ANALISIS TEKNOLOGI DAN PROSEDURAL DALAM PENANGANAN INSIDEN UNTUK MENDUKUNG FORENSIK DIGITAL

Tri Rochmadi, Abdul Fadli, Imam Riadi, Khairul Nisa Panilestari, Yanuar Wicaksono
Sistem Informasi, Universitas Alma Ata
Informatika, Universitas Ahmad Dahlan
Jl. Brawijaya No.99, Jadan, Tamantirto, Kec. Kasihan, Kabupaten Bantul, Daerah Istimewa Yogyakarta
trirochmadi@almaata.ac.id

ABSTRAK

Perkembangan teknologi informasi di lingkungan perguruan tinggi mendorong peningkatan pemanfaatan sistem digital dalam berbagai aktivitas akademik dan administratif. Namun, digitalisasi tersebut juga diikuti oleh meningkatnya risiko insiden keamanan siber yang dapat mengancam integritas, kerahasiaan, dan ketersediaan data. Oleh karena itu, kesiapan teknologi dan prosedural dalam penanganan insiden menjadi aspek penting untuk mendukung proses investigasi forensik digital secara efektif. Penelitian ini bertujuan untuk menganalisis tingkat kesiapan teknologi dan prosedural dalam penanganan insiden keamanan siber pada 10 perguruan tinggi swasta di Daerah Istimewa Yogyakarta. Penelitian menggunakan pendekatan *mixed-method* melalui kuesioner, wawancara, analisis *capability level*, dan *gap analysis* dengan mengacu pada kerangka kerja COBIT 2019 pada domain Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), serta Deliver, Service and Support (DSS). Hasil penelitian menunjukkan adanya variasi tingkat kapabilitas antar wilayah dan universitas. Wilayah Sleman mencapai tingkat *predictable process* dengan indeks pengelolaan insiden 3,61 dan teknologi infrastruktur 3,55, sedangkan wilayah Bantul dan Kota Yogyakarta berada pada tingkat *managed process* dengan nilai rata-rata sekitar 2,29. Temuan juga menunjukkan adanya kesenjangan menuju target *optimising process* (level 5), terutama pada aspek standardisasi prosedur, dokumentasi kebijakan, serta dukungan infrastruktur teknologi. Oleh karena itu, peningkatan tata kelola keamanan informasi, penguatan dokumentasi SOP, dan pengembangan kapasitas sumber daya manusia menjadi rekomendasi utama untuk meningkatkan kesiapan forensik digital di perguruan tinggi.

Kata kunci: Forensik digital, Keamanan siber, Kesiapan teknologi, prosedural, COBIT 2019, Penanganan insiden

1. PENDAHULUAN

Di era digital saat ini, teknologi informasi dan komunikasi telah menjadi landasan utama operasional di berbagai sektor, termasuk pendidikan tinggi. Namun, pesatnya digitalisasi ini berbanding lurus dengan peningkatan ancaman keamanan siber yang semakin kompleks dan dinamis [1]. Data dari Badan Siber dan Sandi Negara (BSSN) pada Januari 2025 mencatat anomali trafik mencapai lebih dari 425 juta, dengan serangan *malware* mendominasi lebih dari 90% total anomali, disusul oleh akses tidak sah dan miskonfigurasi sistem. Tingginya aktivitas serangan ini menuntut organisasi, khususnya perguruan tinggi, untuk tidak hanya menerapkan solusi teknis preventif, tetapi juga memiliki kesiapan dalam menangani insiden secara terstruktur guna meminimalkan kerugian dan menjaga keberlangsungan operasional.

Organisasi menghadapi tantangan besar dalam membangun pendekatan aktif terhadap insiden siber akibat keterbatasan tenaga ahli dan tuntutan respon cepat dalam pengambilan keputusan. Oleh karena itu, penerapan solusi teknis saja tidak cukup; diperlukan strategi menyeluruh yang mencakup manajemen insiden yang terstruktur serta pelatihan kesadaran pengguna secara berkelanjutan. Selain penguatan internal, kolaborasi erat dengan lembaga keamanan eksternal juga menjadi kunci dalam mengamankan infrastruktur dari ancaman siber yang terus berkembang [2]. Penanganan insiden keamanan tidak dapat dipisahkan dari kebutuhan forensik digital, yang berfungsi untuk menjawab pertanyaan mengenai "apa", "siapa", dan "bagaimana"[3]suatu insiden terjadi. Namun, tantangan utama dalam proses ini adalah sifat bukti digital yang sangat rentan, mudah hilang, dan mudah berubah. Kesalahan sekecil apapun dalam prosedur penanganan awal dapat merusak integritas data, sehingga bukti tersebut menjadi tidak valid dalam proses investigasi maupun ranah hukum [3], [4]. Oleh karena itu, kesiapan teknologi dan prosedural dalam tahap awal respons insiden menjadi faktor penentu keberhasilan proses forensik digital selanjutnya.

Digital forensik merupakan teknik yang diterapkan untuk menyelidiki barang bukti dalam bentuk elektronik atau digital, dengan tujuan merekonstruksi tindak kejahatan siber atau mendukung proses analisis pada kasus kriminal berbasis teknologi [5]. Keamanan informasi memegang peranan vital tidak hanya dalam melindungi privasi dan mencegah kejahatan siber, tetapi juga untuk menjaga integritas data, kepercayaan publik, dan kelangsungan operasional organisasi. Di tengah tantangan digitalisasi dan *big data*, upaya ini mencakup peningkatan literasi digital untuk mengurangi risiko faktor manusia serta pemenuhan standar internasional melalui evaluasi berkala. Pada intinya, keamanan informasi bukan sekadar kebutuhan teknis, melainkan strategi fundamental untuk

mengamankan aset, reputasi, dan keberlanjutan organisasi dari ancaman yang terus berkembang [6].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis tingkat kesiapan teknologi dan prosedural dalam penanganan insiden guna mendukung forensik digital pada 10 Perguruan Tinggi Swasta di Daerah Istimewa Yogyakarta. Analisis dilakukan dengan menggunakan kerangka kerja COBIT 2019, yang dipilih karena menyediakan panduan tata kelola TI yang komprehensif, mencakup domain *Align, Plan and Organize* (APO), *Build, Acquire and Implement* (BAI), dan *Deliver, Service and Support* (DSS). Penelitian ini diharapkan diharapkan memberikan gambaran yang informatif terkait kondisi aktual, sekaligus menjadi dasar dalam memberikan rekomendasi perbaikan dalam meningkatkan tingkat kesiapan forensik digital pada perguruan tinggi swasta di DIY.

