PERANCANGAN SISTEM MANAJAMEN INSIDEN KEAMANAN INFORMASI BERDASARKAN SNI ISO/IEC 27035 DI INSTANSI PEMERINTAH

Wikankara[1], Rudy Hartanto[2], Lukito Edi Nugroho[3]
[1,2,3] Magister Teknologi Informasi, Universitas Gadjah mada Yogyakarta
Email: [1]wikankara@mail.ugm.ac.id, [2]rudy@ugm.ac.id, [3]lukito@ugm.ac.id

Masuk: 16 Juli 2020, Revisi masuk: 25 Juli 2020, Diterima: 28 Juli 2020

ABSTRACT

The government services of information technology are required to always run optimally. On the other hand, many information services are still faced with security incidents. In terms of human resources, technology, policy, and procedural aspects, the focus problem has not been on security incidents of information. Therefore, we need information security incident management system as one of the system solutions that must be provided to ensure the sustainability of information services and IT systems. The purpose of this research is able to provide security information of incidents having a management system that was adopted and developed based on ISO/IEC 27035 standardization. The research methodology was carried out by using qualitative methods with case studies. The preparation of the document refers to the results of the assessment approach between the current conditions of business processes and the incident management of information security. It has been carried out with the clauses required by ISO/ IEC 27035. The results of this study are policy documents and procedures for the incident management systems of information security specifically designed as a reference standard in government. Finally, the use of structured policies and procedures can improve performance in handling incidents faced by the government.

Keywords: *Incident, Information security, ISO/IEC 27035, Management.*

INTISARI

Layanan teknologi informasi pemerintah dituntut untuk selalu berjalan optimal tanda kendala. Namun masih banyak ditemukan permasalahan insiden keamanan informasi yang dihadapi. Dari sisi sumber daya manusia, teknologi, maupun dari sisi kebijakan dan prosedural belum fokus pada aspek insiden keamanan informasi. Oleh karena itu diperlukan suatu sistem manajemen insiden keamanan informasi sebagai salah satu solusi sistematis yang harus disediakan untuk menjamin keberlangsungan layanan informasi dan sistem TI. Tujuan dari penelitian ini untuk menyediakan suatu sistem manajemen insiden keamanan informasi yang diadopsi dan dikembangkan berdasarkan standardisasi ISO/IEC 27035. Metode penelitian yang dilakukan menggunakan metode kualitatif dengan studi kasus. Penyusunan dokumen dilakukan mengacu pada pendekatan hasil assesmen antara kondisi saat ini (eksisting) dari proses bisnis dan manajemen insiden keamanan informasi yang telah dilakukan dengan klausul yang dipersyaratkan oleh ISO/IEC 27035. Hasil dari penelitian ini adalah dokumen kebijakan dan prosedur sistem manajemen insiden keamanan informasi yang didesain secara khusus sebagai standar acuan di pemerintahan. Melalui penggunaan kebijakan dan prosedur yang terstruktur akan dapat meningkatkan kinerja dalam penanganan insiden yang dihadapi pemerintah.

Kata-kata kunci: Insiden, ISO/IEC 27035, Keamanan informasi, Manajemen.

PENDAHULUAN

Di masa kini, proses bisnis pemerintahan tidak terlepas dari proses manajemen data seperti mengirim, mengumpulkan, membuat maupun menggunakan data untuk menjalankan berbagai kegiatan atau aktivitas yang terkait dengan bisnisnya. Proses pengelolaan data tersebut menjadikan pemerintah memiliki risiko besar terkait ancaman terjadinya suatu insiden keamanan informasi dari layanan elektronik yang dimilikinya. Adanya ancaman tersebut menyebabkan setiap organisasi melakukan investasi besar untuk mengamankan teknologinya dengan kencenderungan yang semakin meningkat nilainya setiap tahun.

Beragamnya jenis layanan yang dimiliki oleh pemerintah tentunya memiliki tingkat keamanan dan potensi gangguan insiden yang berbeda beda. Gangguan insiden

tersebut disebabkan oleh manusia ataupun akibat kerusakan aplikasi dan perangkat jaringan. Insiden *deface* website milik pemerintah sering terjadi dan menyebabkan layanan tidak bisa diakses. Beragam jenis insiden lainnya seperti serangan DDoS, *malware, spamming*, *phising* maupun serangan *Advanced Persisten Threat* (APT) juga semakin marak terjadi.

Mesipun kejadian insiden semakin marak terjadi, namun pemerintah sampai dengan saat ini belum memberikan perhatian khusus pada penanganan insiden. Investasi yang dilakukan kecenderungannya hanya pada penyediaan infrastruktur teknologi saja. Sedangkan pada penyiapan sumber daya manusia (SDM) yang berkompeten masih belum optimal. Pegawai di lingkungan pemerintah banyak yang belum memiliki kesadaran (*awareness*) keamanan informasi sehingga sangat rentan terkena insiden keamanan informasi. Penyediaan pedoman kebijakan dan prosedur yang sistematis juga masih belum ada menjadikan penanganan dilakukan secara individual dan tidak terkelola dengan baik.

