LAPORAN TUGAS AKHIR

JUDUL PENELITIAN

“Analisis Kebutuhan Dan Perancangan Sistem Informasi Pelaporan Insiden Siber Berbasis Website (Studi Kasus Divisi Persandian dan Keamanan Informasi Dinas Komunikasi dan Informatika Provinsi Jawa Tengah)”

Peneliti

Alwi Kesuma

161708952

UNIVERSITAS ATMA JAYA YOGYAKARTA

Fakultas Teknologi Industri

Program Studi Sistem Informasi

Juli 2020

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

ANALISIS KEBUTUHAN DAN PERANCANGAN SISTEM INFORMASI PELAPORAN INSIDEN SIBER BERBASIS WEBSITE (STUDI KASUS DIVISI PERSANDIAN DAN KEAMANAN INFORMASI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TENGAH)

yang disusun oleh

ALWI KESUMA

161708952

dinyatakan telah memenuhi syarat pada tanggal 08 Juli 2020

		Keterangan
Dosen Pembimbing 1	: Samiaji Sarosa	Telah menyetujui
Dosen Pembimbing 2	: Yohanes Priadi Wibisono, S.T.,M.M.	Telah menyetujui
Tim Penguji		
Penguji 1	: Samiaji Sarosa	Telah menyetujui
Penguji 2	: Aloysius Bagas Pradipta Irianto, S.Kom., M.Eng.	Telah menyetujui
Penguji 3	: Clara Hetty Primasari, S.T., M.Cs	Telah menyetujui

Yogyakarta, 08 Juli 2020

Universitas Atma Jaya Yogyakarta

Fakultas Teknologi Industri

Dekan

ttd

Dr. A. Teguh Siswantoro, M.Sc

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir atau yang disebut dengan Skripsi ini. Skripsi dengan judul "**Analisis Kebutuhan Dan Perancangan Sistem Informasi Pelaporan Insiden Siber Berbasis Website (Studi Kasus Divisi Persandian dan Keamanan Informasi Dinas Komunikasi dan Informatika Provinsi Jawa Tengah)**" disusun sebagai salah satu syarat untuk mendapatkan gelar Sarjana Sistem Informasi di Universitas Atma Jaya Yogyakarta telah diselesaikan oleh penulis dengan sebaik-baiknya.

Dengan selesainya penyusunan skripsi ini, maka dengan rasa hormat dan syukur oleh penulis mengucapkan terima kasih pada semua pihak yang telah memberikan bantuan, bimbingan, waktu, dan pengarahan. Oleh karena itu, dalam kesempatan ini penulis mengucapkan terimakasih yang sebesar-besarnya kepada bapak Samiaji Sarosa, S.E., M.info.Sys., Ph.D. selaku dosen pembimbing skripsi pertama dan bapak Yohanes Priadi Wibisono, S.T., M.M. selaku dosen pembimbing skripsi kedua. Penulis juga berterima kasih kepada keluarga, kerabat dekat dan teman-teman Program Studi Sistem Informasi yang telah memberikan semangat dan dukungannya.

Yogyakarta, …….

Alwi Kesuma

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Penelitian ini bertujuan untuk mengetahui gambaran dari sistem pelaporan insiden siber berbasis website yang diinginkan oleh Dinas Komunikasi dan Informatika provinsi Jawa Tengah khususnya divisi Persandian dan Keamanan Informasi. Permasalahan yang didapatkan akan dianalisis dan disesuaikan dengan kebutuhan dari Koordinator dan *staff* CSIRT Diskominfo Jateng. Peneliti menemukan beberapa masalah terkait pelaporan insiden siber provinsi Jawa Tengah yaitu kurang terdokumentasi dengan baik, tidak adanya progress "*follow up*" ketika adanya penanganan insiden siber kepada pemilik sistem, serta kurangnya pelayanan terkait insiden siber yang mengacu pada Perka BSSN No. 10 Tahun 2019 tentang penyediaan layanan keamanan informasi. Penelitian ini menggunakan metode perancangan SDLC *Waterfall* karena dapat mendeskripsikan tahapan dengan rinci dan terstruktur sesuai dengan karakteristik di lingkup pemerintahan. Penelitian ini berfokus pada tahap analisis dan perancangan yang menggunakan Unified Modeling Language (UML) sebagai alat bantu. Tahap analisis menggunakan alat bantu berupa flowchart untuk merancang proses bisnis pada aplikasi dan use case diagram untuk mendeskripsikan fungsi-fungsi pada aplikasi *website*. Tahap perancangan menggunakan alat bantu berupa Entity Relationship Diagram (ERD), Class Diagram, dan Desain antarmuka. Keluaran dari penelitian ini adalah menghasilkan sebuah rancangan Sistem Pelaporan Insiden Siber (SPIS) berbasis *website* berdasarkan analisis kebutuhan.

Kata Kunci : SDLC; *Waterfall*; Sistem Pelaporan Insiden Siber; Kebutuhan Sistem, *website*.

BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Perkembangan teknologi informasi pada saat ini sangat berpengaruh terhadap kehidupan manusia. Munculnya teknologi komputer modern memberikan mobilitas tinggi terhadap manusia dalam menjalankan kehidupannya. Peningkatan mobilitas dapat berupa memudahkan komunikasi jarak jauh, memudahkan penyebaran informasi, informasi yang dapat didapatkan dimana saja, dan sebagainya. Peningkatan mobilitas dalam memanfaatkan teknologi informasi umumnya dapat dilakukan dengan cara pemanfaatan *smartphone* dan laptop. Mobilitas dalam menggunakan teknologi informasi membutuhkan konektivitas yang memungkinkan pengguna untuk melakukan komunikasi jarak jauh antara satu orang dengan orang lain melalui perangkat komputer yaitu internet.

Internet saat ini digunakan oleh pengguna yang cenderung dengan memanfaatkan PC(*Personal Computer*), *smartphone,* laptop sebagai media untuk berkomunikasi jarak jauh. Dengan adanya komunikasi jarak jauh, banyak pengguna yang dapat melakukan pekerjaan secara *remote*, lingkup pengumpulan data yang menjadi lebih luas, dan sebagainya. Peningkatan kebutuhan akan mobilitas mengakibatkan setiap tahun penggunaan internet semakin meningkat karena dibutuhkannya mobilitas yang tinggi. Berdasarkan *survey* yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pertumbuhan pengguna internet di Indonesia hingga 2017 selama satu dekade mencapai lebih dari 700% [1].

Gambar 1.1 Grafik Pertumbuhan Pengguna Internet di Indonesia Hingga Tahun 2017 [1]

Berdasarkan hasil survei terbaru dari Lembaga yang sama yaitu Asosiasi Penyelanggara Jasa Internet Indonesia (APJII) pada tahun 2018 mengalami peningkatan dibandingkan pada tahun 2017 yaitu peningkatan sebesar 19,48%. Dengan peningkatan yang terjadi setiap tahunnya, tentunya kebutuhan dan jumlah aplikasi memiliki potensi meningkat juga

Gambar 1.2 Penetrasi Pengguna Internet Pada Tahun 2018 [2]

Internet dapat bekerja optimal dalam kehidupan manusia jika adanya aplikasi yang dapat digunakan oleh pengguna untuk melakukan berbagai pekerjaan.

Aplikasi pada umumnya terbagi menjadi tiga jenis *platform* yaitu *desktop*, *mobile*, dan *website*. Aplikasi yang terhubung dengan jaringan internet berpotensi untuk diakses oleh lebih dari satu pengguna dan juga dapat diakses dimanapun tergantung ketentuan yang telah ditetapkan di dalam aplikasi tersebut. Saat ini aplikasi yang cukup mudah digunakan tanpa harus mengunduh aplikasi tersebut yaitu aplikasi berbasis *website.*

Website dapat diakses melalui sebuah aplikasi sebagai perantara dengan cara mengakses alamat URL dari *website* yang akan dituju. Aplikasi perantara yang dimaksud untuk mengakses alamat URL dari berbagai aplikasi berbasis *website* disebut dengan "*browser*" . *Browser* disebut juga dengan peramban *web* atau *web browser* yang memiliki kemampuan untuk merepresentasikan *source code* dari sebuah *website* seperti HTML, CSS, Javascript, dan lain sebagainya menjadi tampilan serta fungsi layaknya sebuah aplikasi independen.

Aplikasi berbasis *website* adalah aplikasi yang dapat diakses dalam jaringan dengan cara di *hosting* sehingga aplikasi tersebut dapat diakses melalui alamat *Uniform Resource Locator* (URL) menggunakan *browser* tanpa harus mengunduh aplikasi tersebut. *Website* pada umumnya memiliki keuntungan bagi pengguna salah satunya adalah mudah untuk diakses. Pada umumnya sistem operasi di setiap *device* seperti *Personal Computer*(PC), *Smartphone* dan Laptop telah menyediakan *browser* untuk dapat mengakses *website*. Dengan adanya *browser*, pengguna cenderung dapat mengakses banyak aplikasi yang berbasis *website* dimanapun dan kapanpun.

Website dapat menjadi salah satu strategi marketing untuk mempromosikan perusahan terkait produk ataupun jasa yang ditawarkan karena penyebarannya lebih luas, lebih murah, dan lebih efektif [3]. Penyebaran dikatakan lebih efektif karena saat ini telah memasuki zaman teknologi dimana informasi banyak tersebar di dunia maya. Berdasarkan studi yang dilakukan oleh Nielson bersumber dari Katadata[4], di Indonesia jumlah pembaca media digital telah melampaui jumlah pembaca media cetak masing-masing dengan jumlah 6 juta orang dan 4,5 juta orang. Orang-orang yang mendapatkan informasi melalui media digital khususnya dari internet pada tahun 2017 berjumlah 43% atau 2.58 juta pengguna. Hasil studi tersebut menyatakan

bahwa semakin banyak masyarakat di Indonesia yang memilih mendapatkan informasi dari media digital.

