BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Keamanan sistem informasi merupakan suatu upaya untuk mengamankan aset informasi terhadap ancaman dari orang yang tidak bertanggung jawab. Keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengoptimalkan pengembalian investasi (*return on inverstment*). Semakin banyak infomasi perusahaan yang disimpan dan di kelola maka semakin besar juga resiko terjadinya kerusakan, Oleh karena itu diperlukan Standar Operasional Prosedur (SOP) keamanan sistem informasi untuk dapat membantu proses penanganan dan pencegahan pada saat terjadi insiden serangan agar insiden serangan dapat di tanggani dengan cepat dan baik.

Ciptaningrum et, al. (2015) telah melakukan penelitian yang berjudul "Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan Cobit 5". Penelitian tersebut berkaitan dengan standar operasional prosedur manajemen pengamanan sistem informasi dan komunikasi Pemerintahan Kota Yogyakarta. Sebagai institusi pemerintah yang sudah memanfaatkan teknologi informasi dan komunikasi selama ini Pemerintahan Kota Yogyakarta belum pernah melaksanakan audit terhadap keamanan sistem informasi. Proses pengecekan keamanan ini bertujuan untuk perwujudan *e-government* dalam lingkungan pelayanan masyarakat (Pemerintah Kota Yogyakarta). Metode yang digunakan dalam penelitian ini adalah COBIT 5. Metode ini digunakan karena banyak penelitian mengenai COBIT 5 yang membuktikan bahwa COBIT 5 merupakan kerangka kerja untuk audit keamanan SI dan mampu menyediakan tata kelola keamanan informasi yang menyeluruh (spremic, 2011:5) (Spremic et al., 2010 :3) (huang et al., 2009:2) (morimoto, 2009:1). Bahkan dalam COBIT 5 juga terdapat tujuan terkait TI keamanan dan juga memiliki satu fungsi dari COBIT 5 yang khusus fokus pada keamanan informasi, yaitu COBIT 5 *for Information Security*. COBIT 5 merupakan sebagai metode yang tepat untuk melakukan audit keamanan Sistem Informasi bagi Pemerintah Kota Yogyakarta.

Pada penelitian yang telah dilakukan oleh Chazar (2015), berjudul "Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005". Penelitian yang telah dilakukan oleh Chazar berkaitan dengan masalah keamanan sistem informasi yang dapat merugikan perusahaan. Masalah keamanan seringkali kurang mendapat perhatian dari pihak *stakeholder*. Ketika sebuah ancaman sudah menimbulkan kerugian pada perusahaan, *stakeholder* dan pengelola sistem mulai melakukan berbagai tindakan pencegahan dan perbaikan atas keamanan sistem informasi. Hal ini dapat menyebabkan perusahaan mengeluarkan pengeluaran ekstra untuk melakukan pengamanan sistem informasi dan perbaikan atas ancaman yang sudah terjadi. Metode yang digunakan dalam penelitian ini adalah ISO/IEC 27001. Metode ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu *confidentiality, integrity dan availability*.

Pada penelitian yang dilakukan oleh Rachmi et, al. (2014), berjudul "Pembuatan Standar Operasional Prosedur (SOP) *Service Desk* berdasarkan kerangka kerja ITIL V3". Penelitian yang telah dilakukan oleh Rachmi berkaitan dengan pembuatan Standar Operasional *service desk* dengan menggunakan kerangka kerja ITIL V3. ITIL merupakan salah satu solusi yang diperlukan dalam upaya meningkatkan layanan TI dan mengatasi masalah yang ada saat ini. Produk akhir yang dihasilkan dari peneltian ini adalah sebuah dokumen *Standard Operating Procedure* (SOP) *Service Desk* dengan standar ITIL V3 yang diverifikasi dan divalidasi dengan menggunakan teknik wawancara dengan pihak terkait, simulasi pengujian SOP, dan *survey*.

Pada penelitian yang telah dilakukan oleh Andy (2016), berjudul "Penanganan dan Pencegahan Insiden pada Serangan DDos di jaringan komputer sesuai Rekomendasi NIST 800-61". Penelitian yang telah dilakukan oleh Andy berkaitan dengan bagaimana cara penanggulangan insiden DDoS pada jaringan yang sesuai dengan standar NIST 800-61 (cichonski et, al.,2012). Metode yang digunakan dalam penelitian ini adalah NIST 800-61. Metode NIST 800-61

(*inciden handling*) merupakan kerangka kerja sukarela yang terdiri dari standar pedoman, dan praktik terbaik untuk mengelola risiko yang terkait dengan *cybersecurity*.

Perbandingan Penelitian Metode Penanganan Insiden yang pernah dilakukan dapat dilihat pada table 2.1 berikut :

Table 2.1. Tabel pembanding Penelitian Penanganan Insiden

Penelitian	Ciptaningrum et,al., 2015	Chazar(2015)	Rachmi et, al., 2014	Andy (2016)	Charles (2019)
Topik	Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan Cobit 5	Standar Manajemen Keamanan sistem Informasi Berbasis ISO/IEC 27001:2005	Pembuatan Standar Operasional Prosedur (SOP) *Service desk* berdasarkan kerangka kerja ITIL V3	Penanganan dan Pencegahan Insiden pada Serangan Dos di jaringan komputer sesuai Rekomendasi NIST 800-61	Analisis Penanganan dan Pencegahan Seranagan Siber pada *website* dengan menggunakan Metode NIST SP 800-61
Metode	COBIT 5	ISO 27001	ITIL V3	NIST 800-61	NIST 800-61
Fungsi Khusus	Manajemen Resiko Teknologi Informasi	*Information Security Management System* (ISMS)	*Best Practice* dalam penerapan Manajemen Layanan Teknologi Informasi	Penanganan Insiden (*Insident Handling*)	Penanganan Insiden (*Insident Handling*)
Publis	*Information Domains Audit and Control Association* (ISACA) IT *Governance Institute*	ISO dan IEC Tahun 2005	*IT Infrastructur e Library*	*National Institute of Standards dan Technology* (NIST) Tahun 2002	*National Institute of Standards dan Technology* (NIST) Tahun 2002
Dapat Digunakan Pada	*Government*	*Government*	*Government*	Umum	Umum
Hasil	standar operasional dan prosedur manajemen pengamanan sistem informasi dan telekomunikasi di lingkungan Pemerintah Kota Yogyakarta	Pedoman *Best Practice* pada manajemen layanan TI (Teknologi Informasi)	Standar Operasional Prosedur (SOP) Pada *Service desk*	Penanganan Insiden Serangan DDOS	Standar Operasional Prosedur (SOP) serangan pada *Website*