2. TINJAUAN PUSTAKA

Penelitian ini didasarkan pada berbagai studi terdahulu yang relevan guna memperkuat landasan teoritis serta memberikan gambaran mengenai perkembangan penelitian yang berkaitan dengan topik yang dikaji.

2.1. Penelitian Terdahulu

Penelitian berjudul "*Towards Digital Forensic Readiness: A Framework for Financial Service Providers*" menggunakan metode penelitian deskriptif untuk menganalisis tingkat kesiapan forensik digital pada organisasi penyedia layanan keuangan. Hasil penelitian menunjukkan bahwa meskipun organisasi telah menerapkan berbagai praktik terbaik dalam pengelolaan teknologi informasi, insiden keamanan siber masih tetap terjadi. Temuan ini mengindikasikan adanya potensi permasalahan dalam aspek kepatuhan serta menunjukkan bahwa penerapan praktik terbaik saja belum sepenuhnya mampu mencegah terjadinya insiden keamanan. Oleh karena itu, penelitian tersebut menekankan pentingnya peningkatan kesiapan forensik digital agar organisasi mampu mengidentifikasi, mengumpulkan, serta mengelola bukti digital secara efektif ketika insiden keamanan terjadi [7].

Penelitian berjudul *"A Novel Digital Forensic Readiness (DFR) Framework for e-Government"* menggunakan metode penelitian kualitatif untuk mengembangkan kerangka kerja kesiapan forensik digital pada lingkungan *e-Government*. Hasil penelitian menunjukkan bahwa studi tersebut berhasil menghasilkan kerangka kerja *Digital Forensic Readiness* (DFR) yang mengintegrasikan keunggulan dari kerangka kerja yang dikembangkan oleh Elyas dkk. dan Klaim. Melalui proses identifikasi dan analisis, penelitian tersebut menghasilkan 37 parameter kesiapan forensik digital, di mana 33 parameter dinilai relevan untuk disusun menjadi kebijakan. Kebijakan yang dihasilkan terdiri dari 8 domain dan 33 pasal yang mencakup aspek perencanaan, implementasi, pemantauan, serta evaluasi dan pelaporan. Penyusunan kebijakan tersebut mengikuti siklus manajemen Deming (*Plan–Do–Check–Act*). Selanjutnya, proses validasi dilakukan melalui penilaian para ahli dan metode member checking yang menunjukkan bahwa kerangka kebijakan yang dihasilkan dinilai relevan serta dapat diimplementasikan. Temuan ini memberikan pedoman praktis bagi organisasi pemerintahan dalam meningkatkan kesiapan forensik digital guna mendukung penanganan insiden keamanan informasi secara lebih efektif [8].

2.2. Forensik Digital

Forensik digital adalah cabang dari ilmu forensik yang berfokus pada proses penyelidikan dan pemeriksaan terkait suatu kasus dengan meneliti serta menemukan data dan konten yang tersimpan dalam perangkat digital [9]. Salah satu cabang dari ilmu forensik adalah forensik digital, yang berfokus pada pengungkapan hasil investigasi terhadap data yang terdapat pada perangkat digital seperti komputer, ponsel, dan perangkat sejenis [10]

2.3. 2019

COBIT 2019 adalah singkatan dari *Control Objective of Information and Related Technology*. Kerangka kerja ini digunakan untuk mengatur tata Kelola, manajemen informasi dan teknologi dalam sebuah organisasi. Tujuannya mencakup seluruh aspek seperti *enterprise* IT yang mengacu pada seluruh teknologi dan pengolahan informasi dalam organisasi untuk mencapai tujuan, tanpa bergantung pada lokasi keberadaannya [11] *Framework* COBIT 2019 dalam instrumen pertanyaan ini adalah.

2.4. *Phyton*

Python merupakan bahasa pemrograman tingkat tinggi yang dikembangkan oleh Guido Van Rossum dan pertama kali diperkenalkan pada tahun 1991. Saat ini, Python termasuk salah satu bahasa pemrograman yang paling populer. Selain bersifat serbaguna, *Python* juga banyak dimanfaatkan dalam berbagai bidang, termasuk pengembangan *Machine Learning* dan *Deep Learning* [12]

2.5. *Capability Level*

Proses *Capability level* digunakan sebagai alat untuk menilai tingkat kematangan tata kelola TI dalam suatu organisasi. Model ini mengacu pada standar ISO/IEC 15504 sebagai kerangka penilaian proses. Melalui model ini, kinerja proses pada area tata kelola dan manajemen dapat diukur secara sistematis, sekaligus menjadi dasar dalam melakukan perbaikan dan peningkatan pada area yang telah teridentifikasi [13].

3. METODE PENELITIAN

Proses pengumpulan data menggunakan pendekatan mixed-method melalui kuesioner kepada staf IT perguruan tinggi swasta dan wawancara mendalam. Instrumen penelitian disusun berdasarkan kerangka kerja COBIT 2019 (domain APO, BAI, dan DSS). Pengolahan data dilakukan menggunakan *python*, dilanjutkan dengan analisis tematik dan analisis kesenjangan (*gap analysis*). Tahap awal analisis mencakup perhitungan rekapitulasi jawaban untuk menentukan *capability level* (tingkat kapabilitas) saat ini. Berikut rumus perhitungannya [13].