Pengguna media digital yang dimaksud tentunya juga termasuk dari pengguna website dan media lainnya. Saat ini website yang tersebar di internet memiliki jumlah yang banyak, berdasarkan temuan yang dilakukan oleh Pengelola Nama Domain Internet Indonesia (PANDU) di Indonesia tercatat kurang lebih 318.000 *domain website* di tahun 2019 [7]. Dengan banyaknya jumlah *domain website* di Indonesia, maka tidak menutup kemungkinan bahwa potensi serangan siber yang terjadi pada website juga berjumlah besar. Seluruh aplikasi *website* yang ada saat ini tidak sepenuhnya sempurna dan berpotensi mendapat serangan dari berbagai pihak yang tidak bertanggung jawab. Serangan-serangan siber seperti *deface*, *phishing*, *SQL Injection*, *Backdoor attack*, dan lain sebagainya menyerang kerentanan yang ada pada *website* yang dituju.

Gambar 1.3 Jumlah Serangan Siber Yang Terjadi Di Indonesia Tahun 2018 [5]

Gambar 1.4 Sumber Serangan Siber Yang Terjadi Di Indonesia Tahun 2018 [5]

Berdasarkan data yang telah disajikan oleh Badan Sandi dan Siber Negara (BSSN) terkait jumlah serangan siber pada tahun 2018, jumlah serangan siber selama satu tahun yang terjadi di Indonesia adalah lebih dari tiga belas juta serangan dari serangan *hacker* maupun serangan *malware*. Data yang disajikan oleh BSSN cukup untuk menyatakan bahwa butuhnya tenaga ahli yang dapat menjaga keamanan-keamanan aplikasi di Indonesia yang tersebar di dunia maya. Tenaga ahli yang dimaksud dapat disebut dengan *Penetration Tester*(PenTester). PenTester berfungsi untuk menangani insiden dari aplikasi yang terkena serangan siber serta memberikan rekomendasi ataupun memberi perbaikan kepada aplikasi-aplikasi yang terkena serangan siber.

Dinas Komunikasi dan Informatika (Diskominfo) provinsi Jawa Tengah adalah organisasi pemerintahan yang melayani masyarakat provinsi Jawa Tengah terkait komunikasi, persandian, dan statistik. Pekerjaan terkait pelayanan persandian ditangani oleh divisi Persandian dan Keamanan Informasi dimana divisi ini memiliki fokus pekerjaan yang menjurus pada keamanan informasi. Divisi tersebut memiliki PenTester yang berfungsi untuk memberikan pelayanan penanganan insiden siber di Jawa Tengah termasuk kepada Organisasi Pemerintahan Daerah (OPD).

Berdasarkan wawancara yang dilakukan penulis bahwa PenTest akan dilakukan dalam 3 jenis yaitu *by request*, *by incident*, dan *Routine*. PenTest *Routine* dilakukan khusus untuk Organisasi Pemerintahan Daerah (OPD) dan telah terdokumentasi dengan baik. Menurut Pak Subroto pada skrip wawancara nomor 4, PenTest *by request* dan *by incident* dilakukan ketika adanya pengajuan dari pihak pemilik aplikasi melalui email, namun proses *follow up* dilakukan melalui Whatsapp sehingga pelaporan insiden siber tidak terdokumentasi dengan baik. Menurut penanggung jawab PenTest, dokumentasi tidak dilakukan dengan optimal karena tidak adanya prosedur *follow up* yang terdokumentasi secara lebih rinci dan tidak jelas terkait pelaporan penanganan insiden siber karena koordinasi dengan pelapor hanya dilakukan melalui aplikasi WhatsApp [35]. Hal tersebut mengingatkan bahwa dokumentasi yang rinci sangatlah diperlukan di dalam organisasi pemerintahan. Dengan adanya dokumentasi yang lebih rinci, maka diharapkan dapat meningkatkan *score* dari berbagai *assessment* yang nantinya membutuhkan dokumentasi dan

mendukung perkembangan *Cyber Security Incident Response Team*(CSIRT) provinsi Jawa tengah.

Kebutuhan Koordinator CSIRT terhadap sistem pelaporan insiden siber diharapkan bersifat responsive dan pembangunan sistem dilakukan tanpa memikirkan jenis sistem operasi seperti iOS, Windows, Android, dan sebagainya [8][35]. Pengguna yang diperbolehkan untuk melaporkan insiden siber kepada Diskominfo Jateng adalah OPD Jateng dan masyarakat umum Jawa Tengah. Pelaporan insiden siber di Jawa Tengah tidak menggunakan *tools* seperti *Security Information and Event Management* (SIEM) dan lain sebagainya. Hal tersebut dikarenakan *tools* seperti itu hanya dapat bekerja jika telah *embeded* ke dalam sistem [6], selain itu pemilik *website* masyarakat di Jawa Tengah tidak seluruhnya menerapkan *tools* terkait pelaporan insiden siber. Insiden siber yang terjadi pada website milik masyarakat Jawa Tengah yang tidak dapat ditangani secara pribadi dapat dilaporkan secara manual kepada Dinas Komunikasi dan Informatika provinsi Jawa Tengah.

Sistem pelaporan insiden siber dapat diterapkan karena didukung oleh Perka BSSN No. 10 Tahun 2019 tentang pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, disebutkan bahwa Penyelenggaraan Persandian untuk Pengamanan Informasi Pemda berupa pengamanan sistem elektronik dan non elektronik serta penyediaan layanan keamanan informasi. Dengan diterapkannya sistem pelaporan insiden siber diharapkan pihak eksternal Diskominfo Jawa tengah dan masyarakat umum dapat berperan dalam memantau serta melaporkannya jika terjadi insiden siber yang tidak dapat menangani sendiri. Hal tersebut bertujuan untuk dapat segera menangani insiden siber tersebut dan setiap langkah yang dikerjakan dalam penanganan insiden siber dapat terdokumentasikan dengan baik.

Dengan adanya analisis kebutuhan dan dirancangnya sebuah sistem diharapkan data-data terkait pelaporan insiden siber menjadi lebih aman dikarenakan data-data yang tersimpan di Whatsapp milik karyawan yaitu Koordinator CSIRT memiliki risiko yang lebih besar. *Device* milik Koordinator CSIRT adalah *device* pribadi sebagai *device daily driver* yang berpotensi membuat data menjadi kurang aman seperti terhubung dengan jaringan internet diluar dari jaringan Diskominfo

Jateng yang tidak diketahui tingkat keamanannya, aplikasi-aplikasi yang dapat mencatat log aktivitas device, potensi *device* rusak yang tidak ada manajemen penanganannya, dan lain sebagainya. Sistem pelaporan insiden siber yang tersimpan di service milik pemerintahan Diskominfo Jateng juga telah memasang Honeypot pada jaringan miliknya dengan tujuan lebih meningkatkan keamanan terhadap seluruh sistem yang ada di server dan jaringannya. Menurut cyberthreat.id, Honeypot adalah sebuah sistem yang dirancang untuk menjaring penyerang seolah2 bekerja seperti sistem yang ditarget oleh penyerang namun tanpa disadari penyerang telah masuk kedalam perangkap. Honeypot juga dapat bekerja sebagai indikator deteksi jika terjadi serangan sehingga sistem-sistem yang ada akan lebih terjaga (termonitor) dengan baik.

1.2. RUMUSAN MASALAH

Penulis merumuskan persoalan yang akan diangkat dalam penelitian ini dalam bentuk pertanyaan yaitu :

1. Bagaimana masyarakat dapat melaporkan insiden siber yang terjadi pada websitenya dengan mudah dan dapat ditangani oleh pihak terpercaya?
2. Bagaimana Pelaporan Insiden Siber provinsi Jawa Tengah dapat didokumentasi dengan baik?
3. Bagaimana Dinas Komunikasi dan Informatika provinsi Jawa Tengah dalam merancang sistem yang dibutuhkan untuk meningkatkan pelayanan terkait pelaporan insiden siber?

1.3. BATASAN MASALAH

Penelitian ini tertuju pada Dinas Komunikasi dan Informatika provinsi Jawa Tengah untuk meningkatkan dokumentasi pelaporan insiden siber, membantu perkembangan pembentukan Cyber Security Incident Response Team (CSIRT), dan meningkatkan pelayanan kepada masyarakat provinsi Jawa Tengah terkait Pelaporan Insiden Siber.

1.4. TUJUAN PENELITIAN

Penelitian ini ditujukan untuk menemukan jawaban berdasarkan rumusan masalah yang telah ditentukan, yaitu :

1. Mengetahui cara untuk memberikan kemudahan bagi masyarakat provinsi Jawa Tengah untuk melaporkan insiden siber.
2. Mengetahui dokumentasi terkait pelaporan insiden siber dapat dilakukan dengan baik.
3. Mengetahui cara menggali kebutuhan dan merancang sistem berbasis website Pelaporan Insiden Siber sesuai dengan kebutuhan Dinas Komunikasi dan Informatika provinsi Jawa Tengah.

