan standar atau tujuan yang ditetapkan dalam COBIT 2019

Berikut ini adalah gap analysis yang didapat dari hasil rating process analysis:

Domain	As-Is	To-Be	Gap
APO12	3	4	1
	3	4	1
APO13	3	4	1
	3	4	1
DSS05	3	4	1
	3	4	1
MEA03	3	4	1
	3	4	1

BAB 5. Hasil dan Analisis

5.1 Gambaran Umum Hasil Audit

Website SILATURAHMI UPN “Veteran” Jawa Timur telah menjalani audit menggunakan kerangka kerja COBIT 2019 melalui kuesioner dengan skala Likert 1–5. Audit ini difokuskan pada empat domain utama: APO12, APO13, DSS05, dan MEA03. Berdasarkan analisis data, semua proses yang diaudit memperoleh rata-rata nilai 3.0. Nilai tersebut menghasilkan persentase skor 60%, yang tergolong dalam kategori "Cukup". Ini menunjukkan bahwa pengelolaan keamanan telah dilakukan, tetapi masih bersifat acak dan belum sepenuhnya terstandarisasi.

5.2 Analisis Hasil Audit per Domain

- APO12 – Mengelola Risiko (Skor 3. 0): Proses manajemen risiko untuk Website SILATURAHMI telah dilakukan, tetapi tahap identifikasi dan analisis risiko belum sepenuhnya terstandarisasi dan tidak tercatat dengan baik dalam dokumen resmi.
- APO13 – Mengelola Keamanan (Skor 3. 0): Organisasi telah membuat kebijakan mengenai keamanan informasi, tetapi pelaksanaan kontrol keamanan di lapangan masih belum optimal dan belum seragam di berbagai bagian sistem.
- DSS05 – Mengelola Layanan Keamanan (Skor 3. 0): Layanan keamanan operasional seperti perlindungan server dan respons insiden sudah tersedia, tetapi masih belum sepenuhnya terintegrasi dan belum menjalani pengujian secara rutin.
- MEA03 – Memantau, Mengevaluasi, dan Menilai Kepatuhan (Skor 3. 0): Kegiatan pemantauan terhadap kepatuhan keamanan telah dilakukan, akan tetapi belum berjalan secara konsisten dan belum terjadwal dengan baik.

5.3 Analisis Kesenjangan (Gap Analysis)

Analisis kesenjangan dilakukan dengan menilai kondisi yang ada saat ini (As-Is) dibandingkan dengan kondisi yang diinginkan (To-Be) yang memiliki skor 4. Semua domain yang diaudit menunjukkan perbedaan sebesar 1 tingkat. Kesenjangan ini menunjukkan bahwa meskipun dasar pengelolaan keamanan telah tersedia, masih ada kebutuhan untuk perbaikan yang signifikan terkait konsistensi pelaksanaan, dokumentasi resmi, serta evaluasi yang terus-menerus.

5.4 Analisis Tingkat Kapabilitas Proses

Berdasarkan nilai rata-rata yang didapat, kemampuan manajemen keamanan untuk Website SILATURAHMI terletak pada Level 3 (Proses yang Ditetapkan). Di level ini, prosedur keamanan telah ditetapkan dan diimplementasikan, namun performanya belum sepenuhnya diukur secara kuantitatif dan belum dipantau secara regular untuk menjamin efektivitasnya.

BAB 6. Kesimpulan dan Saran

6.1 Kesimpulan

Berdasarkan temuan dari pemeriksaan keamanan sistem informasi di Website SILATURAHMI dengan menggunakan kerangka kerja COBIT 2019, dapat disimpulkan bahwa:

1. Keselarasan Strategis: Terdapat keselarasan antara sasaran bisnis strategis (Tujuan Perusahaan) dengan sasaran yang berhubungan dengan TI (Tujuan Terkait TI) untuk mendukung manajemen risiko dan pemenuhan regulasi.
2. Kondisi Tata Kelola: Secara keseluruhan, pengelolaan aspek keamanan berada pada tingkat "Cukup" dengan nilai rata-rata 3,0. Ini menunjukkan bahwa proses keamanan telah diidentifikasi dan diterapkan, namun masih terdapat kekurangan dalam konsistensi dan dokumentasinya.
3. Tingkat Kapabilitas: Manajemen keamanan Website SILATURAHMI saat ini berada di Tingkat Kapabilitas 3 (Proses yang Terbentuk). Proses ini telah tercatat, tetapi memerlukan sistem pengukuran kinerja yang lebih formal untuk mencapai stabilitas dan prediktabilitas yang lebih baik.

6.2 Saran

Untuk meningkatkan keamanan Website SILATURAHMI secara berkelanjutan, disarankan agar:

1. Peningkatan Konsistensi: Tim pengelola perlu mendokumentasikan secara resmi dan menyelaraskan semua prosedur operasional keamanan agar diterapkan secara konsisten.
2. Pencapaian Level Lebih Tinggi: Menetapkan target untuk mencapai Tingkat Kapabilitas 4 (Proses yang Dapat Diprediksi) dalam domain utama (APO13 dan DSS05) dengan mulai menerapkan pengukuran kinerja keamanan yang berbasis data serta metrik yang dapat diukur.
3. Audit dan Evaluasi Berkala: Menetapkan jadwal secara rutin untuk pemantauan dan penilaian kepatuhan (MEA03) agar setiap potensi celah keamanan dapat terdeteksi lebih awal sebelum berubah menjadi insiden.
4. Penguatan Integrasi: Memasukkan proses manajemen risiko (APO12) dalam setiap perubahan sistem informasi sehingga upaya mitigasi risiko selalu menjadi bagian dari operasional website.