1. Menghitung rekapitulasi jawaban responden

$$\mathbf{RK} = \frac{\mathbf{C}}{\sum \mathbf{R}} \times \mathbf{100}\% \quad (1)$$

Keterangan:
RK : Rekapitulasi jawaban responden kuesioner
C : Hasil banyaknya jawaban untuk setiap level 0 sampai 5 setiap aktivitas proses
$\sum R$: Jumlah responden

2. Menghitung nilai *capability level*

$$\mathbf{AK} = \frac{(\mathbf{RK}\times\mathbf{L0})+(\mathbf{RK}\times\mathbf{L1})+(\mathbf{RK}\times\mathbf{L2})+(\mathbf{RK}\times\mathbf{L3})+(\mathbf{RK}\times\mathbf{L4})+(\mathbf{RK}\times\mathbf{L5})}{\mathbf{100}} \quad (2)$$

Keterangan:
AK : Nilai kapabilitas
RK : Hasil rekapitulasi jawaban responden kuesioner
L : Level 0 sampai 5

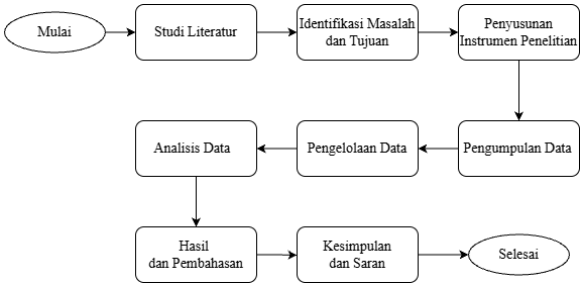
Nilai tersebut kemudian dipetakan ke dalam skala pembulatan indeks sebagi berikut [14]

Tabel 1. Skala Pembulatan Indeks

Skala	Tingkat Model	Level Model *Capability*
Maturity		
4,51-5,00	5-Optimalisasi	5-*Optimising Process*
3,51-4,50	4-Diatur	4-*Preditable Process*
4,51-3,50	3-Ditetapkan	3-*Establised Process*
1,51-2,50	2-Dapat Diulang	2-*Managed process*
0,51-1,50	1-Inisialisasi	1-*Performed Process*
0,00-0,50	0-Tidak Ada	0-*Incomplate Process*

Keterangan setiap levelnya [15].

a. Level 0 *(Incomplete Process)*: Proses belum ada atau belum berjalan dengan semestinya
b. Level 1 *(Performed Process)*: Proses telah diterapkan, namun dokumentasinya masih minim
c. Level 2 *(Managed Process)*: Proses sudah terdokumentasi dan dikelola, tetapi belum memiliki standar yang baku
d. Level 3 *(Established Process)*: Proses memiliki standar yang jelas dan diterapkan secara konsisten
e. Level 4 *(Predictable Process)*: Proses telah dipantau serta diukur secara sistematis
f. Level 5 *(Optimizing Process)*: Proses berada pada tahap penyempurnaan secara terus-menerus untuk peningkatan kualitas



Gambar 1. Flowchart

Berdasarkan alur penelitian diatas pada tahapan uji validitas instrumen tidak dicantumkan. Uji validitas instrumen sudah dilakukan penelitian sebelumnya dengan melibatkan tujuh pakar dari tujuh perguruan tinggi (tiga orang praktisi dan empat orang akademik) [16].

4. HASIL DAN PEMBAHASAN

4.1. Analisis Tematik

4.1.1 Tema : Pengalaman Insiden

1. Jenis Insiden

Berdasarkan analisis data pertanyaan terbuka, mayoritas insiden yang dilaporkan berkaitan erat dengan serangan teknis terhadap aplikasi situs web dan server, di mana kerentanan pada *Content Management System* (CMS) seperti WordPress menjadi target utama penyebaran *malware*, penyusupan konten ilegal seperti judi online, serta serangan *brute force*. Selain serangan pada aplikasi, pola insiden juga menunjukkan tingginya upaya akses ilegal (*unauthorized access*) oleh pihak eksternal yang berusaha menembus pertahanan jaringan dan mencuri kredensial pengguna. Namun, di luar ancaman siber, terdapat kegagalan infrastruktur fisik, seperti gangguan kelistrikan, menjadi ancaman serius yang berdampak fatal pada ketersediaan layanan (*availability*). Oleh karena itu, meskipun gangguan keamanan paling sering disebabkan oleh serangan siber, keandalan perangkat keras pendukung tetap menjadi komponen vital yang tidak boleh diabaikan dalam menjaga keberlangsungan operasional layanan digital.

2. Penanganan Insiden

Berdasarkan data dari pertanyaan terbuka partisipan menunjukkan bahwa prosedur penanganan insiden di beberapa universitas masih cenderung reaktif dan bergantung pada laporan dari pengguna sebelum ditindaklanjuti oleh tim keamanan. Sebagian mengandalkan tim berwenang untuk investigasi kasus spesifik seperti *defacement*, partisipan lain secara terbuka mengakui bahwa manajemen penanganan ancaman di tempat mereka belum terstruktur dengan baik.

3. Solusi Insiden

Berdasarkan data dari pertanyaan terbuka partisipan menunjukkan bahwa solusi untuk menanggulangi insiden keamanan yang terjadi. Pada

tingkat yang paling dasar, solusi mencakup langkah investigasi untuk memahami jenis serangan, seperti pada kasus *defacement*. Namun, untuk insiden yang berdampak langsung pada integritas sistem seperti infeksi *malware*, solusi yang diterapkan lebih teknis, mulai dari pembersihan (*cleaning*) dan penutupan celah keamanan (*patching*) hingga tindakan pemulihan total berupa instalasi ulang aplikasi ketika sistem sudah tidak dapat diselamatkan.

4. Tantangan Utama

Berdasarkan data dari pertanyaan terbuka partisipan menunjukkan bahwa tantangan utama pada aspek ketersediaan data forensik dan kesiapan Sumber Daya Manusia (SDM). Secara teknis, ketidaklengkapan pencatatan aktivitas sistem (*logging*) menjadi kendala yang menyulitkan proses penelusuran jejak digital saat insiden terjadi. Masalah ini diperberat oleh faktor organisasional, yaitu belum terbentuknya tim khusus yang fokus pada forensik digital serta keterbatasan jumlah personil keamanan. Selain itu, rendahnya kesadaran keamanan (*security awareness*) di kalangan pengguna dan adanya batasan akses informasi antar divisi turut menghambat deteksi dini dan respons yang efektif.