1.5. MANFAAT PENELITIAN

Berdasarkan permasalahan yang diangkat dan tujuan penelitian yang telah ditentukan, maka manfaat dari penelitian diharapkan yaitu :

1. Memberikan ide dan solusi kepada divisi Persandian dan Keamanan Informasi Dinas Komunikasi dan Informatika terkait pelaporan insiden siber yang lebih terdokumentasi dengan baik serta dapat dilakukan oleh masyarakat selain Organisasi Pemerintahan Daerah (OPD).
2. Memberikan potensi peningkatan pelayanan masyarakat kepada Dinas Komunikasi dan Informatika provinsi Jawa Tengah.
3. Hasil penelitian dapat digunakan oleh civitas Universitas Atma Jaya Yogyakarta untuk melakukan riset lebih lanjut terkait pelaporan insiden siber yang lebih efektif dan efisien.

BAB II

TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Studi yang dilakukan oleh Agum Septian Gumelar terkait Analisa Kebutuhan dan perancangan Sistem Informasi Produksi Dinas Peternakan dan Kesehatan Hewan Kabupaten Malang Berbasis Teknologi *Service Oriented Architecture* (SOA) menyatakan bahwa perancangan sistem merupakan salah satu tahap dasar dalam pengembangan sistem. Pelaporan informasi terkait perkembangan peternakan ternak, pakan, dan budidaya yang ada di kabupaten malang kepada pusat pemerintahan Malang. Penerapan sistem pelaporan dibutuhkan karena *sharing data* kurang *update* dan perekapan data yang kurang efektif dan efisien. Dengan diterapkannya sistem berbasis SOA dapat memaksimalkan kegiatan pelaporan [24]. Penelitian dilakukan dengan cara menganalisis kebutuhan, merancang sistem, memastikan konsistensi, dan memastikan memenuhi beberapa kriteria SOA. Kebutuhan sistem dilakukan dengan cara observasi, *interview*, dan studi pustaka.

Penelitian dilakukan dengan metodologi *Ripple* yang menghasilkan definisi dari kebutuhan dan artefak perancangan, kemudian proses pengujian perancangan dan *Service Litmus Test* untuk mengetahui apakah perancangan sudah memenuhi beberapa kriteria pada SOA. Pengujian terkait konsistensi menghasilkan sebuah nilai *Requirement Consistency Index* (RCI) dan memenuhi persamaan pada *business alignment* serta *reusable* pada *litmus test*. Artefak yang dihasilkan dari perancangan sistem meliputi : *user interface sketch, communication diagram, class diagram, sequence diagram,* dan *database schema*. Pengujian konsistensi pendefinisian kebutuhan menghasilkan nilai RCI 100% yang berarti sistem sudah konsisten dengan sempurna.

Studi kasus terhadap suatu toko yang dilakukan oleh [25] mengenai Analisis dan Perancangan Sistem Informasi Toko Untuk Mencapai Keunggulan Kompetitif menyatakan bahwa penelitian bertujuan untuk mengetahui proses bisnis secara umum terkait pencatatan data barang dan data transaksi, menganalisis

permasalahan yang ada pada saat ini, dan untuk mengembangkan sistem informasi pada lingkup perencanaan sistem informasi. Metode penelitian yang digunakan oleh penulis adalah metode deskriptif kualitatif. Sumber data yang dipakai adalah data primer yang dilakukan melalui *interview* dan observasi serta data sekunder didapatkan dari dokumen-dokumen yang diperoleh langsung dari toko lokasi penelitian. Data yang telah didapatkan dianalisis menggunakan metode analisis data tiga tahap oleh Miles dan Huberman yang meliputi *data reduction*, *data display*, dan *conclusion:drawing/verification*.

Proses analisis pada penelitian dimulai dari deteksi masalah, investigasi awal, analisis kebutuhan, menentukan dan memilih sistem yang tepat, dan analisis kelayakan sistem. Proses perancangan sistem meliputi perancangan *output*, perancangan *input*, perancangan proses, perancangan *database*, dan *design* tampilan sistem. Berbagai proses analisis dan perancangan yang dilakukan didapatkan hasil bahwa adanya sistem yang diterapkan saat ini namun masih bersifat manual dalan pencatatan dan pengelolaan data sehingga perlu adanya pengembangan sistem yang lebih memadai dalam pengelolaan data untuk meningkatkan keunggulan strategis, taktis, dan operasional.

2.2. DASAR TEORI

Internet merupakan jaringan komputer terbesar di dunia yang dapat menghubungkan jutaan piranti komputer berdasarkan jaringan yang telah ditentukan [9]. Jaringan yang dimaksud adalah konektivitas yang menghubungkan dua atau lebih sistem komputer [9]. Internet adalah kombinasi antara interaksi tekstual dan dunia virtual yang memungkinkan komunikasi manusia secara global. Implikasi mengakses internet terkait jumlah dan interaksi dapat semakin mendalam. Bahkan bukan hanya peluang manusia berinteraksi di internet tetapi rasa dan keterlibatan sosial yang menjadi berbeda [13]. Dengan terhubungnya banyak piranti komputer, perlu adanya *software* aplikasi untuk dapat melaksanakan pekerjaan yang dapat dilakukan oleh banyak orang pada waktu yang sama dan hasil pekerjaannya tersimpan di dalam *database* aplikasi tersebut. Pekerjaan-pekerjaan tersebut dapat

dilakukan dimanapun dan kapanpun sesuai dengan jam operasional serta hak akses yang telah ditentukan.

IT*(Information Technology) Platform* merupakan produk terintegrasi atau rangkaian produk yang mencakup server aplikasi, server portal, *software* untuk Service Oriented Architecture (SOA), dan Business Process Management (BPM). Beberapa *platform* juga menyertakan *database* dan business intelligence untuk analisis dan pelaporan [6]. *Platform* dalam lingkungan teknologi Informasi sebagai dasar dari teknologi yang dapat digunakan untuk bekerja dengan satu atau banyak pengguna. *Platform* pada umumnya seperti *mobile, desktop,* atau *website* yang membutuhkan sistem operasi untuk menjalankan aplikasi. Aplikasi *website* memiliki kebutuhan khusus dibandingkan kedua *platform* lainnya yaitu membutuhkan aplikasi perantara untuk dapat menjalankannya. Aplikasi perantara yang dimaksud untuk menelusuri alamat URL dari sebuah aplikasi *website* adalah *web browser* atau *browser*.

Web Browser merupakan salah satu *tools* yang digunakan sebagai "pintu" untuk mengakses alamat URL dari sebuah *website* [14]. Browser adalah sebuah *software* perantara dijalankan oleh pengguna untuk menampilkan hasil komputasi dokumen atau informasi *web* yang diambil dari *web server* [15]. Web Browser berperan sebagai antarmuka antara pengguna dan *web server* untuk mengambil dan menyajikan sumber informasi di dunia maya yang teridentifikasi oleh Uniform Resource Identifier (URL) dimana kontennya berupa gambar, tulisan, video, teks, dan lain sebagainya [16].

Menurut [17], Website adalah dokumen-dokumen yang ditulis dengan format HyperText Markup Language (HTML) yang dapat diakses melalui HyperText Transfer Protocol (HTTP). HTTP merupakan protokol untuk mengirim informasi dari *web server* ke *web browser* untuk menampilkan dokumen HTML bersifat statis maupun dinamis yang membentuk satu rangkaian saling berkaitan dengan jaringan. Website atau dapat disebut dengan situs adalah kumpulan dari berbagai halaman yang menampilkan informasi teks berupa data seperti gambar, video, teks, dan lainnya bersifat statis maupun dinamis membentuk rangkaian yang terhubung dengan jaringan-jaringan di halamannya [18].

Menurut [19], *Cyber Crime* atau kejahatan siber merupakan salah satu tindakan pelanggaran terhadap data, sistem, dan jaringan internet yang terhubung dengan komputer. *Cyber Crime* termasuk memasukkan, mentransmisikan, merusak, menghapus, mengubah, atau menekan data komputer, serangan virus, dan lain serangan lainnya. Definisi *Cyber Crime* cenderung seperti membaca daftar belanjaan yang gagal diantisipasi dari berbagai jenis kriminal di dunia maya [20]. Menurut [21], Gordon dan Ford menyatakan bahwa Cyber Crime adalah kejahatan di dunia maya yang berkembang berdasarkan pengalaman. Dengan berkembangnya teknologi terus menerus maka pelaku *Cyber Crime* akan menjadi lebih canggih lagi dalam berbuat kriminal.

Cyber Security atau keamanan siber didefinisikan sebagai teknologi dan proses yang dibangun untuk melindungi *hardware*, *software*, *network*, dan data dari berbagai akses yang tidak diizinkan dari *Cyber Crime [22]*. Menurut [23], *Cyber Security* terkait dengan melindungi peralatan digital berbasis internet, jaringan, dan informasi anda dari perubahan yang tidak sah. Internet menawarkan banyak manfaat dan memberikan berbagai kesempatan untuk memudahkan proses berjalannya bisnis di seluruh dunia namun internet dasarnya tidak pernah dirancang untuk melacak serangan siber dan melacak perilaku pengguna melainkan yang dapat melacak adalah jaringan.

Pelaporan *Cyber Incident*(Insiden Siber) perlu adanya penanganan yang terencana dan terorganisir sehingga dapat dilaksanakan secara terdokumentasi untuk setiap penanganan dan insiden yang dilaporkan. Panduan terkait pelaporan insiden siber khususnya di sektor pemerintahan telah dibuat dan ditetapkan oleh Badan Sandi dan Security Negara(BSSN). Prosedur pelaporan insiden secara umum yang telah ditentukan dimulai dari verifikasi insiden siber, *approvement*, laporan insiden siber, respon insiden, *open ticket*, dan *close ticket* [27].