Penanganan insiden secara sistematis penting dilakukan karena insiden dapat memberikan dampak buruk bagi pemerintah. Insiden menyebabkan terjadinya kegagalan teknis dan dapat menimbulkan kerusakan data permanen. Kegagalan teknis akan mengakibatkan terganggu atau terhentinya proses bisnis pemerintahan dalam melaksanakan tugas fungsinya untuk memberikan pelayanan publik. Apabila tidak ditangani secara benar dampak yang diterima akibat insiden dapat menyebabkan reputasi pemerintahan menjadi buruk dan menurukan tingkat kepercayaan publik terhadap pemerintah.

Penelitian mengenai manajemen insiden secara umum sangat berkembang saat ini. Pada perusahaan pernah dilakukan penelitian mengenai manajemen insiden menggunakan *framework* ITIL (Ilvarianto dan Legowo, 2017; Nugraha dan Legowo, 2017; Azizah dkk, 2020). Hasil dari beberapa penelitian tersebut adalah sebuah standar prosedur dalam penanganan insiden. Melalui penggunaan prosedur yang baik akan mempermudah dalam penanganan insiden.

Selanjutnya penelitian mengenai manajemen insiden di perguruan tinggi juga pernah dilakukan menggunakan *framework* ITIL (Palilingan dan Batmetan, 2018). Fokus penelitian ini adalah pada sistem layanan akademik perguruan tinggi. Hasil penelitian ini menjelaskan bahwa menggunakan tata kelola manajemen insiden akan mempercepat proses penanganan insiden, sehingga layanan di sistem layanan akademik akan berjalan dengan baik dan efisien. Penelitian ini hanya membahas mengenai mekanisme layanan penanganan insiden yang baik tanpa mempertimbangkan aspek keamanan informasi.

Penelitian lainnya membahas tentang pembuatan arsitektur penanganan keamanan siber dan implementasinnya (Tsakalidis dkk, 2019). Dari hasil penelitian ini disimpulkan bahwa otomatisasi pada manajemen insiden akan berguna bagi lembaga terkait untuk mendapatkan wawasan dan mengkoordinasikan tindakan masing-masing. Namun penelitian ini tidak membahas mengenai potensi insiden keamanan informasi yang lain, seperti kegagalan sistem, kelistrikan, maupun gangguan lainnya.

Penelitian manajemen insiden di bidang pemerintahan sendiri masih jarang dilakukan. Salah satu penelitian yang pernah dilakukan adalah mengenai rekomendasi pembentukan tim penanganan insiden di pemerintah daerah (Setiawan, 2014). Penelitian ini menyarankan setiap pemerintah daerah untuk membentuk GovCSIRT sebagai tim pengelola insiden di daerah dan dapat selalu berkoordinasi dengan CSIRT Pusat. Penelitian implementasi manajemen insiden juga pernah dilakukan di Pemerintah Kota Surabaya (Rizky dkk, 2017). Penelitian ini menggunakan *framework* ITIL V3 dan menghasilkan sebuah dokumen SOP manajemen insiden.

Sebagian besar penelitian yang telah dilakukan sebelumnya lebih banyak membahas pada sisi teknis penanganan insiden (deteksi, respon, dan pembelajaran insiden). Aktivitas pra insiden, seperti pembuatan kebijakan dan prosedur yang sistematis, pembuatan program pelatihan dan peningkatan *awareness* pegawai, maupun pembentukan tim respon insiden belum dibahas dalam penelitian sebelumnya. Padahal dalam sebuah proses manajemen insiden yang baik haruslah terdiri dari suatu kesatuan yang lengkap, mulai dari fase persiapan dan perencanaan, pelatihan dan peningkatan *awareness* hingga pendeteksian, respons, dan

pembelajaran dari insiden (Tello-Oquendo dkk, 2019).

Berdasarkan kesenjangan di atas, maka perancangan sistem manajemen insiden keamanan informasi yang sistematis dan menyeluruh perlu dilakukan penelitian lebih lanjut. Hal ini penting, karena dengan adanya sistem manajemen insiden keamanan informasi yang lengkap akan menjadikan pengelolaan insiden menjadi lebih tertib dan teratur. Selain itu juga dapat mengurangi potensi terjadinya insiden secara berulang di kemudian hari.

Penelitian ini bertujuan untuk mengusulkan sebuah dokumen panduan *best practice* dalam sistem manajemen insiden keamanan informasi di bidang pemerintahan, dengan batasan ruang lingkup pada instansi pemerintahan tingkat provinsi. Peneliti ini menggunakan SNI ISO/IEC 27035 sebagai acuan dalam perancangan tata kelola manajemen insiden keamanan informasi, dikarenakan SNI ISO/IEC 27035 dirancang secara khusus untuk dapat sesuai pada semua jenis organisasi. SNI ISO/IEC 27035 memiliki model penanganan proaktif dan mempunyai fase manajemen insiden yang detail, mulai dari perencanaan, deteksi, respon hingga pembelajaran pasca insiden. Model penanganan proaktif tersebut memberikan keunggulan tindakan gabungan dari layanan reaktif dan preventif.