4.1.2 Tema : Kebijakan dan Prosedur

1. Kebijakan dan Prosedur Tertulis

Berdasarkan data dari pertanyaan terbuka partisipan menunjukkan bahwa dalam aspek tata kelola terkait penanganan insiden forensik digital. Beberapa partisipan mengonfirmasi bahwa belum memiliki kebijakan atau prosedur operasional standar (SOP) yang tertulis. Meskipun demikian, menunjukkan bahwa secara operasional tahapan penelusuran dan investigasi insiden telah dijalankan oleh tim teknis namun pelaksanaannya masih berbasis pada praktik yang tidak terdokumentasi. Hal ini, menunjukkan bahwa manajemen insiden saat ini masih sangat bergantung pada inisiatif dan pengetahuan personal tertentu, bukan pada sistem yang berstandar.

2. Kesiapan Tim IT

Berdasarkan data dari pertanyaan terbuka partisipan menunjukkan bahwa mulai dari tingkat kematangan *Intermediate-Mature* hingga penilaian kesiapan yang rendah. Sebagian partisipan memiliki struktur tim yang spesifik, seperti keberadaan *network engineer* dan bahkan memberikan penilaian kuantitatif yang cukup tinggi terhadap kapabilitas tim mereka (7.5/10). Namun, terdapat perspektif menarik mengenai kesiapan tim terbentuk karena pengalaman menangani insiden yang sudah terjadi, bukan akibat perencanaan sebelumnya.

4.1.3 Tema : Teknologi, Infrastruktur, dan Keamanan

1. Penerapan Standar Keamanan Informasi

Berdasarkan data yang diperoleh tingkat penerapan standar keamanan partisipan menunjukkan respon yang cukup baik. Di satu sisi, terdapat universitas yang telah memiliki tata kelola keamanan yang matang dengan mengadopsi standar internasional seperti ISO 27001 dan SNI, serta menerapkan *Best Practice* dari OWASP untuk keamanan aplikasi. Namun, masih menyatakan belum memiliki acuan standar keamanan yang baku. Kondisi ini menunjukkan bahwa sosialisasi kebijakan keamanan belum merata.

2. Koordinasi dengan Pihak Eksternal

Berdasarkan data dari pertanyaan terbuka menunjukkan bahwa hingga saat ini belum ada inisiatif untuk melibatkan pihak ketiga baik itu aparat penegak hukum maupun penyedia jasa forensik digital swasta. Keputusan ini didasari oleh penilaian bahwa kapabilitas sumber daya internal masih dianggap memadai untuk menanggulangi skala ancaman yang dihadapi. Insiden yang terjadi sejauh ini kemungkinan masih dikategorikan sebagai gangguan teknis internal, belum mencapai tingkat keparahan yang memerlukan intervensi hukum.

4.1.4Tema : Evaluasi dan Pembelajaran dari Insiden Sebelumnya

1. Penggunaan Perangkat Lunak dan Alat Forensik Digital

Berdasarkan data dari pertanyaan terbuka menunjukkan bahwa perangkat lunak yang digunakan dalam proses investigasi memperlihatkan pada penggunaan bawaan sistem operasi (*native tools*) dan solusi berbasis *open-source*, perangkat lunak forensik. Alat yang diidentifikasi mencakup pemantauan jaringan dan *log* sistem seperti *Fail2ban*, *Journalctl*, serta fitur monitoring pada perangkat MikroTik (*Torch/Packet Sniffer*). Selain itu, penggunaan *Imunify* 360 dan *Mod Security* menegaskan fokus pertahanan pada lapisan aplikasi web, yang selaras dengan temuan sebelumnya mengenai tingginya insiden pada *web server*.

2. Pembelajaran Utama dari Pengalaman Insiden

Berdasarkan data dari pertanyaan terbuka menunjukkan bahwa partisipan mengenai pelajaran yang diperoleh dari penanganan insiden bahwa telah menyadari urgensi keamanan siber dalam keberlangsungan operasional organisasi. Secara spesifik, partisipan menyoroti dua aspek utama dalam upaya mitigasi risiko yaitu pentingnya peningkatan kesadaran keamanan pada level individu serta kebutuhan akan kapabilitas teknis berupa deteksi dini dan manajemen *log* yang aman untuk mendukung kesiapan forensik. Selain itu, teridentifikasi adanya hambatan komunikasi di mana pemahaman mengenai kondisi keamanan siber masih terbatas pada tim teknis. Meskipun kesadaran akan risiko sudah terbentuk, institusi masih perlu meningkatkan prosedur dokumentasi dan memperkuat koordinasi.

3. Perubahan Kebijakan, Teknologi, dan Prosedur Pasca-Insiden

Berdasarkan evaluasi terhadap perubahan prosedur pasca-insiden, ditemukan bahwa partisipan yang terlibat langsung dalam penanganan insiden mengonfirmasi adanya kebijakan akses, instalasi perangkat lunak pencegahan intrusi seperti *fail2ban* serta penutupan *port* jaringan yang berisiko. Langkah-langkah ini menunjukkan adanya upaya mitigasi untuk mencegah berulangnya insiden serupa.

4.2. *Capability Level Analysis*

Berdasarkan hasil pengumpulan data dan pengolahan kuesioner. Di bawah ini memperlihatkan nilai rata-rata kapabilitas yang dicapai oleh tingkat wilayah.

Tabel 2. Capability Level *Wilayah*

Wilayah	*Index Capability*	
	Insiden & Penyelidikan	**Teknologi Infrastruktur**
Sleman	3,60	3,65
Bantul	2,29	1,73
Kota Yogyakarta	2,29	2,47

Pada komponen Pengelolaan Insiden dan Penyelidikan, universitas di Kabupaten Sleman mencapai status *Predictable Process* (rata-rata 3,60), sedangkan universitas di Kabupaten Bantul dan Kota Yogyakarta berada pada status *Managed Process* (rata-rata 2,29) yang terkelola namun belum baku. Selanjutnya, pada komponen Teknologi dan Infrastruktur, wilayah Sleman menunjukkan variasi hasil antara *Predictable Process* (3,65) dan *Managed Process* (1,73), sementara Kota Yogyakarta secara keseluruhan berada pada level *Managed Process* (2,47). Data ini menunjukkan adanya perbedaan signifikan pada tingkat kapabilitas keamanan TI di masing-masing universitas. Berikut hasil *capability level* pada Tingkat universitas.

