TUGAS MATA TATA KELOLA TI KELAS A
REVIEW ARTIKEL : AN INFORMATION SECURITY PERFORMANCE MEASUREMENT TOOL FOR SENIOR MANAGERS: BALANCED SCORECARD INTEGRATION FOR SECURITY GOVERNANCE AND CONTROL FRAMEWORKS

NAMA ANGGOTA :

1. Akmal Ihab Syauqi 222410101034
2. Muhammad Faiq Ammar 222410101039
3. Haikal Nuril Abiyit 222410101058
4. Rafi Jauhari 222410101087
5. Muhammad Afif Rohman M. 222410101095

PRODI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS JEMBER

2024

1. Pembukaan

Di era digital, keamanan informasi telah menjadi keharusan bisnis strategis, yang membutuhkan keselarasan dengan tujuan organisasi. Tinjauan ini mengusulkan kerangka kerja yang sederhana, yaitu *Information Security Balanced Scorecard* (InfoSec BSC), untuk memfasilitasi penilaian kinerja strategi keamanan. Dengan mengintegrasikan berbagai kerangka kerja tata kelola dan kontrol, panduan praktis disediakan untuk mengembangkan ukuran kinerja dan indikator kinerja utama untuk manajemen keamanan informasi. Sebuah studi kasus di *North American University* (NAU) menggambarkan penerapan InfoSec BSC, yang memberikan wawasan berharga bagi para praktisi.

2. Balanced Scorecard Approach to Information Security

2.1. Need for a Balanced Scorecard Pertaining to Information Security

Manajemen strategis keamanan informasi muncul sebagai pertimbangan penting bagi organisasi, yang membutuhkan pemahaman yang bernuansa tentang kerangka kerja dan standar yang ada. Meskipun ada berbagai model teoritis dan model khusus industri, penerapan bersyarat dan kompleksitasnya menimbulkan tantangan. Pengukuran kinerja, khususnya melalui alat seperti *Balanced Scorecard* (BSC), sangat penting dalam menyelaraskan strategi keamanan dengan tujuan organisasi, memfasilitasi tata kelola yang dapat dipahami di berbagai tingkatan.

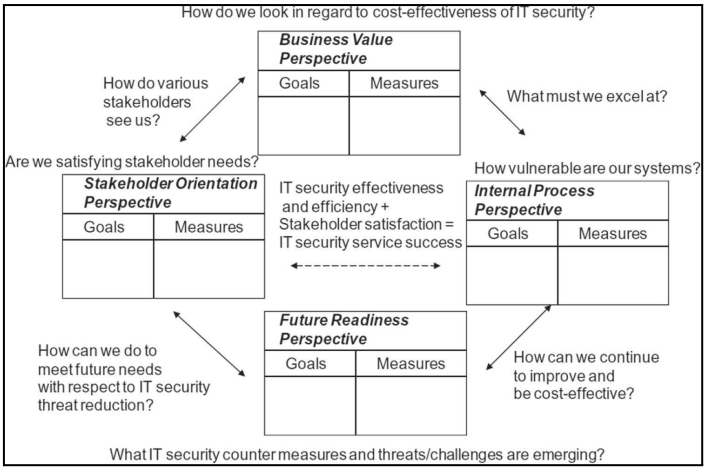
Tantangan tetap ada dalam menjustifikasi investasi keamanan, mengukur tujuan, dan mensintesis data terkait keamanan yang luas. Kebutuhan akan alat untuk mengatur data secara bermakna dan mengevaluasi strategi keamanan di luar metrik keuangan tradisional menjadi jelas. Mengkomunikasikan manfaat strategi keamanan kepada manajemen senior menghadirkan rintangan lebih lanjut.

Keputusan penting mengenai internalisasi versus outsourcing aktivitas keamanan, ditambah dengan tingkat investasi sumber daya strategis, membentuk strategi keamanan organisasi. Klasifikasi organisasi ke dalam kelompok-kelompok berdasarkan komitmen mereka terhadap keamanan informasi menggarisbawahi kompleksitas proses pengambilan keputusan ini.

Bagi organisasi yang memilih untuk menangani aktivitas keamanan secara internal, menjawab pertanyaan kritis mengenai implementasi dan efektivitas mekanisme keamanan sangatlah penting. Ini menekankan perlunya pandangan strategis dan tata kelola yang efisien untuk menavigasi kompleksitas manajemen keamanan informasi secara efektif.