SNI ISO/IEC 27035 merupakan standar yang dikembangkan oleh *International Organisation for Standardisation* (ISO) dan telah diadopsi secara resmi di Indonesia oleh Badan Standardisasi Nasional (BSN) menjadi SNI ISO/IEC 27035. Seperti ISO yang lainnya, ISO 27035 juga didesain secara generik untuk beragam organisasi maupun institusi. ISO/IEC 27035 merupakan standar turunan dari ISO/IEC 27001 Sistem Manajemen Keamanan Informasi khususnya pada domain A.16 Manajemen Insiden Keamanan Informasi. SNI ISO/IEC 27035 versi terakhir dirilis resmi pada tahun 2016. Dalam rilis tersebut terdapat 2 bagian, yaitu:

1. SNI ISO/IEC 27035-1:2016-Teknologi Informasi-Teknik Keamanan-Manajemen Insiden Keamanan Informasi-Bagian 1: Prinsip manajemen insiden.
2. SNI ISO/IEC 27035-2:2016-Teknologi Informasi-Teknik Keamanan-Manajemen Insiden Keamanan Informasi-Bagian 2: pedoman perencanaan dan persiapan respon insiden.

Dengan menggunakan *framework* ISO/IEC 27035 akan menjadikan layanan yang dilakukan dalam manajemen insiden keamanan informasi tidak hanya responsif terhadap insiden, namun juga memberikan layanan preventif untuk meminimalisir kejadian insiden akan terulang kembali. Selain itu, dengan mengadopsi ISO/IEC 27035 membuat dokumen yang dihasilkan tetap selaras dengan standar manajemen keamanan informasi yang telah digunakan saat ini.

Insiden Keamanan Informasi

Istilah insiden keamanan informasi memiliki beragam definisi. Menurut definisi dari ISO 27035, insiden adalah serangkaian peristiwa atau kejadian keamanan informasi yang tidak diinginkan atau tidak terduga yang memiliki probabilitas signifikan untuk mempengaruhi operasional bisnis dan mengancam keamanan informasi(ISO , 2019). Kejadian insiden keamanan informasi dapat beragam, diantaranya adalah pencurian data, bencana alam, bahaya dari lingkungan sekitar seperti kebakaran, kegagalan saluran data, *system crash, packet flooding*, penggunaan akses atau penggunaan sumber daya sistem yang tidak sah, penggunaan akun pengguna lain secara tidak sah, penggunaan hak sistem tanpa izin, perusakan *web*, penetrasi/intrusi sistem, maupun serangan virus yang masif.

Manajemen Insiden Keamanan Informasi

Manajemen insiden keamanan informasi merupakan satu atau serangkaian proses mendeteksi dan merespon insiden keamanan informasi, termasuk didalamnya adalah proses pembelajaran insiden dan menggunakan hasil pembelajaran yang didapat sebagai bagian dari input dalam keseluruhan proses manajemen selanjutnya.

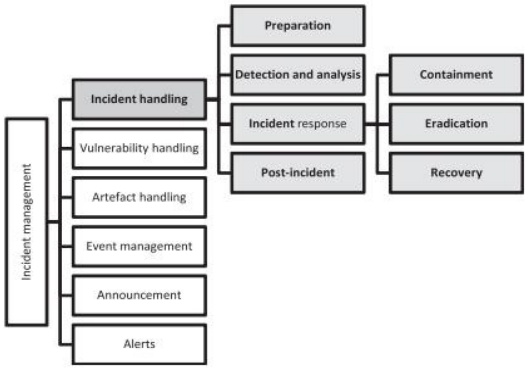
Manajemen insiden keamanan informasi dapat diadopsi dari berbagai macam *framework* atau standar yang ada di dunia. Sebagai contoh, standar ITIL 2011, ISO/IEC 27035, NIST SP 800-61, ENISA, dan SANS secara umum memiliki pedoman yang hampir sama (Line dkk, 2014).

Seluruh standar insiden manajemen keamanan informasi mempunyai kesamaan, yaitu terdiri dari beberapa fase/tahapan dalam proses manajemennya (Hove dkk, 2014). Beberapa standar memiliki fase persiapan (*preparation*) yang digunakan untuk mempersiapkan kapasitas dalam

penanganan insiden. Di fase berikutnya, hampir seluruh standar mempunyai fase deteksi, analisis dan respon atas insiden. Sedangkan fase pembelajaran (*lesson learned*) terdapat di semua standar.

Perbedaan di antara beberapa standar terletak pada model penanganannya. ISO 27035, NIST SP 800-61, dan SANS merupakan standar yang mengedepankan model penanganan secara proaktif, artinya lebih mengedepankan inisiatif yang didalamnya juga ada tindakan preventif dalam menghadapi insiden. Sedangkan ITIL, CERT, dan ENISA merupakan model penanganan dengan sifat reaktif yang hanya akan bereaksi ketika terjadi insiden (Tondel dkk, 2014). Strategi proaktif yang berarti seimbang antara preventif dan reaktif sangat penting, karena insiden yang terjadi sangat dinamis (Baskerville dkk, 2014).

Manajemen insiden lebih dari sekedar penanganan insiden. Di dalam manajemen insiden juga terdapat proses proaktif seperti pemberian *warning/alert* maupun *awareness* kepada pengguna layanan, peningkatan kapasitas melalui pelatihan dan *training*. Selain itu juga terdapat proses penanganan dan pembelajaran pasca insiden (Ab Rahman dan Choo, 2015), seperti ditampilkan pada Gambar 1.