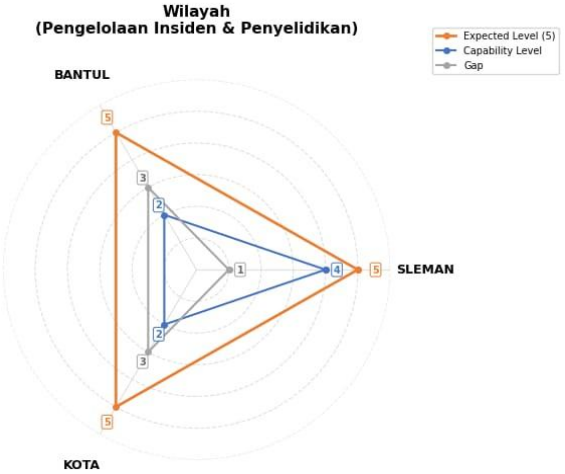
Tabel 3. *Capability Level* Universitas

Universitas	*Index Capability*	
	Insiden & Penyelidikan	**Teknologi Infrastruktur**
R1	3,57	4,00
R2	3,71	3,40
R3	4,14	4,20
R4	3,00	3,00
R5	1,29	1,00
R6	3,57	3,20
R7	2,00	1,40
R8	4,14	3,80
R9	1,29	1,40
R10	1,43	2,20

Berdasarkan hasil perhitungan tabel 3 menunjukkan variasi tingkat kapabilitas pada dua komponen utama. Pada komponen pengelolaan insiden dan penyelidikan, mayoritas responden (R1, R2, R3, R6, dan R8) telah mencapai tingkat kapabilitas 4 (*Predictable Process*) dengan proses yang terpantau dan terukur, sementara R4 berada di tingkat 3, R7 di tingkat 2, dan kelompok R5, R9, serta R10 berada di tingkat 1 karena dokumentasi yang masih minim. Pola serupa terlihat pada komponen Teknologi dan Infrastruktur, di mana R1, R3, dan R8 berhasil mencapai tingkat 4, diikuti oleh R2, R4, dan R6 pada tingkat 3 yang sudah memiliki standar jelas. Namun, kesenjangan masih terlihat dengan R10 yang berada di tingkat 2, serta R5, R7, dan R9 yang menempati posisi terendah (tingkat 1) akibat minimnya dokumentasi pendukung teknologi yang diterapkan.

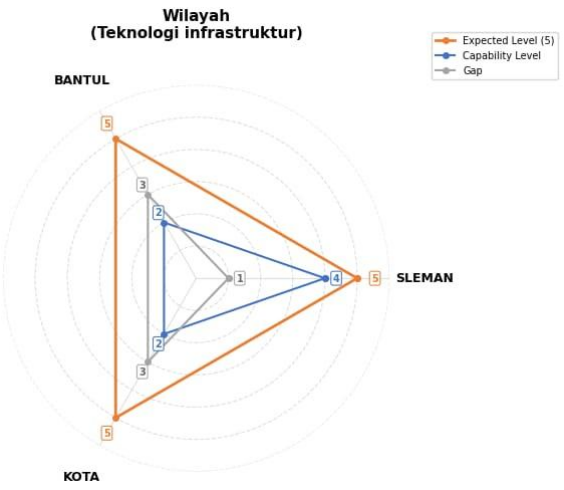
4.3. Analisis GAP/Kesenjangan

Setelah mengetahui nilai kapabilitas saat ini *(current capability)*, langkah selanjutnya adalah melakukan analisis kesenjangan *(gap analysis).* Analisis ini bertujuan untuk mengetahui selisih antara tingkat kapabilitas yang dicapai dengan target yang diharapkan (Level 5). Berikut adalah nilai kesenjangan (gap) yang terjadi pada setiap wilayah dan universitas.



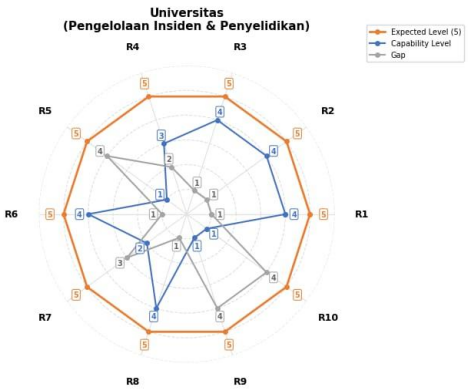
Gambar 2. Diagram Gap Insiden Wilayah

Berdasarkan Gambar 2, target level yang diharapkan untuk seluruh proses komponen pengelolaan insiden dan penyelidikan ditetapkan pada level 5 (*Optimizing Process*), yang berarti proses tersebut memerlukan penyempurnaan berkelanjutan untuk mendukung kebutuhan organisasi. Kondisi saat ini menunjukkan adanya kesenjangan pencapaian di setiap wilayah terhadap target tersebut. Wilayah Sleman memiliki nilai *capability level* sebesar 3,60 dengan *gap* 1,40, sedangkan wilayah Bantul dan Kota Yogyakarta sama-sama memiliki nilai *capability level* 2,29 dengan *gap* sebesar 2,71. Berdasarkan analisis ini, diperlukan peningkatan yang signifikan dan terarah agar proses pengelolaan insiden dan penyelidikan dapat mencapai tingkat optimal. Selanjutnya, analisis *gap* juga dilakukan pada komponen teknologi infrastruktur di tingkat wilayah.