Pengaduan insiden siber ke pihak penanganan insiden siber dapat dilakukan melalui layanan yang tersedia seperti email maupun aplikasi yang telah disediakan. Pelaporan insiden siber yang diterima akan diverifikasi terlebih dahulu terkait data-data lengkap identitas pengelola *website*, jenis insiden, log aplikasi, dan dampak yang terjadi akibat insiden tersebut. Tahap verifikasi bertujuan untuk identifikasi insiden

yang terjadi dan melakukan dokumentasi. *Approvement* adalah tahap disetujui atau tidaknya pelaporan insiden siber guna untuk penanganan insiden selanjutnya. Pelaporan insiden siber yang telah di *approve* maka akan diberlakukan sistem *open ticket* yang berisi informasi mengenai nomor tiket insiden dan informasi terkait penanganan insiden. Ticket yang telah dibuat akan dilanjutkan ke tim CSIRT(*Cyber Security Incident Response Team*). Ticket ini bertujuan untuk melakukan manajemen laporan insiden dan monitoring terkait sejauh mana insiden ditangani [27].

Respon insiden berfungsi untuk koordinasi dengan pihak pengelola website untuk memberikan panduan terkait penanggulangan dan pemulihan *website*. Jika perlu adanya tindakan khusus, maka tim CSIRT dapat melakukan membantu pemulihan secara *on-site*. Close ticket berfungsi untuk pemantauan oleh tim CSIRT terhadap pemulihan website yang terkena insiden siber. Jika insiden dapat diatasi maka *close ticket* dapat dilakukan [27].

UML adalah sebuah model pengembangan sistem perangkat lunak yang menggunakan pendekatan berbasis objek. Saat ini UML terdiri 2 aspek yaitu aspek perilaku dan aspek struktural. Aspek perilaku mendeskripsikan perubahan yang terjadi pada sistem seiring perubahan waktu. Aspek struktural merupakan konsep dari sebuah aplikasi yang mendefinisikan struktur dari elemen membentuk sistem tanpa ada kaitan dengan waktu [30].

Use Case Diagram merupakan diagram UML yang memberikan visualisasi interaksi yang terjadi antara aktor (pengguna) dengan sistem. Diagram ini cukup baik untuk menjelaskan konteks dari sebuah sistem sehingga batasan-batasan yang dapat dilakukan antara aktor dengan sistem [28].

Entity Relationship Diagram adalah sebuah alat analisis untuk merancang diagram data sebagai tempat penyimpan data dari sistem yang akan dibangun [31].

Class Diagram pada UML adalah jembatan antara spesifikasi perangkat lunak di sisi pengguna dengan realisasi pengembangan perangkat lunak di sisi pengembang sehingga perlu adanya pedoman yang kuat untuk mengidentifikasi kelas objek berdasarkan masalah [32].

BAB III

METODOLOGI PENELITIAN

3.1. Waktu Penelitian

Penelitian akan dilakukan dari bulan Februari tahun 2020 hingga bulan Mei tahun 2020.

3.2. Lokasi Penelitian

Penelitian ini berlokasi di Dinas Komunikasi dan Informatika provinsi Jawa Tengah dan Laboratorium Teknologi dan Sistem Informasi (ITSI) Universitas Atma Jaya Yogyakarta.

3.3. Metode Penelitian

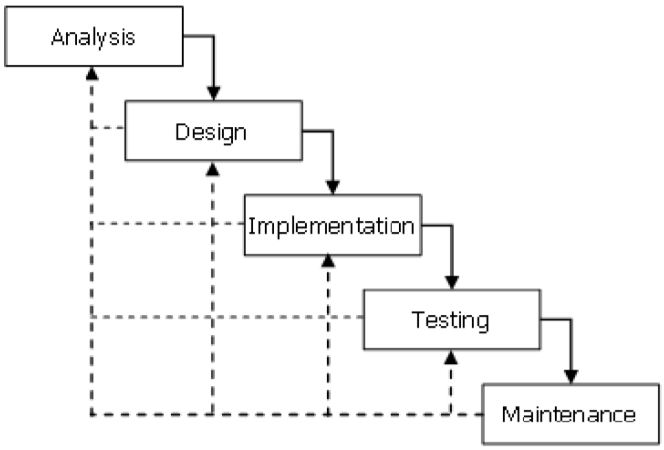
Perancangan Sistem Pelaporan Insiden Siber membutuhkan suatu metode perancangan sehingga fase-fase perancangan dari awal dapat berjalan hingga menghasilkan produk. Metode yang digunakan untuk merancang Sistem Pelaporan Insiden Siber adalah System Development Life Cycle (SDLC). SDLC merupakan metode yang mencakup seluruh proses terkait sistem dimulai dari tahap membangun (*build*), menyebarkan (*deploy*), menggunakan (*use*), dan memperbarui (*update*)[29]. Salah satu model yang digunakan untuk mendukung tahapan SDLC adalah metode *Waterfall*.

SDLC model *Waterfall* adalah proses pembangunan perangkat lunak dimana setiap kemajuan dianggap mengalir ke bawah mirip air terjun. Model ini mendefinisikan urutan fase yang harus diselesaikan satu demi satu untuk dapat melanjutkan fase berikutnya. Pada dasarnya, SDLC model Waterfall terdiri dari lima fase yaitu analisis, desain, implementasi, pengujian, dan pemeliharaan[33]. Pada penelitian ini hanya sampai pada tahap desain, tahap implementasi dan pengujian

sebenarnya telah dilakukan, namun pada penelitian ini hanya fokus pada analisis dan desain. Fase pemeliharaan dilakukan oleh Diskominfo Jateng.

Terdapat beberapa alasan mengapa penelitian ini menggunakan Metode Pengembangan SDLC model Waterfall, antara lain proses yang lebih mudah dipahami dan teratur serta adanya kesesuaian karakteristik dengan projek pada pembangunan sistem pelaporan insiden siber. Proyek pemerintahan biasanya memiliki birokrasi yang panjang dan rumit sehingga membutuhkan dokumentasi yang jelas, lebih terstruktur, dan mudah dipahami. SDLC model waterfall sesuai dengan kriteria tersebut karena mengutamakan requirement yang telah didefinisikan saat proses Requirement Gathering dalam pembangunan sebuah sistem. Dengan memakai SDLC model waterfall, proses pengelolaan proyek menjadi lebih mudah dan deskripsi kebutuhan sistem juga menjadi lebih jelas. Selain itu, SDLC model Waterfall digunakan karena memiliki kesesuaian karakteristik dengan project pada pembangunan sistem pelaporan insiden siber. Hal ini dikarenakan model Waterfall mengutamakan requirement terhadap pembangunan sistem, dokumentasi yang terstruktur dan mudah dipahami [37].

Penggunaan SDLC model Waterfall juga di dukung dari hasil observasi saat penulis mengamati proses pelaporan insiden siber yang sedang berlangsung sembari menjadi asisten auditor Indeks KAMI, penulis mengumpulkan beberapa dokumen yang diperlukan salah satunya dokumen perancangan sistem informasi yang bersifat rahasia. Dokumen tersebut saat diminta dan di verifikasi ternyata menunjukkan bahwa perancangan-perancangan sistem yang terdokumentasi cenderung menggunakan SDLC model Waterfall. Berdasarkan informasi yang didapatkan, bahwa karyawan yang ada di Diskominfo provinsi jateng cenderung lebih terbiasa dengan SDLC Waterfall karena seringnya penggunaan model tersebut.



Gambar 3.1 SDLC model *Waterfall*

Rouyce, W (1970 dalam Y, Bassil. 2011:2) menyatakan fase SDLC menggunakan model Waterfall sebagai berikut [33]:

a. Fase Analisis

Sering dikenal dengan *Software Requirements Specification*(SRS) yang merupakan deskripsi lengkap dari sifat sistem yang akan dibangun. Hal itu melibatkan analisis bisnis dan sistem untuk mendefinisikan kebutuhan fungsional dan non-fungsional. Kebutuhan fungsional ditentukan menggunakan *Use Case Diagram* untuk menggambarkan interaksi antara pengguna dengan perangkat lunak. Kebutuhan non-fungsional mengacu pada kinerja, keandalan, ketersediaan, keamanan, pemeliharaan, dan kegunaannya. Pada fase analisis akan dilampirkan flowchart *current state* sebagai acuan untuk menyelaraskan proses bisnisnya dengan SPIS.

b. Fase Design

Fase ini merupakan proses perencanaan dan pemecahan masalah untuk menghasilkan solusi perangkat lunak. Pada tahapan ini melibatkan pengembang perangkat lunak dan desainer untuk menentukan rencana terkait desain algoritma, desain arsitektur perangkat lunak, skema konseptual database, desain konsep, dan *Graphical User Interface* (GUI).

c. Fase Implementation

Fase ini mengacu pada realisasi kebutuhan bisnis dan spesifikasi desain ke dalam pemrograman, database, situs web, atau komponen perangkat lunak lainnya. Dengan kata lain, fase ini merupakan konversi dari seluruh kebutuhan dan hasil analisis ke dalam proses pembuatan sistem.