Gambar 1. Cakupan manajemen insiden (Ab Rahman dan Choo, 2015)

Respon insiden (*incident response*) merupakan salah satu bagian dari proses penanganan insiden (*incident handling*), dan penanganan insiden merupakan bagian dari keseluruhan manajemen insiden *(incident management*). Penanganan insiden dilakukan oleh suatu tim respon insiden yang dapat dinamakan IRT (*Incident Response Team*), CSIRT (*Computer Security Incident Response Team*), atau CERT (*Computer Emergency response Team*).

Beberapa tujuan utama manajemen insiden keamanan informasi menurut ISO 27035 adalah:

1. Menghindari terjadinya insiden kemanan informasi.
2. Meminimalkan dampak insiden keamanan informasi terhadap kerahasiaan, ketersediaan, atau integritas layanan, aset informasi, dan operasi organisasi.
3. Mengurangi ancaman dan kerentanan saat terjadi insiden.
4. Meningkatkan koordinasi dan manajemen insiden keamanan informasi dalam industri investasi.
5. Mengurangi dampak biaya yang disebabkan oleh insiden keamanan informasi.
6. Melaporkan temuan kepada manajemen eksekutif.

ISO/IEC 27035 membagi fase proses manajemen insiden menjadi lima tahap aktivitas (ISO, 2019), yaitu *plan and prepare*, *detection and reporting*, *assessment and decision*, *responses*, dan *lessons learn*. Kelima fase tersebut merupakan siklus yang berksinambungan dan terus menerus.

METODOLOGI PENELITIAN

Fokus dalam penelitian ini adalah merancang sistem manajemen insiden keamanan informasi untuk lembaga pemerintah berdasarkan SNI ISO/IEC 27035. Penelitian ini dilaksanakan secara kualitatif menggunakan metode studi kasus. Dinas Komunikasi dan Informatika Pemda DIY dipilih sebagai objek studi dengan pertimbangan sudah memiliki tata kelola teknologi informasi namun tingkat kerentanan maupun kejadian insiden yang terjadi masih cukup besar. Hasil penelitian ini diharapkan dapat dipergunakan oleh instansi lainnya yang sejenis.

Tahapan penelitian ini adalah sebagai berikut:

1. Pengumpulan dan analisis data
2. Identifikasi ruang lingkup dan proses bisnis organisasi
3. Identifikasi aset
4. Identifikasi insiden
5. Menentukan bentuk tim respon insiden
6. Merancang dokumen manajemen insiden
7. Verifikasi dan validasi

PEMBAHASAN

Pengumpulan dan Analisis Data

Penelitian ini diawali dengan melakukan studi literatur mengenai manajemen insiden keamanan informasi serta standar SNI ISO/IEC 27035. Berikutnya adalah pengumpulan data tentang dokumen tata kelola maupun aturan yang dimiliki oleh Pemda DIY. Observasi dilakukan terhadap proses bisnis yang sedang berjalan untuk mengetahui kondisi riil yang dihadapi, terutama dalam menghadapi insiden. Wawancara dengan pihak-pihak terkait di Pemda DIY dilakukan untuk memperoleh informasi tambahan yang diperlukan untuk penyusunan kerangka kerja.

Setelah data terkumpul, dilanjutkan proses analisis data. Analisis data dilakukan melalui assesmen data eksisting dengan kontrol yang ada pada SNI ISO/IEC 27035. ISO/IEC 27035 memiliki 198 kontrol dengan rincian terdapat 56 kontrol pada bagian 1 dan 142 kontrol pada bagian 2, seperti ditampilkan pada Tabel 1. Berdasarkan hasil assesmen pada data eksisting, dihasilkan temuan bahwa dari 198 kontrol pada SNI ISO/IEC 27035, terdapat 24 kontrol yang sudah diterapkan dan dijalankan secara menyeluruh oleh Dinas Komunikasi dan Informatika DIY. Sisanya sebanyak 106 kontrol baru dijalankan sebagian, dan 68 kontrol lainnya tidak dijalankan sama sekali. Atas dasar hasil assesmen tersebut kemudian dilakukan penggalian data lebih lanjut melalui wawancara.

Tabel 1. Hasil asesmen pemenuhan klausul SNI ISO/IEC 27035:2016

Klausul	Judul Klausul	Implementasi			Jumlah Kontrol
		Semua	Sebagian	Tidak	
SNI ISO/IEC 27035:2016-Bagian 1					
4,2	*Objectives of Incident Management*	0	5	1	6
4,4	*Adaptability*	1	3	0	4
5,2	*Plan & Prepare*	0	2	6	8
5,3	*Detect & Report*	2	6	0	8
5,4	*Assessment & Decision*	1	4	2	7
5,5	*Responses*	2	11	3	16
5,6	*Lessons Learnt*	0	3	4	7
		6	**34**	**16**	**56**
SNI ISO/IEC 27035:2016-Bagian 2					
4,1	*Information security incident management policy*	1	2	2	5
4,2	*Involved Parties*	1	4	0	5
4,3	*Information Security Management Content*	5	10	12	27
5,1	*Updating Information Security Polices*	2	2	0	4
5,2	*Linking of Policy Documents*	0	2	0	2
6,1	*Creating Incident Management Plan*	3	6	0	9
6,2	*Plan is built on consensus*	0	0	3	3
6,3	*Involved Parties*	1	2	2	5
6,4	*Incident Response Plan Content*	4	39	11	54
6,5	*Incident Classification Scale*	0	0	2	2
6,6	*Incident Forms*	1	4	2	7
6,7	*Process & Procedures*	0	0	12	12
6,8	*Trust & Confidence*	0	0	6	6
6,9	*Handling Confidential or Sensitive Information*	0	1	0	1
		18	**72**	**52**	**142**