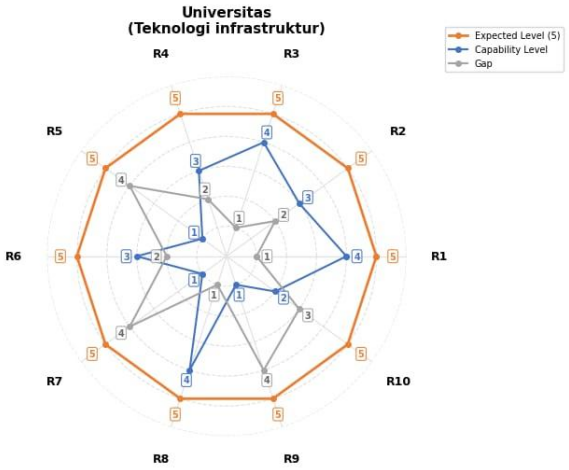
Gambar 3. Diagram Gap TI Wilayah

Berdasarkan gambar 3, target kapabilitas untuk seluruh proses komponen pengelolaan insiden dan penyelidikan ditetapkan pada level 5 (*Optimizing Process*), yang menuntut penyempurnaan teknologi infrastruktur secara berkelanjutan demi mendukung kebutuhan organisasi. Namun, kondisi saat ini menunjukkan adanya kesenjangan pencapaian target di berbagai wilayah, di mana Sleman berada pada *capability level* 3,65 dengan gap 1,35, Bantul pada level 3,27 dengan gap 1,73, dan Kota Yogyakarta pada level 2,53 dengan gap 2,53. Hal ini mengindikasikan bahwa pengelolaan dan pengendalian teknologi infrastruktur di ketiga wilayah tersebut belum optimal, sehingga diperlukan upaya peningkatan terarah untuk mencapai target level 5, serta perluasan analisis hingga ke tingkat universitas untuk memperoleh gambaran kapabilitas yang lebih menyeluruh.



Gambar 4. Diagram Gap Insiden Universitas

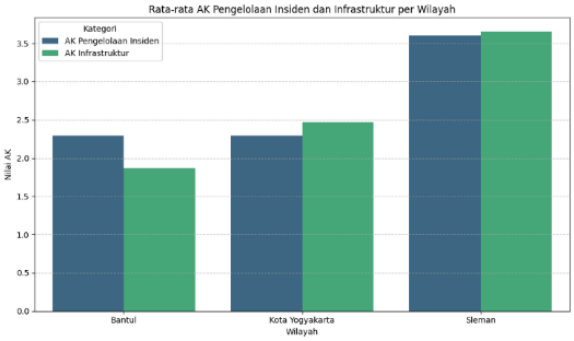
Berdasarkan gambar 4, target kapabilitas untuk proses pengelolaan insiden dan penyelidikan di seluruh universitas ditetapkan pada Level 5 (*Optimizing Process*), yang mengindikasikan perlunya peningkatan kualitas secara berkelanjutan. Saat ini, kondisi tiap universitas masih bervariasi dengan rentang nilai kapabilitas mulai dari yang terendah pada R5 dan R9 (1,29), diikuti R10 (1,43), R7 (2,00), R4 (3,00), R1 dan R6 (3,57), R2 (3,71), hingga yang tertinggi pada R3 dan R8 (4,14). Adanya kesenjangan (*gap*) capaian ini, khususnya pada R5 dan R9 yang memiliki nilai terendah, agar mencapai target optimalisasi perlunya evaluasi kinerja dan inovasi teknologi untuk mencapai target yang diharapkan. Selanjutnya, analisis kesenjangan ini juga akan dilakukan pada komponen teknologi infrastruktur.



Gambar 5. Diagram Gap TI Universitas

Berdasarkan Gambar 5, target kapabilitas komponen teknologi infrastruktur ditetapkan pada Level 5 (*Optimizing Process*) yang berfokus pada penyempurnaan berkelanjutan guna mendukung kebutuhan organisasi. Saat ini, kondisi universitas tersebar di antara level 1 hingga 4 dengan kesenjangan (*gap*) yang bervariasi terhadap target. Universitas R3 memiliki capaian tertinggi dengan level 4,20 (gap 0,80), diikuti oleh R1 (level 4,00; gap 1,00), R8 (level 3,80; gap 1,20), R2 (level 3,40; gap 1,60), R6 (level 3,20; gap 1,80), R4 (level 3,00; gap 2,00), dan R10 (level 2,20; gap 2,80). Universitas R7 dan R9 sama-sama berada di level 1,40 (gap 3,60), sedangkan Universitas R5 memiliki capaian terendah yaitu level 1,00 (gap 4,00). Untuk mencapai Level 5, khususnya bagi R5, diperlukan implementasi teknologi pengelolaan insiden yang terintegrasi, seperti sistem pencatatan dan pemantauan, agar menghasilkan luaran yang optimal di masa mendatang..

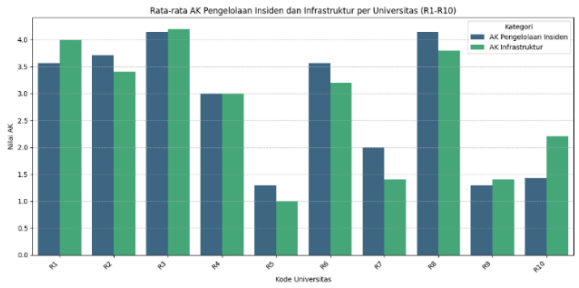
4.4. Pembahasan dan Rekomendasi



Gambar 6. Diagram Perbandingan Wilayah

Berdasarkan data yang diperoleh, terdapat beberapa perbedaan pada tingkat kesiapan yang cukup signifikan antar wilayah dan universitas. Diagaram di bawah ini memperlihatkan perbandingan anatara komponen insiden dan penyelidikan serta teknologi infrastruktur pada level wilayah dan universitas.

Berdasarkan diagram Wilayah pada Gambar 6, Sleman menunjukkan kapabilitas tertinggi dan seimbang dengan skor 3,60 untuk pengelolaan insiden serta 3,65 untuk teknologi infrastruktur. Sebaliknya, Wilayah Bantul memiliki capaian yang lebih rendah, yakni 2,29 pada pengelolaan insiden dan 1,73 pada teknologi infrastruktur, di mana keterbatasan teknologi menjadi penghambat kinerja. Sementara itu, Kota Yogyakarta mencatatkan nilai pengelolaan insiden sebesar 2,29 dan teknologi infrastruktur 2,47, yang menandakan dukungan teknologi sedikit lebih unggul namun keduanya belum mencapai tingkat yang diharapkan. Secara keseluruhan, terdapat kesenjangan kapabilitas antarwilayah di mana Sleman paling unggul sementara Bantul dan Kota Yogyakarta memerlukan peningkatan, serta terlihat adanya variasi signifikan tingkat kapabilitas antar universitas. Berikut jika dibandingkan setiap universitas.