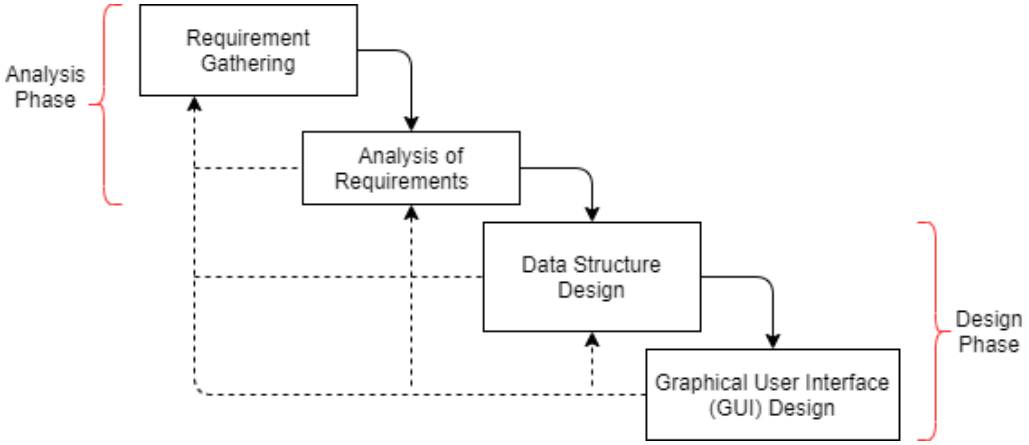
d. Fase Testing

Fase ini merupakan tahapan verifikasi dan validasi bahwa solusi perangkat lunak yang ditawarkan telah memenuhi kebutuhan bisnis dan spesifikasi yang relevan. Verifikasi ini adalah proses mengevaluasi perangkat lunak untuk menentukan apakah produk perangkat lunak tersebut memenuhi kondisi yang ditentukan. Jika saat pengujian berlangsung terdapat *bug* atau gangguan sistem, maka dapat dilakukannya perbaikan dan penyempurnaan yang sesuai.

e. Fase Maintenance

Fase ini adalah proses memodifikasi solusi perangkat lunak untuk menyempurnakan *output*, memperbaiki *error* sistem yang muncul secara tiba-tiba atau bahkan tidak terlihat, meningkatkan kinerja dan kualitas. Kegiatan pemeliharaan ini adalah untuk mengakomodasi kebutuhan baru dari pengguna seiring berjalannya waktu serta meningkatkan keandalan perangkat lunak.

Berdasarkan model diatas, penelitian ini fokus pada tahapan analisis dan design, sehingga memunculkan rincian terkait 2 tahapan tersebut pada metode SDLC .



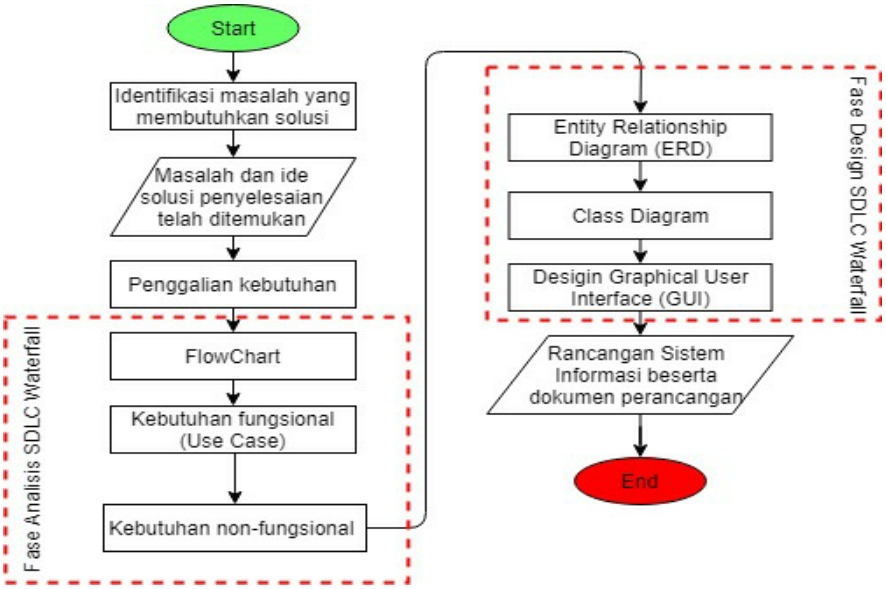
Gambar 3.2 Rincian fokus penelitian menggunakan SDLC model *Waterfall*

Tahapan penelitian terkait analisis kebutuhan dan perancangan mengacu pada SDLC model Waterfall. Penggalian kebutuhan berfungsi untuk mengumpulkan informasi terkait kebutuhan sistem dari CSIRT Diskominfo Jateng. Informasi kebutuhan yang didapatkan pada hasil observasi dan wawancara akan dipetakan dan direpresentasikan pada tahap analisis kebutuhan menggunakan Flowchart, Use Case Diagram sebagai kebutuhan fungsional, dan kebutuhan non-fungsional. Tahap perancangan menggunakan fase *design* pada model Waterfall dimana tahapan yang dilakukan merancangan struktur database menggunakan Entity Realtionship Diagram (ERD), Class Diagram digunakan untuk merepresentasikan alur data yang terjadi di balik layar saat sistem sedang berproses, serta Design Graphical User Interface (GUI) untuk merepresentasikan tampilan sistem yang kedepannya akan dibangun.

Penelitian ini menggunakan salah satu jenis data sebagai sumber analisis dan perancangan yaitu data primer. Data Primer diperoleh dari observasi, wawancara, ataupun kuesioner [26]. Dalam penelitian ini yang menjadi data primer adalah informasi dari wawancara dan observasi yang berkaitan dengan kebutuhan pelaporan insiden siber dari masyarakat dan OPD kepada Diskominfo Jateng. Peneliti melakukan observasi dan melontarkan beberapa pertanyaan secara informal terhadap CSIRT Diskominfo Jateng terkait proses pelaporan serta penanganan insiden siber untuk mengetahui kebutuhan dan permasalahan yang dialami. Proses observasi sering dapat dilakukan karena

lokasi magang penulis berada satu divisi dengan karyawan yang menangani pelaporan insiden siber.

3.4. Tahapan Penelitian



Gambar 3.3 Tahapan Penelitian

Pencarian masalah dilakukan sebagai tahap awal penelitian terhadap Dinas Komunikasi dan Informatika provinsi Jawa Tengah khususnya divisi Persandian dan Keamanan Informasi. Hal ini dilakukan dengan tujuan untuk mencari masalah yang benar-benar membutuhkan solusi penanganan. Setelah masalah ditemukan maka akan dilakukan penggalian kebutuhan dengan metode wawancara maupun kuesioner untuk mengetahui apa yang dibutuhkan oleh divisi Persandian dan Keamanan Informasi dalam mengatasi masalah yang ada. Berdasarkan data dan informasi yang didapatkan dari hasil *requirement gathering* selanjutnya kebutuhan dianalisis sehingga dapat memberikan solusi yang tepat sasaran berdasarkan masalah dan kebutuhan dari divisi Persandian dan Keamanan Informasi. Hasil dari analisis kebutuhan akan di eksekusi berupa berbagai tahap dalam perancangan sistem sehingga menghasilkan rancangan untuk sebuah sistem beserta dokumentasinya.

Model perancangan Waterfall yang diterapkan akan didukung menggunakan *Unified Modeling Language* (UML) sebagai alat pendukung untuk merancang sistem

yang telah direncanakan. Terdapat beberapa diagram UML yang digunakan untuk merancang sekaligus mendeskripsikan batasan-batasan terkait apa saja yang dapat dilakukan oleh pengguna dan sistem. Diagram yang digunakan pada penelitian adalah *Use Case Diagram*, *Entity Relationship Diagram* (ERD), dan *Class Diagram*. Sistem Database sering di rancangan menggunakan *Entity Relationship Diagram*(ERD) karena dapat merepresentasikan "*blueprint*" dari aliran data pada sistem. Class diagram digunakan untuk merepresentasikan bagaimana proses sistem yang terjadi di balik layar terkait alur data.

BAB V

KESIMPULAN DAN SARAN

5.1.Kesimpulan

Pembahasan penelitian ini dalam bab sebelumnya menjawab rumusan masalah yang ada, sehingga dapat disimpulkan sebagai berikut.

1. Berdasarkan hasil observasi dan wawancara yang telah dilakukan terhadap CSIRT Dinas Komunikasi dan Informatika (Diskominfo) provinsi Jawa Tengah bahwa dibutuhkannya sebuah *platform* pelaporan insiden siber yang tidak membutuhkan spesifikasi *device* yang ketat dalam penggunaannya sehingga dapat digunakan oleh masyarakat umum dan OPD provinsi Jawa Tengah dalam melaporkan serangan siber yang terjadi pada aplikasi milik mereka khususnya aplikasi *website*. Dengan adanya Sistem Pelaporan Insiden Siber berbasis *website*, warga di provinsi Jawa Tengah dapat dengan mudah melaporkan serangan siber dan mendapat penanganan dari Diskominfo Jateng sebagai pihak yang dapat dipercaya.
2. Pelaporan insiden siber menggunakan sebuah sistem membuat seluruh pelaporan serangan siber yang telah dilakukan oleh OPD maupun pengguna umum provinsi Jawa Tengah dapat terdokumentasi secara rinci dan tersimpan dengan baik serta dapat direpresentasikan pada tampilan yang konsisten pada sistem yang telah dirancang.
3. Berdasarkan hasil dari pembahasan pada penelitian ini, kebutuhan Diskominfo Jateng untuk meningkatkan pelayanan keamanan informasi pada Perka BSSN No. 10 Tahun 2019 dilakukan dengan cara menganalisis kebutuhan CSIRT Diskominfo Jateng didapat melalui melalui wawancara dan observasi lapangan. Hasil analisis akan digunakan untuk merancang sistem yang dimaksud menggunakan System Development Life Cycle (SDLC) konsep Waterfall dan diagram Unified Modeling Language(UML) sebagai alat pendukung. SDLC konsep Waterfall digunakan digunakan karena prosesnya lebih mudah dipahami dan lebih teratur, pengelolaan proyek menjadi lebih mudah dan

deskripsi kebutuhan sistem lebih jelas karena di dalam lingkup pemerintahan terdapat birokrasi yang panjang dan rumit sehingga membutuhkan dokumentasi yang jelas, lebih terstruktur, dan mudah dipahami.