Atas dasar hasil assesmen tersebut kemudian dilakukan penggalian data lebih lanjut melalui wawancara. Dari hasil observasi lebih lanjut dapat disimpulkan beberapa permasalahan utama dari manajemen insiden keamanan informasi yang dijalankan oleh Dinas adalah sebagai berikut:

1. Dinas Komunikasi dan Informatika DIY sering mengalami kejadian keamanan informasi (*event*) yang kemudian berujung pada terjadinya insiden, seperti *web defacement*, serangan DDoS, *phising email*, dan lainnya.
2. Dinas sudah memiliki dokumen kebijakan dan prosedur manajemen insiden

keamanan informasi, namun dokumen tersebut belum memenuhi sebagian besar klausul dalam SNI ISO/IEC 27035.
3. Implementasi dari dokumen kebijakan dan prosedur manajemen insiden keamanan informasi tidak dilakukan dengan baik, disebabkan oleh:
   a. Keterbatasan infrastruktur pendukung fungsi layanan teknologi informasi yang dimiliki,
   b. Keterbatasan SDM yang menguasai keahlian penanganan insiden keamanan informasi.
4. Rendahnya kesadaran pegawai terkait pentingnya manajemen insiden keamanan informasi.
5. Dokumentasi laporan dan kegiatan penanganan insiden tidak dilakukan dengan baik.

Identifikasi Ruang Lingkup dan Proses Bisnis Organisasi

Dalam mengembangkan dokumen kebijakan dan prosedur manajemen insiden keamanan informasi yang efektif, diperlukan sebuah proses awal untuk mengidentifikasi seluruh proses bisnis layanan teknologi informasi pada Dinas Komunikasi dan Informatika DIY. Aktifitas memahami proses bisnis yang dijalankan sangatlah penting agar ruang lingkup dan konteks yang ditentukan dapat tepat sasaran dan tidak menjadikan masalah baru. Pada aktifitas ini, berhasil diidentifikasi proses bisnis yang dilakukan oleh Dinas Komunikasi dan Informatika DIY, seperti pada Tabel 2.

Tabel 2. identifikasi proses bisnis

Proses Bisnis	Fungsi Bisnis
Pelayanan *data center*	Penyediaan layanan *hosting*
	Penyediaan layanan *subdomain*
	Penyediaan layanan *mail server*
	Penyediaan layanan *colocation server*
	Pemeliharaan infrastruktur data center
Pelayanan jaringan	Penyediaan akses internet
	Penyediaan fasilitas *video conference*
	Pemeliharaan infrastruktur jaringan

Identifikasi Aset

Dalam tahap ini dilakukan proses identifikasi aset yang dikelola oleh Dinas Komunikasi dan Informatika DIY. Identifikasi aset akan digunakan untuk menentukan bagian area mana saja yang terdampak ketika sebuah insiden terjadi. Hasil identifikasi aset kemudian dituangkan dalam bentuk tabel *aset register* dengan rincian terdapat 165 buah aset fisik, 161 buah aset aplikasi, dan 8 buah sarana pendukung yang harus dilindungi dari ancaman terjadinya insiden.

Identifikasi Insiden

Proses identifikasi insiden dilakukan dengan mengambil klasifikasi jenis insiden dengan mengacu pada SNI ISO/IEC 27035 dan disesuaikan dengan kondisi maupun potensi yang dihadapi. Hasil klasifikasi insiden yang ditetapkan ada 8 jenis,yaitu:
1. Akses tidak sah
2. *Denial of Service (DoS)*
3. *Malware*
4. Kebocoran Informasi
5. Penggunaan yang tidak benar
6. Kegagalan sistem
7. *Web defacement*
8. Gangguan jaringan

Hasil dari proses identifikasi insiden akan dituangkan dalam dokumen kebijakan dan prosedur yang akan dibuat pada tahap berikutnya. Setelah selesai melakukan klasifikasi jenis insiden, dilakukan tahapan penentuan kriteria dampak yang diakibatkan oleh suatu insiden. Kriteria dampak yang ditetapkan untuk manajemen insiden keamanan informasi yang ditetapkan ditampilkan pada Tabel 3.

Hasil dari penentuan kriteria dampak digunakan untuk menentukan seberapa besar akibat yang dihasilkan oleh insiden yang terjadi. Setelah kriteria dampak ditetapkan dilanjutkan dengan penentuan standar tingkat layanan insiden. Hal ini diperlukan untuk memastikan bahwa insiden dikelola dan ditanggapi sesuai dengan tingkat layanan yang telah ditetapkan. Tingkat layanan ini berlaku sebagai komitmen respon untuk semua jenis insiden keamanan informasi. Waktu respons insiden bervariasi sesuai dengan tingkat prioritas yang ditetapkan untuk insiden tersebut. Standar tingkat layanan dituangkan dalam bentuk tabel yang disesuaikan dengan dampak insiden yang telah ditetapkan sebelumnya.