Gambar 7. Diagram Perbandingan Universitas

Berdasarkan diagram pada gambar 7, universitas terlihat tingkat kapabilitas yang cukup signifikan antar universitas. R1, R2, R3, dan R8 menunjukkan kinerja paling unggul dengan pengelolaan insiden yang baik serta didukung infrastruktur memadai, sementara R4 memiliki kapabilitas yang seimbang dan stabil pada tingkat cukup baik. Di sisi lain, R6 dan R10 berada pada level menengah di mana proses pengelolaan insiden sudah berjalan namun belum didukung teknologi yang maksimal. Sebaliknya, R5, R7, dan R9 masih tertinggal dengan nilai rendah pada kedua aspek, terutama akibat keterbatasan infrastruktur teknologi yang menjadi kendala utama..

4.4.1 Rekomendasi

Dalam mencapai target yang diharapkan untuk setiap domain yang telah ditetapkan, disusun rekomendasi perbaikan pada tingkat wilayah dan universitas dapat mencapai target yang diharapkan, yaitu pada level 5. Berikut ini adalah rincian rekomendasi yang diberikan untuk setiap komponen guna mencapai target.

Tabel 4. Rekomendasi Insiden dan Penyelidikan

Wilayah	Insiden dan Penyelidikan
Sleman	Penguatan manajemen insiden dan forensik digital memerlukan kebijakan serta prosedur baku yang terstruktur dengan pembagian peran yang jelas.
Bantul	Diperlukan informasi atau *logging* terkait hal yang terjadi, sehingga memudahkan proses identifikasi dan solusi dari serangan, sehingga penanganan dan keamanan server lebih terjamin. Peningkatan kualitas SDM tim IT dan dokumentasi serta SOP juga sangat diperlukan untuk kesiapan dalam menghadapi serangan siber.
Kota Yogyakarta	Diperlukan peningkatan informasi atau *log* yang disentralisasi terkait hal yang terjadi, sehingga memudahkan proses identifikasi beberapa perangkat yang terkena serangan dan solusi dari serangan. Peningkatan kualitas SDM tim IT dan dokumentasi serta SOP yang lebih lengkap juga sangat diperlukan untuk kesiapan dalam menghadapi serangan siber.

Tabel 5. Rekomendasi Teknologi Infrastruktur

Wilayah	Teknologi dan Infrastruktur
Sleman	Penerapan standar keamanan IT perlu ditingkatkan menjadi implementasi yang berkelanjutan, bukan sekadar referensi, serta didukung oleh optimalisasi alat forensik dan monitoring keamanan. Selain itu, peningkatan kompetensi dan kesadaran SDM menjadi kunci utama yang harus diperkuat melalui pelatihan rutin, simulasi insiden, dan dokumentasi pembelajaran secara berkala.
Bantul	Penggunaan perangkat keras maupun lunak harus sesuai, baik sesuai standar keamanan umum atau standar spesifikasi minimal agar tidak terjadi serangan siber melalui celah yang ada. Selain penggunaan fitur bawaan baik dari perangkat lunak atau keras, sangat disarankan untuk melakukan penambahan berupa perangkat lunak untuk mendukung keamanan yang lebih baik.
Kota Yogyakarta	Untuk mencegah serangan siber, penggunaan perangkat keras dan lunak wajib memenuhi standar keamanan serta dilengkapi dengan proteksi eksternal demi perlindungan yang lebih optimal. Selain itu, pembaruan sistem secara berkala harus dilakukan untuk memastikan keamanan dan kelancaran operasional secara menyeluruh.

Berdasarkan rekomendasi diatas adapun rekomendasi pada tingkat universitas sebagai berikut.

Tabel 6. Rekomendasi Universitas

Kode	Insiden dan Penyelidikan
Pengelolaan insiden dan penyelidikan forensik	
R1	Menyusun SOP penanganan insiden, membuat dokumentasi prosedur khusus, memperkuat peran tim keamanan IT, dan meningkatkan kesiapan yang lebih matang agar proses penanganan insiden dapat berjalan lebih terstruktur dan efektif
R2	Membentuk tim penanganan insiden , membuat laporan kemanan secara tertulis untuk bahan pemantauan dan evaluasi yang dapat dilakukan secara lebih struktur dan konsisten
R3	Membuat kebijakan prosedur secara tertulis untuk meningkatkan keamanan TI, meningkatkan kesadaran SDM terhadap kemana Siber.
R4	Meningkatkan kesadaran SDM terhadap kemanan siber, membentuk tim kemanan dan dokumentasi kebijakan prosedur secara tertulis.
R5	Membuat dokumentasi kebijakan tertulis, meningkatan kesadaran terhadap SDM dalam menangani insiden supaya cepat teratasi secara efektif.
R6	Membuat kebijakan prosedur secara tertulis dan dokumentasi kemanan TI, serta meningkatkan kesadaran SDM dalam mengidentifikasi insiden.
R7	Meningkatan pemahaman terkait insiden, membuat dokumentasi dan prosedur kebijakan kemanan TI secara tertulis guna mengetahui insiden sejak dini.
R8	Melakukan perekrutan SDM dibidang TI dalam penanganan masalah kemanan TI, membuat dokumentasi dan prosedur kebijakan tertulis yang lebih lengkap.
R9	Mempersiapkan tim keamanan TI dan perlu adanya dokumentasi kebijakan secara tertulis agar setiap insiden dapat menjadi bahan pembelajaran untuk memperkuat kebijakan serta prosedur keamanan informasi.
R10	Membuat dokumentasi kebijakan prosedur secara tertulis, meningkatkan kesadaran SDM.
Teknologi Infrastruktur	
R1	Konfigurasi pada *website* diperbaiki sesuai standar, agar tidak terjadi *take over* akun, membatasi hak akses untuk admin dan kontributornya, serta memasang tools kemanan pihak ke 3 agar bisa mendeteksi insiden sejak dini.
R2	Meningkatkan meningkatkan standar keamanan dan alat atau *tools*, manambahakan cadangan untuk *power* pada *server*.
R3	Memperkuat dukungan teknis terhadap pengelolaan insiden dengan Meningkatkan standar dan alat keamanan TI agar kemanan lebih terjamin.
R4	Meningkatkan kualitas kemanan TI sesuai standar.
R5	Penggunaan teknologi pendukung penggunaan teknologi pendukung atau standar keamanan lainnya juga direkomendasikan untuk meningkatkan kemampuan deteksi dan penanganan insiden keamanan secara dini.
R6	Melakukan *backup* pada database *website* secara berkala menggunakan aplikasi pihak ke 3 untuk keamanan yang lebih baik dengan menggunakan alat yang sesuai dengan standar kemanan TI untuk mendeteksi insiden sejak dini.
R7	Menggunakan aplikasi pihak ke 3 sesuai standar keamanan TI agar bisa mendeteksi insiden sejak dini.
R8	Meningkatkan alat sesuai standar kemanan TI, membatasi hak akses terhadap *server* dan *website.*
R9	Penggunaan teknologi pendukung yng standar keamanan TI juga direkomendasikan untuk meningkatkan kemampuan deteksi dan penanganan insiden keamanan secara dini.
R10	Menggunakan tools pihak ke 3 sesuai dengan standar kemana TI guna meningkatkan keamanan dan mendeteksi insiden sejak dini.