5.2.Saran

Hasil penelitian yang diperoleh dari pembahasan, diharapkan kepada peneliti yang mengangkat topik sama dengan penelitian ini di kemudian hari menjadi lebih baik, yaitu:

1. Penelitian selanjutnya dapat melanjutkan ke fase-fase berikutnya terkait SDLC konsep Waterfall yaitu sampai pada fase maintenance sehingga analisis, pengembangan hingga pemeliharaan memiliki dokumentasi yang lengkap dan menjadi salah satu aset dokumen bagi Diskominfo Jateng serta berguna dalam pengembangan lebih lanjut oleh Diskominfo Jateng.
2. Penelitian selanjutnya dapat menghitung keuntungan-keuntungan dari segi waktu dan financial setelah implementasi sistem telah dilakukan. Hal ini bertujuan untuk memberikan informasi baru bagi Diskominfo Jateng sehingga dapat memutuskan *upgrade* apa yang harus diterapkan di kemudian hari.

DAFTAR PUSTAKA

[1] Asosiasi Penyelenggara Jasa Internet Indonesia, "Penetrasi Dan Perilaku Pengguna Internet Indonesia 2017", 2017.

[2] Asosiasi Penyelenggara Jasa Internet Indonesia, "Penetrasi Dan Profil Perilaku Pengguna Internet Indonesia 2018", 2018.

[3] "IMPORTANCE OF BUSINESS WEBSITE," [Online]. Available: https://solutionsresource.com/importance-of-business-website/.

[4] M. Reily, "Nielsen: Pembaca Media Digital Sudah Lampaui Media Cetak," December 2017. [Online]. Available: https://katadata.co.id/berita/2017/12/07/nielsen-pembaca-media-digital-sudah-lampaui-media-cetak.

[5] A. Yusuf dkk, "HONEYNET PROJECT BSSN - IHP", 2018.

[6] Forcepoint, "What is SIEM," [Online]. Available: https://www.forcepoint.com/cyber-edu/siem.

[7] Pengelola Nama Domain Internet Indonesia (PANDI), "Jumlah Domain .id Tembus 318.000 di Pertengahan 2019," July 2019. [Online]. Available: https://pandi.id/jumlah-domain-id-tembus-318-000-di-pertengahan-2019/.

[8] J. Summerfield, "Mobile Website vs. Mobile App: Which is Best for Your Organization?," [Online]. Available: https://www.hswsolutions.com/services/mobile-web-development/mobile-website-vs-apps/.

[9] Goodwill Community Foundation, Internet 101 "What is the Internet?", 2013.

[10] B. Wellman and K. Hampton, "Living networked in a wired world," *Contemporary Sociology,* vol. 28, 1999.

[11] D. J. Schiano, "Lessons from 'LambdaMOO': A Social, Text-Based Virtual Environment", *Presence,* vol. 8, 1999.

[12] LUMINIS, "Application Platform Optimization," [Online]. Available: https://luminisindia.com/application-platform-optimization/124-application-platform-optimization.

[13] K. Y. A. McKenna, A. S. Green and M. E. J. Gleason, "Relationship Formation on the Internet: What's the Big Attraction?", *Journal of Social Issues,* vol. 58, pp. 9-31, 2002.

[14] BBC WEBWISE, “What is a web browser?”, 2013.

[15] A. N. Rachman, A. I. Gufroni, N. Hiron and G. Rahmayati , "Analisis Perbandingan Performansi dan Pemilihan Web Browser," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, Yogyakarta, 2013.

[16] M. Loganathan and K. E. Dharani, "ADVANCED WEB BROWSER WITH EFFECTIVE TOOLS", *International Journal of Computer Science and Mobile Computing ,* vol. 3, pp. 228-234, 2014.

[17] A. Zaki, “Kiat Jitu Membuat Website Tanpa Modal” dalam “ANALISIS LAYANAN WEBSITE SEBAGAI MEDIA PROMOSI, MEDIA TRANSAKSI DAN MEDIA INFORMASI DAN PENGARUHNYA TERHADAP BRAND IMAGE PERUSAHAAN PADA HOTEL CIPUTRA DI KOTA SEMARANG”, 2009.

[18] R. Harminingtyas, "ANALISIS LAYANAN WEBSITE SEBAGAI MEDIA PROMOSI, MEDIA", *JURNAL STIE SEMARANG,* vol. 6, 2014.

[19] United States Department of Justice, "Cyber Crimes", Department Of Justice.

[20] T. Finnie, T. Petee and J. Jarvis, "Future Challenges of Cybercrime", in *Proceedings of the Futures Working Group*, Virginia, 2010.

[21] S. Gordon and R. Ford, "On the definition and classification of cybercrime", *Journal of Computer Virol,* vol. 2, pp. 13-20, 2006.

[22] R. K. Goutam, "Importance of Cyber Security", *International Journal of Computer Applications ,* vol. 111, 2015.

[23] H. F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", 2002.

[24] A. S. Gumelar, M. C. Saputra and N. H. Wardani, "Analisa Kebutuhan dan Perancangan Sistem Informasi Produksi Dinas Peternakan dan Kesehatan Hewan Kabupaten Malang Berbasis Teknologi Service Oriented Architecture", *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* vol. 1, pp. 1215-1225, 2017.

[25] N. A. Wibisono and R. Y. Dewantara, "ANALISIS DAN PERANCANGAN SISTEM INFORMASI TOKO UNTUK MENCAPAI KEUNGULAN KOMPETITIF (Studi pada Toko Sakinah Motor Kabupaten Sukoharjo)", *Jurnal Administrasi Bisnis (JAB),* vol. 47, 2017.

[26] C. Kothari, “Research Methodology: Methods and Techniques”, New Dehli: New Age International, 2004.

[27] Direktorat Penanggulangan dan Pemulihan Pemerintah, "Panduan Pelaporan Insiden", Desember 2018. [Online]. Available: https://govcsirt.bssn.go.id/download/panduan pedoman_teknis/Panduan-Pelaporan-Insiden.pdf. [Accessed Maret 2020].

[28] C. Larman, "Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development Third Edition", Addison Wesley Professional, 2004.

[29] Satzinger, Jackson, Burd. 2010. "System Analysis and Design with the Unified Process. USA: Course Technology", Cengage Learning.

[30] Object Management Group, "OMG Unified Modeling Language (OMG UML) Version 2.5.1", 2017.

[31] V. Singh, "Database Design Using Entity Relationship Diagram".

[32] O. Nikiforova, J. Sejans and A. Cernickins, "Role of UML Class Diagram in Object-Oriented", *Scientific Journal of Riga Technical University,* vol. 44, p. 65, 2011.

[33] Y. Bassil, "A Simulation Model for the Waterfall Software Development Life Cycle", *International Journal of Engineering & Technology (iJET),* vol. 2, p. 2, 2012.

[34] M. Mizan, Narasumber, *Wawancara Terhadap Proses Pelaporan Insiden Siber Provinsi Jawa Tengah Hingga Insiden Siber Selesai Ditangani oleh Diskominfo Jateng.* [*Interview*]. 14 Oktober 2019.

[35] S. B. Utomo, Narasumber, *Wawancara Terhadap Proses Pelaporan Insiden Siber Provinsi Jawa Tengah Hingga Insiden Siber Selesai Ditangani oleh Diskominfo Jateng.* [*Interview*]. 14 Oktober 2019.

[36] Aminnudin, Narasumber, *Wawancara Terhadap Proses Pelaporan Insiden Siber Provinsi Jawa Tengah Hingga Insiden Siber Selesai Ditangani oleh Diskominfo Jateng.* [*Interview*]. 14 Oktober 2019.

[37] N. M. A. Munassar and A. Govardhan, "A Comparison Between Five Models Of Software Engineering," *IJCSI International Journal of Computer Science Issues,* vol. 7, 2019.

Lampiran

1. Lampiran Wawancara

Wawancara Terhadap Proses Pelaporan Insiden Siber Provinsi Jawa Tengah Hingga Insiden Siber Selesai Ditangani oleh Diskominfo Jateng

Pewawancara : Alwi Kesuma (AL)

Narasumber :

1. Subroto Budhi Utomo (SBU)= Kepala Sub Divisi (Kasi) Pengamanan Persandian dan Informasi serta sebagai Koordinator CSIRT,
2. Mualiful Mizan (MM) = PenTester,
3. Aminnudin (A) = PenTester.

Pada awal bulan September Kepala Sub Divisi (Kasi) Pengamanan Persandian dan Informasi memberikan sebuah tugas kepada salah satu mahasiswa Universitas Dian Nuswantoro (UDINUS) yang sedang melakukan Kuliah Praktek (KP) selama sebulan. Tugas yang dimaksud adalah membuat sebuah prototype website pelaporan insiden siber untuk memudahkan pelaporan insiden siber masyarakat Jawa Tengah. Selama satu bulan berlangsung ternyata, mahasiswa UDINUS tersebut tidak menyelesaikan website yang menjadi tugasnya. Penulis mencoba menawarkan diri untuk mengambil alih tugas pembuatan prototype website pelaporan insiden siber kepada Kasi Pengamanan Persandian dan Informasi. Pada tanggal 10-30 Oktober 2019, penulis mencoba mengamati bagaimana pelaporan insiden siber dan penanganan insiden siber berlangsung. Observasi dilakukan sembari melemparkan beberapa pertanyaan informasi kepada dua PenTester di Diskominfo Jateng terkait proses yang diterapkan pada saat itu. Wawancara secara informal tersebut dilakukan pada tanggal 14 Oktober 2019.