Tabel 3. Dampak insiden

Dampak	keterangan	Contoh
Kritis	Jika tidak segera diselesaikan, insiden akan mengakibatkan gangguan pada layanan dari sistem informasi yang berkategori kritis, atau terjadinya pelanggaran keamanan yang mengakibatkan terjadinya kerugian finansial atau kerusakan reputasi	- Kerusakan substansial, dengan cakupan luas, aktual atau potensial terhadap kerahasiaan, integritas, atau ketersediaan aset informasi dan sumber daya TIK - Sebuah insiden yang berdampak pada ketersediaan infrastruktur keamanan TI - Eksposur besar-besaran dari informasi berklasifikasi rahasia ke dalam domain publik, di mana paparan tersebut menghasilkan atau menimbukan konsekuensi kerusakan reputasi
Signifikan	Jika tidak diselesaikan tepat waktu, insiden dapat memengaruhi operasional layanan IT utama dan menyebabkan terjadinya pelanggaran keamanan. Kerugian finansial atau kerusakan reputasi juga mungkin terjadi	- Kerusakan aset informasi dan sumber daya TIK. (10% pengguna tidak dapat menggunakan sumber daya TIK) - Paparan sejumlah kecil informasi yang berklasifikasi rahasia atau sensitif ke dalam domain publik atau kepada individu yang tidak berwenang
Penting	Jika tidak diselesaikan dalam jangka waktu yang wajar, dapat menimbulkan kerentanan dan memungkinkan terjadinya risiko gangguan layanan yang lebih tinggi terhadap sistem informasi yang dimiliki. Kerugian finansial atau kerusakan reputasi mungkin terjadi jika kerentanan tersebut dieksploitasi lebih lanjut secara sengaja atau oleh pihak yang tidak berwenang	- Insiden *malware* yang tidak sampai pada level keparahan lebih tinggi - Insiden kehilangan data yang tidak berklasifiikasi rahasia - Serangan *phishing* terkon informasi yang berdampak pada lebih dari 100 pengguna
Rendah	Insiden ini terkait dengan sistem informasi yang dikategorikan tidak kritis atau data yang tidak sensitif, dan kemungkinan menyebabkan gangguan layanan, kerugian finansial atau reputasi sangat kecil Namun, mungkin diperlukan kontrol tambahan atau prosedur operasional alternatif untuk mempertahankan tingkat layanan dan dapat menyebabkan penurunan kualitas layanan	- Beberapa ketidaknyamanan penggunaan sistem TI pada tingkatan lokal, tetapi tidak ada dampak signifikan terhadap keseluruhan TI

Tabel 4. Standar layanan insiden

Dampak Insiden	Notifikasi	Penanganan dan Pemulihan	Pemangku Kepentingan yang Diberi Notifikasi
Kritis	Segera	8 jam	Tim Pengelola TI, Manajemen, BSSN
Signifikan	4 jam	24 jam	Tim Pengelola TI, Manajemen, BSSN
Penting	24 jam	5 hari kerja	Tim Pengelola TI
Rendah	N/a	N/a	N/a

Menentukan Tim Respon Insiden

Tahapan pembentukan Tim Respon Insiden dilakukan sesuai dengan standar ISO/IEC 27035. Atas dasar pertimbangan terbatasnya SDM yang ada di Dinas Komunikasi Informatika DIY, maka Tim Respon Insiden dibentuk dengan melibatkan beberapa pihak luar yang berkompeten di bidangnya.

Tim Respon Insiden dibentuk dengan nama JOGJAPROVCSIRT yang diwujudkan dalam bentuk rancangan surat keputusan Kepala Dinas, didalamnya terdiri dari:

1. Ketua,
2. Wakil Ketua,
3. Sekretaris,
4. Sub tim, terdiri dari:
   a. Sub tim pengelolaan pengaduan,
   b. Sub tim keamanan aplikasi,
   c. Sub tim keamanan basis data,
   d. sub tim keamanan infrastruktur,
   e. Sub tim keamanan *malware*.
   f. Sekretariat.

Layanan yang diberikan oleh JOGJAPROVCSIRT ditetapkan menjadi 3 jenis, yaitu:

1. Layanan reaktif, yaitu:
   a. Pemberian peringatan siber (*alerts and warning*),
   b. Penanggulangan dan pemulihan insiden siber (*incident handling*),
   c. Penanganan kerawanan (*vulnerability handling*), dan
   d. Penanganan artifak (*artifact handling*).

2. Layanan proaktif yaitu audit atau penilaian keamanan (*security audit or assessment*).
3. Layanan manajemen kualitas keamanan, yaitu:
   a. Analisis risiko (*risk analysis*); dan
   b. Edukasi dan pelatihan (*education/training*).