5. KESIMPULAN DAN SARAN

Penelitian menyimpulkan bahwa kesiapan teknologi dan prosedur penanganan insiden PTS di DIY mencapai tahap *managed* hingga *predictable process*, namun belum optimal akibat ketimpangan kapabilitas di mana wilayah Sleman lebih unggul dibandingkan Bantul dan Kota Yogyakarta. Hal ini terlihat dari rentang nilai antar universitas sebesar 1,00 hingga 4,20 yang masih berjarak signifikan dari target level 5 (*optimising process*). Mengingat kelemahan utama terletak pada dokumentasi dan infrastruktur, disarankan agar pihak kampus meningkatkan dokumentasi kebijakan, melengkapi alat berstandar forensik digital, serta melakukan evaluasi berkala.

DAFTAR PUSTAKA

[1] N. Kristianti and R. Kurniasi, "Peraturan dan regulasi keamanan siber di era digital," *Satya Dharma: Jurnal Ilmu Hukum*, vol. 7, no. 1, pp. 297–310, 2024.

[2] A. Irawan, W. H. N. Fadholi, Z. Erikamaretha, and F. Sinlae, "Tantangan dan strategi manajemen keamanan siber di Indonesia berbasis IoT," Journal Zetroem, vol. 6, no. 1, pp. 114–119, 2024.

[3] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It Journal Research And Development*, vol. 3, no. 1, pp. 13–21, Aug. 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[4] A. L. Sariani, "Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia," AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum, vol. 3, no. 1, pp. 54–62, 2025.

[5] T. Rochmadi, "Deteksi bukti digital pada ADrive cloud storage menggunakan live forensik," Cyber Security dan Forensik Digital, vol. 2, no. 2, pp. 65–68, 2019.

[6] S. Nugroho and T. Rochmadi, "Analysis of Information Security Readiness Using the Index

KAMI," *Decode: Jurnal Pendidikan Teknologi Informasi*, vol. 4, no. 3, pp. 881–886, Oct. 2024, doi: 10.51454/decode.v4i3.602.

[7] G. Odhiambo, R. Omollo, and P. Abuonji, "Towards Digital Forensic Readiness: A Framework for Financial Service Providers," East African Journal of Information Technology, vol. 7, no. 1, Apr. 2024.

[8] H. A. Nugroho, O. C. Briliyant, and S. U. Sunaringtyas, "A Novel Digital Forensic Readiness (DFR) Framework for e-Government," IEEE International Conference on Cryptography, Informatics, and Cybersecurity, 2023.

[9] S. Rachmie, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," *LITIGASI*, no. 21, pp. 104–127, Jul. 2020, doi: 10.23969/litigasi.v21i1.2388.

[10] Amsori, Fakhri Awaluddin, and Momon Mulyana, "Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital," *Journal Humaniora: Jurnal Hukum dan Ilmu Sosial* , vol. 02, no. 1, pp. 14–19, 2024.

[11] M. Adhisyanda Aditya, R. Dicky Mulyana, A. Mulyawan, S. LIKMI Bandung, and S. Mardira Indonesia, "Perbandingan Cobit 2019 Dan Itil V4 Sebagai Panduan Tata Kelola Dan Management It," *Jurnal Computech & Bisnis*, vol. 13, no. 2, pp. 100–105, 2019.

[12] M. R. S. Alfarizi, M. Z. Al-farish, M. Taufiqurrahman, G. Ardiansah, and M. Elgar, "Penggunaan Python sebagai bahasa pemrograman untuk machine learning dan deep learning," Karya Ilmiah Mahasiswa Bertauhid (KARIMAH TAUHID), vol. 2, no. 1, pp. 1–6, 2023.

[13] A. Al-Rasyid, I. Atastina, and B. Subagjo, "Analisis audit sistem informasi berbasis COBIT 5 pada domain deliver, service, and support (DSS) (Studi kasus: SIM-BL di Unit CDC PT Telkom Pusat Tbk)," eProceedings of Engineering, vol. 2, no. 2, 2015.

[14] D. Simanjuntak and H. Widi Nugroho, "Evaluasi Tata Kelola Teknologi Informasi pada Siatem informasi bimbingan konseling menggunakan Framework Cobit 2019 dan Balanced Scorecard," *Explore: Jurnal Sistem Informasi dan Telematika*, vol. 15, no. 2, p. 204, Dec. 2024, doi: 10.36448/jsit.v15i2.3882.

[15] M. A. Solikhah, "Pengukuran capability level pada sistem informasi akademik di STAI Kuningan menggunakan COBIT 2019," Jurnal Teknik Indonesia, vol. 3, no. 2, pp. 72–81, 2024.

[16] T. Rochmadi, A. Fadlil, and I. Riadi, "Developing a Delphi validated instrument for assessing digital forensics readiness based on COBIT 2019," International Journal of Advances in Data and Information Systems, vol. 6, no. 3, pp. 749–762, 2025