1 AL : Permisi Pak Subroto, sepertinya website yang menjadi tugas mahasiswa UDINUS tidak selesai. Apakah saya boleh mengambil alih tugasnya? Kebetulan saya cukup mampu sembari belajar untuk membuat website pelaporan insiden siber karena saya masih ada waktu hingga januari baru selesai magang. Jadi saya rasa waktunya cukup untuk membuat prototypenya.

2 SBU : Oh.. silahkan mas, soalnya itu lumayan perlu untuk assessment terkait pelayanan oleh BSSN kedepannya. Mas Alwi selesaikan jadi prototype saja, nanti diserahkan ke mas Aminnudin dan Mas Mizan.

3 AL : Baik pak. Saya sekalian observasi beberapa hari untuk cari tahu gimana nanti websiteny dibuat sekaligus tanya-tanya secara informal ke Pak Subroto, mas Amin, atau mas Mizan. Ini saya mau tanya kenapa butuh sistem berbasis website untuk pelaporan insiden siber? Apakah proses pelaporan insiden siber yang saat ini belum sesuai harapan pak?

4 SBU : Ok.. ok.. Nah kita sebagai dinas pemerintahan yang tugasnya memberikan pelayanan khususnya kepada warga provinsi Jawa Tengah butuh sistem yang tidak pilih-pilih device, jadinya kita sepakat pakai sistem berbasis website karena lebih responsif dalam arti tidak perlu download aplikasi dan semua *platform device* dapat menggunakannya. Kalau pakai basisnya website juga smartphone atau device komputer lain saat ini cenderung sudah bisa akses minimal google chrome ataupun browser bawaan dari sistem operasi device tersebut, jadinya siapapun bisa melaporkan insiden siber. Proses pelaporan selama ini kita hanya pakai email dan Whatsapp (WA) sebagai media untuk pelaporan insiden siber,

sampai follow up penanganannya. Email dipakai saat pelaporan insiden siber pertama kali dilakukan oleh pelapor, nantinya dari *Helpdesk* yang jadi admin email akan melakukan *open ticket* serta meneruskan pelaporannya ke saya selaku Koordinator CSIRT untuk follow up pakai WA. Sebenarnya kalau pakai WA bisa dilayani dengan cepat tapi prosedur tidak begitu jelas dan alurnya tidak berjalan sempurna. Kalau di pemerintahan kan kalau bisa melakukan kegiatan secara efisien, terstruktur, dan terdokumentasi. Pemakaian WA sebenarnya sudah mencapai salah satu *goal* nya yaitu efektif di segi kemudahan karena orang-orang cenderung sudah familiar menggunakan WA, tapi dokumentasinya tidak tertata dan tidak terstruktur pencatatannya untuk organisasi pemerintahan.

5 AL : Koordinasi pakai WA emang terlihat cukup mudah karena orang-orang juga sudah familiar sih pak, tapi tidak terdokumentasi dengan baik dan tidak terstruktur. Prosesnya bisa dijelasin dari pelaporan insiden siber hingga penangan selesai beserta dokumentasinya pak?

6 SBU : Pengguna yang melapor juga cenderung dari lingkungan pemerintahan Jawa Tengah. Mereka harus melapor ke email Diskominfo yang ada di Website dulu, nanti Helpdesk Diskominfo akan verifikasi dan minta Kontak WA milik pelapor. Nanti kontak WA dari pelapor akan diteruskan ke saya, dari informasi pelaporan tersebut saya koordinasikan dengan tim penanganan juga untuk penanganan lebih lanjutnya. Hasil koordinasi dengan tim penanganan itu adalah perlu atau tidak untuk mengeksalasikan insiden siber tersebut ke BSSN. Setelah itu sudah dikoordinasikan, kita langsung identifikasi insidennya dan solusi yang ingin

diimplementasikan oleh tim penanganan. Kalau sudah selesai ditanganai nantinya tim dokumentasi akan buat laporan dokumen penanganan insiden ke OPD terkait dan Helpdesk juga melakukan close ticket. Tim dokumentasi kemudian membuat dokumen hasil pelaksanaan kegiatan kepada Kepala Dinas, Gubernur/Sekda. Proses follow up penanganan insiden siber bakal ada 2 macam yaitu secara terpandu atau remote. Kalau sudah selesai ditangani, bakal dibuat laporan dokumen penanganan insiden siber untuk di ajukan ke kepala dinas supaya ditandatangani. Kalau sudah nanti salah satu laporan kita simpan dan satunya lagi di serahkan ke pelapor. Singkatnya begitu sih.

7 A : Kalau kita pakai WA sebenarnya untuk pribadi gk masalah, tapi engga cocok untuk organisasi pemerintahan krna pencatatan kegiatan pelaporan dan penanganan kan tidak terstruktur dan hanya tercatat di WA. Pelapor biasanya kan koordinasi sama Pak Subroto selaku Kasi. Alangkah baiknya kalau pelaporan kita buat satu platform yang datanya tersimpan di Diskominfo. Jadi data pelaporan hingga penanganan insiden siber semuanya tercatat di server Diskominfo gt. Semisal kita mau buka data penanganan insiden 6 bulan lalu juga bisa diakses. Kalau di WA saja kan bisa rentan terformat atau hal lainnya. Kalau terformat ya proses penangannya di WA hilang.

8 MM : Jadi kita pengennya semua masyarakat Jawa Tengah bisa lapor tanpa harus melalui proses email seperti itu. Kita pengennya mereka bisa lapor langsung ke sebuah platform, nanti bakal langsung diverifikasi dan ditangani sama kita. Semua kegiatan juga tercatat dengan terstruktur dan bisa diakses log pencatatannya di kemudian hari. Kalau pencatatan sudah disimpan di satu platform

dan terstruktur, kita juga lebih mudah buat laporan penanganan insiden siber karena informasinya kan sudah jelas di website tanpa harus kita cari2 di WA.

9 AL : Kalau untuk website seperti itu nanti saya buatkan open ticket gimana? Jadi ada pilihan “Pending”, “Ditolak”, “Diterima”, “Dieksekusi”, “Selesai”, dan “Ditutup”. “Pending” itu default kalau pelaporan baru dilakukan oleh pemilik aplikasi. Nah kalau tim CSIRT sudah verifikasi permasalahannya baru bisa open ticket ke “Eksekusi”, di sini fitur berbalas pesan pakai email. CSIRT pakai email resminya Diskominfo untuk meningkatkan kepercayaan masyarakat dalam berbalas pesan, mungkin nanti ada email tersendiri untuk respon insiden siber. Kalau penanganan insiden siber sudah selesai, ubah statusnya jadi “Selesai”. Maka fitur email akan menghilang lagi yang artinya kasus ditutup dan status menjadi close ticket.

10 A : Boleh kok, itu malah sesuai dengan peraturannya di BSSN kalau ada open ticket, penanganan jadi lebih terstruktur dengan pelapor. Oh ya ditambahin ada fungsi login ya. Jadi bisa login jadi 3 jenis Superadmin (CSIRT diskominfo), admin (Organisasi Pemerintahan Daerah Jateng), dan umum(untuk masyarakat umum). Nanti setiap login punya fungsi yang beda2. Super admin bisa nampilin data semuanya dan hanya superadmin yang bisa mengubah status open ticketnya. Admin hanya bisa menampilkan data milik organsasinya saja dan pengguna umum hanya bisa menampilkan data miliknya

saja. Tambahan lagi, CSIRT kan ada 4 bagian yaitu koodinator, helpdesk, tim penanganan, dan tim dokumentasi. Empat bagian CSIRT itu disatukan dalam akun Super Admin saja.

11 AL : Ok mas, Amin. Berarti ada rolenya ya. Untuk masalah registrasi nanti gimana enaknya, kan ada 3 jenis akun soalnya. Kalau menurut saya sih dibedakan jenis registrasinya.

12 MM : Kalau ada role yang berbeda ya di kasih login deh. Terkait registrasi akun nanti satu akun SuperAdmin langsung dibuatkan aj sm kamu, kita nanti yang edit datanya dan berikan fungsi tambah user Super Admin juga. Akun Admin nanti dibuatkan satu akun untuk satu OPD Jateng oleh Super Admin, nanti dari akun yang kita kasih melalui surat pemerintahan, mereka bisa menambahkan akun admin lainnya untuk organisasinya mereka sendiri. Pengguna umum nanti buatkan halaman registrasi saja di sekitaran halaman login. Oh ya jangan lupa untuk fungsi delete user di menu pengelolaan user pada Super Admin dan Admin itu tidak bisa delete akunnya sendiri ya. Hal ini untuk memastikan bahwa OPD Jawa Tengah tetap ada akun untuk melaporkan insiden siber.

13 AL : Kalau yang saya paham berarti nanti bakal ada data master Jenis insiden siber dan OPD. Kalau data relasional kayak user butuh data dari OPD untuk menunjukkan kalau dia kalau usernya jenis Admin, tapi kalau usernya jenis umum gk perlu data dari OPD. Untuk open ticket nanti bakal ditangani sama Super Admin dan jenis insiden untuk mengkategorikan insiden yang dilaporkan sih di atur sama super admin aja, seperti insiden A ternyata waktu di analisis tuh jenisnya “Phishing attack”. Respon untuk komunikasi dengan pelapor insiden pake email yang di embed ke website. Data-data juga hanya Super Admin yang bisa lihat semuanya, gitu kan?

14 A : Iya, sementara gitu aja untuk menu-menunya, diberi halaman dashboard yang bisa menampilkan jumlah dan menampilkan data insiden berdasarkan statusnya, aplikasi, dan pengguna juga. Nanti kalau sudah jadi prototypenya, kita mau modifikasi sedikit sesuai kebutuhan terupdate nantinya.