Perancangan Dokumen Manajemen Insiden Keamanan Informasi

Atas dasar hasil tahapan sebelumnya, dilanjutkan dengan tahap perancangan dokumen manajemen insiden. Terdapat 2 aktifitas perancangan yang harus dilakukan untuk memperbaiki sistem manajemen insiden keamanan informasi di Dinas Komunikasi dan Informatika DIY, yaitu:

1. Penyusunan dokumen kebijakan dan prosedur manajemen insiden keamanan informasi yang sesuai dengan SNI ISO/IEC 27035,
2. Penyusunan formulir pendukung aktifitas dalam dokumen kebijakan dan prosedur manajemen insiden keamanan informasi,

Pembuatan dokumen baru dilakukan mengacu pada seluruh kontrol dalam ISO/IEC 27035 dengan mempertimbangkan hasil assesmen pada Tabel 2. Dari hasil assemen awal, hanya 24 kontrol yang sudah dijalankan kemudian diperbaiki agar dokumen dapat meliputi seluruh kontrol yang sesuai standar. Dokumen kebijakan dan prosedur manajemen keamanan informasi yang telah dihasilkan didalamnya terdiri dari beberapa unsur sebagai berikut:

1. Tujuan dan sasaran,
2. Referensi,
3. Ruang lingkup,
4. Tanggung jawab dan komitmen manajemen,
5. Kebijakan umum,
6. Definisi insiden keamanan informasi,
7. Deskripsi kategori insiden keamanan informasi,
8. Deskripsi proses pelaporan insiden,
9. Alur proses insiden mulai dari deteksi sampai dengan resolusi,
10. Kebutuhan aktifitas peninjauan pasca insiden, seperti pembelajaran dan proses perbaikan yang disesuaikan dengan resolusi insiden yang telah dilakukan,
11. Definisi dari masing masing peran, tanggung jawab, dan wewenang pengambilan keputusan yang ditetapkan untuk setiap fase dari proses manajemen insiden keamanan informasi dan kegiatan terkait lainnya,
12. Program pelatihan kompetensi pegawai dan peningkatan kesadaran (*awareness*) keamanan informasi yang terjadwal

Dokumen kebijakan dan prosedur manajemen insiden keamanan informasi yang dibuat juga memuat formulir-formulir aktifitas, yaitu laporan kejadian (*event*) keamanan informasi, laporan insiden keamanan informasi, rekap kejadian(*event*) keamanan informasi, dan rekap insiden keamanan informasi.

Verifikasi dan Validasi

Proses verifikasi dan validasi dilakukan dengan membawa dokumen kebijakan dan prosedur manajemen insiden keamanan informasi kepada Kepala Bidang Keamanan Informasi, Administrator Jaringan, serta Administrator Data Center. Tahap verifikasi dilakukan dengan cara melakukan diskusi. Hal tersebut dilakukan untuk mengetahui apa saja kekurangan pada dokumen serta apakah dokumen sudah sesuai dengan kebutuhan dan ekspektasi yang diiharapkan.

Berdasarkan hasil verifikasi terdapat dua poin perbaikan yaitu:

1. Penambahan dokumen referensi, yaitu dokumen SMKI yang dimiliki oleh Dinas,
2. Perbaikan alur penanganan insiden.

Setelah melewati uji verifikasi atas dokumen yang telah dibuat, dilanjutkan dengan tahapan validasi. Tahapan ini dilakukan dengan cara pembuatan skenario pengujian prosedur serta membuat *checklist* kegiatan yang telah dibuat. Skenario kemudian dijalankan oleh Administrator Data Center dan Administrator Jaringan. Dari proses validasi ini disimpulkan bahwa dokumen kebijakan dan prosedur manajemen keamanan informasi yang telah dibuat dapat dijalankan dengan baik.

KESIMPULAN

Dalam penelitian ini telah dihasilkan dokumen kebijakan dan prosedur manajemen insiden keamanan informasi yang baru dan sesuai dengan standar SNI ISO/IEC 27035. Di dalam sistem manajemen insiden yang dibuat telah meliputi seluruh fase yang diterapkan dalam manajemen isiden secara lengkap. Terdapat penambahan kebijakan dalam pembentukan Tim Respon Insiden, program pelatihan dan peningkatan kapasitas pegawai, peningkatan kesadaran (*awareness*)

keamanan informasi, serta penambahan aktifitas pembelajaran pasca insiden.

Dokumen manajemen insiden keamanan informasi ini akan dijadikan sebagai dokumen baku yang digunakan sebagai acuan resmi dalam manajemen insiden di Dinas Komunikasi dan Informatika DIY pada masa mendatang.

Saran yang diberikan untuk penelitian selanjutnya adalah sebagai berikut :

1. Mengingat hasil dari penelitian ini berupa dokumen pada level kebijakan, maka perlu dilakukan penelitian lanjutan mengenai perancangan prosedur teknis terkait insiden tertentu.
2. Perlu dilakukan penelitian pada objek lain agar dokumen yang telah dibuat ini lebih teruji.
3. Perlu dilakukan penelitian mengenai otomatisasi sistem manajemen insiden keamanan informasi yang sesuai dengan penelitian ini untuk memudahkan dalam penanganan insiden.

DAFTAR PUSTAKA

Ab Rahman, N. H. dan Choo, K. K. R. (2015) "A survey of information security incident handling in the cloud," *Computers and Security*. Elsevier Ltd, 49, hal. 45–69.