15 SBU : Halaman pengelolaan laporan insiden siber untuk yang Super Admin nanti dibagi2 saja untuk Helpdesk, Koordinator, dan Tim Penanganan tapi tidak perlu dibedakan, levelnya tetap sebagai Super Admin. Hanya saja untuk mengkategorikan halaman, CSIRT juga bisa lebih fleksibel jika salah satu bagian seperti Helpdesk lagi tidak di tempat, tapi Koordinator dapat menerima pelaporan insidennya dari si pelapor.

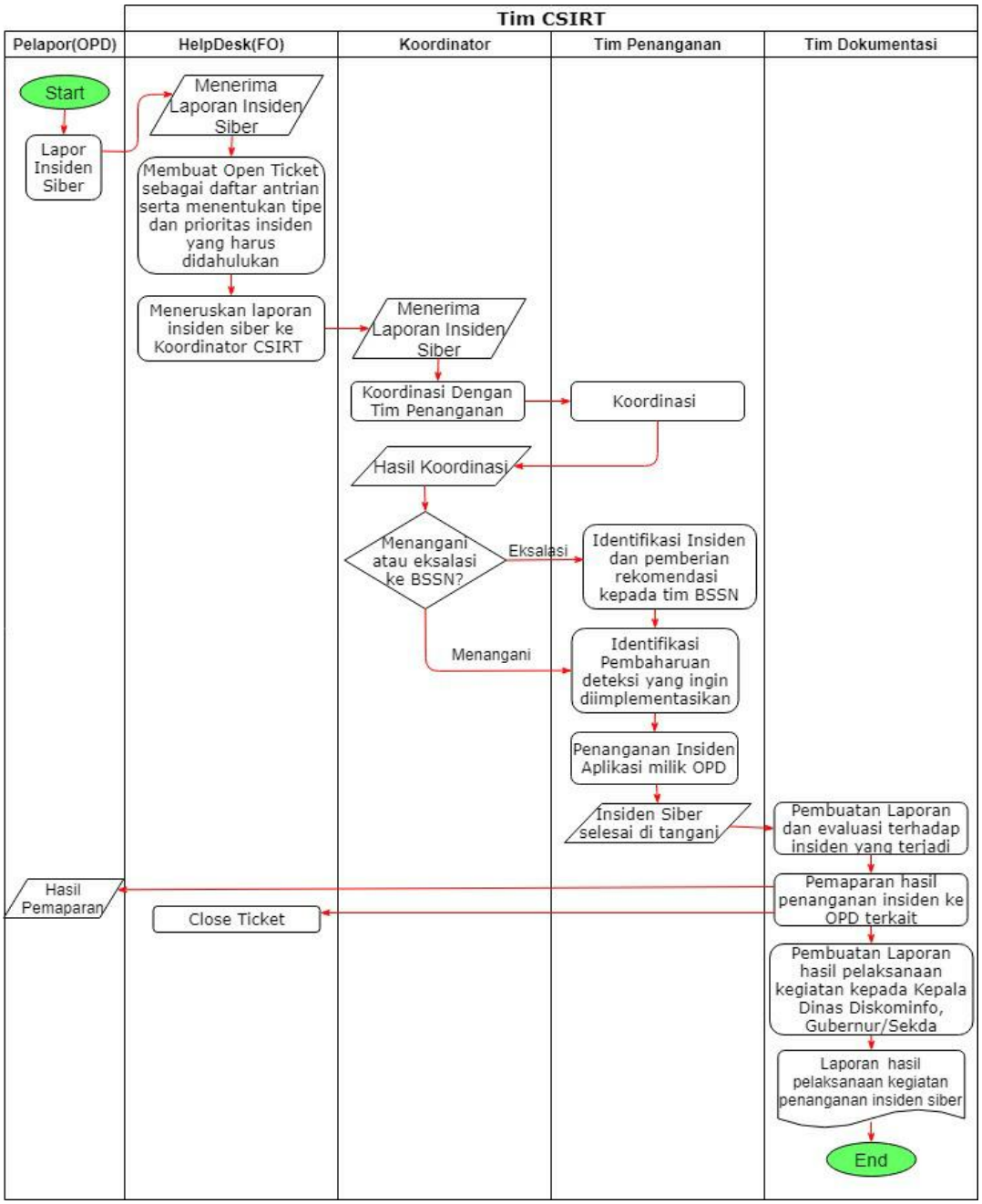
16 AL : Saya mau tanya terkait pengiriman pesan kan pakai email yang *embedded* di sistem, nah untuk inbox emailnya itu butuh integrasikan dengan sistemnya pak? Mungkin bisa di jelaskan teknisnya sedikit.

17 SBU : Saat ini tidak perlu dulu di *embedded* inboxnya email ke sistem, nanti dari kami yang akan kembangkan lagi. Telegram mungkin menjadi salah satu pilihan nanti kita *embedded*. Sementara mas Alwi buat sampai pengiriman pesan dari sistem ke email si pelapor saja, untuk inboxnya nanti kita pakai inbox yg di email saja dulu.

16 AL : Ok pak, saya coba buatin dl *website* nya, semoga bisa selesai tepat waktu. Ini saya sambil amatin alurnya kalau ada pelaporan insiden siber.

2. Hasil Observasi

Observasi dilakukan dari tanggal 10-30 Oktober 2019 untuk mengetahui proses nyata yang terjadi di lapangan. Kegiatan observasi memberikan hasil yang dideskripsikan menggunakan *FlowChart* dan didukung juga dari hasil wawancara.



Gambar 6.1 Proses Bisnis Penanganan Pelaporan Insiden Siber Yang Sedang Diterapkan

FlowChart di atas juga telah disesuaikan dengan hasil wawancara dan SOP CSIRT Diskominfo Jateng yang baru saja diresmikan untuk persiapan ISO 27001 di tahun 2020. Saat ini pelayanan pelaporan insiden siber hanya berlaku untuk OPD provinsi Jawa Tengah saja. OPD yang mengalami insiden siber pada website milik organisasinya dapat melaporkannya ke Tim CSIRT Diskominfo Jateng untuk mendapatkan penanganan serta optimasi keamanan. Tim CSIRT dibagi menjadi Helpdesk, Koordinator, Tim Penanganan, dan Tim Dokumentasi yang memiliki tugas masing-masing dalam menangani pelaporan insiden siber.

Menurut Pak Subroto pada skrip wawancara nomor 6, saat OPD mengalami insiden siber pada websitenya, mereka dapat melakukan pelaporan ke Diskominfo Jateng melalui email yang akan diterima oleh bagian Helpdesk serta melakukan open ticket untuk diteruskannya pelaporan kepada koordinator CSIRT untuk proses follow up dan penanganan. Sebelum penanganan dan follow up dilakukan, koordinator koordinasi dengan tim penanganan terlebih dahulu untuk memutuskan apakah insiden ini hanya sekedar ditangani atau perlu dieksalasikan juga ke BSSN. Jika insiden dieksalasikan ke BSSN, maka Diskominfo Jateng sebagai pihak pertama yang mendapatkan laporan dapat melakukan identifikasi dan memberikan informasi terkait insiden kepada BSSN dan kemudian menentukan solusi yang ingin di implementasikan. Sebaliknya jika tidak perlu mengeksalasikan ke BSSN, maka Diskominfo Jateng langsung melakukan identifikasi dan menentukan solusi yang ingin diimplementasikan [35].

Setelah insiden siber selesai ditangani secara teknis, maka tim dokumentasi akan membuat laporan berupa dokumen yang kemudian akan diberikan hasil paparannya dalam bentuk dokumen kepada pelapor. Helpdesk melakukan close tiket kepada pelapor tersebut setelah hasil paparan telah disampaikan kepada pelapor. Tim dokumentasi melanjutkan membuat laporan hasil pelaksanaan kegiatan kepada internal Diskominfo Jateng dan Gubernur/Sekda sebagai akhir tahap dari penanganan pelaporan insiden siber [35].

Penulis saat melakukan observasi juga mendapatkan informasi di luar dari proses pelaporan insiden siber yaitu terkait model perancangan yang sering

digunakan oleh Diskominfo Jateng. Peneliti saat magang melakukan observasi pelaporan insiden siber sembari menjadi asisten auditor Indeks KAMI yang salah satu tugasnya adalah mengumpulkan dokumen-dokumen yang dibutuhkan untuk peniliaian Indeks KAMI yang salah satu dokumennya adalah dokumen perancangan sistem informasi. Diketahui bahwa dokumen perancangan sistem informasi milik Diskominfo Jateng cenderung sistem-sistemnya menggunakan SDLC model waterfall serta merupakan dokumen yang sangat rahasia dan diawasi saat mengaksesnya. Berdasarkan informasi tersebut, diketahui bahwa model perancangan yang sering digunakan oleh Diskominfo Jateng adalah SDLC model Waterfall.

Tabel Revisi

No	Tugas Revisi	Halaman revisi
1.	Alasan penggunaan SDLC di Diskominfo Provinsi Jawa Tengah	- Halaman 16 paragraf 1 dan 2
2.	Kesesuaian judul dengan rumusan masalah dan pembahasan (perlu lebih ditegaskan bagaimana analisis dilakukan, atau judul dan permasalahanya yang disesuaikan dengan isi)	- Halaman 7 paragraf 1 - Halaman 14 paragraf 2,3,4, dan 5 - Halaman 18 paragraf 4
3.	Dalam skripsi diklaim bahwa sistem yang diusulkan lebih aman daripada yang lama, perlu ditegaskan/diperjelas maksudnya	- Halaman 7 paragraf 3 - Halaman 139 paragraf 4