Azizah, N., Kusumawati, Y. dan Sani, R. R. (2020) "Perancangan Manajemen Insiden pada Layanan Teknologi Informasi Inventory Menggunakan Framework ITIL Versi3 (Studi Kasus : PT. Genta Semar Mandiri Semarang)," *JOINS (Journal of Information System)*, 5(1), hal. 136–146.

Baskerville, R., Spagnoletti, P. dan Kim, J. (2014) "Incident-centered information security : Managing a strategic balance between prevention and response," *Information & Management*. Elsevier B.V., 51(1), hal. 138–151.

Hove, C., Marte, T., Line, M. B., Bernsmed, K. (2014) "Information security incident management : Identified practice in large organizations," in *Eighth International Conference on IT Security Incident Management & IT Forensics Information*, hal. 27–46.

Ilvarianto, D. S. dan Legowo, N. (2017) "Incident management implementation using continual service improvement method at PT AOP," in *Proceedings - 2017 International Conference on Applied Computer and Communication Technologies, ComCom 2017*, hal. 1–7.

International Organization for Standardization. (2019) *SNI ISO/IEC 27035-1:2016 - Teknologi Informasi - Teknik Keamanan - Manajemen Insiden Keamanan Informasi - Bagian 1 : Prinsip manajemen insiden*. Badan Standardisasi Nasional, Jakarta.

Line, M. B., Tøndel, I. A. dan Jaatun, M. G. (2014) "Information security incident management : Planning for failure," in *Eighth International Conference on IT Security Incident Management & IT Forensics*. IEEE, hal. 47–61.

Nugraha, A. D. dan Legowo, N. (2017) "Implementation of incident management for data services using ITIL V3 in telecommunication operator company," in *Proceedings - 2017 International Conference on Applied Computer and Communication Technologies, ComCom 2017*, hal. 1–6.

Palilingan, V. R. dan Batmetan, J. R. (2018) "Incident Management in Academic Information System using ITIL Framework," in *IOP conferences Series : materials Science and Engineering*. IOP, hal. 0–9.

Rizky, A. F., Herdiyanti, A. dan Susanto, T. D. (2017) "Pembuatan Prosedur Operasional Standar Pengelolaan Insiden pada Government Resources Management Systems Kota Surabaya Berdasarkan ITIL V3," 06(02), hal. 199–214.

Setiawan, A. B. (2014) "Perencanaan Strategis Sistem Informasi Pada Pusat Penanganan Insiden Keamanan Informasi Sektor Pemerintah," *Jurnal Masyarakat Telematika dan Informasi*, 5(1), hal. 1–24.

Tello-Oquendo, L., Tapia, F., Fuertes, W., Andrade, R., Erazo, N. S., Torres, J., Cadena, A (2019) "A structured approach to guide the development of incident management capability for security and privacy," in *ICEIS 2019 - Proceedings of the 21st International Conference on Enterprise Information Systems*, hal. 328–336.

Tondel, I. A., Line, M. B. dan Jaatun, M. G. (2014) "Information security incident management : Current practice as reported in the literature," *Computers & Security*, 45(September), hal. 42–57.

Tsakalidis, G. *et al.* (2019) "A cybercrime incident architecture with adaptive

response policy," *Computers and Security*. Elsevier Ltd, 83, hal. 22–37.

BIODATA PENULIS

Wikankara, S.Kom., lahir di Kulon Progo, tanggal 14 September 1986, menyelesaikan pendidikan S1 Teknik Informatika di IST AKPRIND Yogyakarta tahun 2010. Saat ini sedang menempuh pendidikan jenjang S2 pada Magister Teknologi Informasi di Universitas Gadjah Mada Yogyakarta dengan bidang minat penelitian tata kelola teknologi informasi dan keamanan sistem informasi.

Dr. Ir. Rudy Hartanto, M.T., IPM, lahir di Semarang pada tanggal 15 Maret 1964, menyelesaikan pendidikan S1 bidang ilmu Teknik Elektro dari Universitas Gadjah Mada Yogyakarta tahun 1989, S2 bidang ilmu Teknik Elektro dari Universitas Gadjah Mada Yogyakarta tahun 1995, dan S3 bidang ilmu Teknik Elektro dari Universitas Gadjah Mada Yogyakarta tahun 2015. Saat ini tercatat sebagai Dosen Tetap di Universitas Gadjah Mada Yogyakarta dengan jabatan akademik Lektor Kepala pada bidang minat komputer grafik, multimedia, *human computer interaction* (HCI), sistem informasi, *image processing*, dan *computer vision.*

Ir. Lukito Edi Nugroho, M. Sc., Ph.D, menyelesaikan pendidikan S1 bidang ilmu Teknik Elektro dari Universitas Gadjah Mada Yogyakarta tahun 1989, S2 dari James Cook University of North Queensland, Australia tahun 1994, dan S3 dari School of Computer Science and Software Engineering, Monash University Australia tahun 2002. Saat ini tercatat sebagai Dosen Tetap di Universitas Gadjah Mada Yogyakarta dengan jabatan akademik Lektor Kepala pada bidang minat *distributed & internet computing, context-aware computing, software engineering*, dan *IT for education.*