2.2. Traditional Balanced Scorecard (BSC)

Balanced Scorecard (BSC), yang diperkenalkan oleh Robert Kaplan dan David Norton, menawarkan sistem manajemen kinerja yang komprehensif yang bertujuan untuk menyelaraskan aktivitas bisnis dengan tujuan strategis. Dengan menggabungkan perspektif keuangan, pelanggan, proses internal, inovasi, dan pembelajaran organisasi, BSC memungkinkan para manajer untuk mendapatkan pandangan holistik tentang kinerja organisasi dan mengidentifikasi keterkaitan antara berbagai metrik. Melalui BSC, organisasi dapat merampingkan tujuan mereka, melacak kemajuan secara efektif, dan mengalokasikan sumber daya berdasarkan bobot kepentingan indikator kinerja utama. Model ini menekankan empat pertanyaan mendasar yang harus dijawab oleh para manajer, dengan fokus pada persepsi pelanggan, keunggulan bisnis internal, inovasi dan pembelajaran, serta nilai pemegang saham. Namun, implementasi yang sukses membutuhkan penyelarasan yang cermat dengan strategi organisasi, dengan metrik yang berfungsi sebagai indikator kemajuan menuju tujuan, baik yang terdepan maupun yang tertinggal. Indikator-indikator utama berfungsi sebagai pendorong kinerja yang unik untuk unit bisnis tertentu, yang berkontribusi pada pencapaian tujuan organisasi secara menyeluruh. Secara keseluruhan, BSC menawarkan kerangka kerja yang fleksibel yang dapat disesuaikan dengan konteks organisasi yang beragam, sehingga memudahkan pengambilan keputusan dan pemecahan masalah.



Contoh InfoSec BSC

2.3. Balanced Scorecards for IT and Information Security

Model *Balanced Scorecard* (BSC), meskipun banyak digunakan untuk melacak kinerja organisasi, sering kali mengabaikan aspek penting dari keamanan informasi. Memasukkan keamanan informasi ke dalam kerangka kerja BSC sangat penting mengingat meningkatnya ketergantungan pada teknologi dalam bisnis. Modifikasi yang diusulkan pada perspektif BSC tradisional menekankan pentingnya menyelaraskan TI dan keamanan informasi dengan tujuan bisnis secara keseluruhan. Secara khusus, kerangka kerja InfoSec BSC menawarkan pendekatan yang komprehensif dengan mempertimbangkan nilai bisnis, orientasi pengguna, proses internal, dan kesiapan masa depan dalam kaitannya dengan tata kelola keamanan informasi.

Perspektif Nilai Bisnis dari InfoSec BSC menunjukkan pentingnya menyelaraskan strategi keamanan dengan tujuan bisnis untuk meningkatkan kinerja, melindungi reputasi, dan menumbuhkan kepercayaan di antara para pemangku kepentingan. Metrik harus menunjukkan nilai yang diperoleh dari investasi TI sambil memastikan keamanan dalam batasan anggaran.

Orientasi Pengguna dari InfoSec BSC menyoroti beragam pemangku kepentingan yang mendapatkan manfaat dari layanan keamanan TI, menekankan perlunya mengatasi masalah kegunaan dan masalah privasi bagi karyawan dan pelanggan.

Perspektif Proses Internal dari InfoSec BSC berfokus pada penyediaan produk dan layanan keamanan secara efisien dan efektif dengan

mempertimbangkan dampaknya terhadap operasi organisasi. Metrik harus menilai perencanaan, penerapan, dan pemeliharaan inisiatif keamanan, serta pelatihan karyawan dan peningkatan teknologi untuk meminimalkan risiko keamanan.

Perspektif Kesiapan Masa Depan dari InfoSec BSC menekankan pada peningkatan berkelanjutan dan kesiapan untuk menghadapi ancaman keamanan siber yang terus berkembang. Hal ini mencakup pelatihan berkelanjutan bagi staf TI dan pengguna, peningkatan infrastruktur teknologi, dan penelitian solusi inovatif untuk mengantisipasi tantangan di masa depan.

Secara keseluruhan, InfoSec BSC menyediakan kerangka kerja holistik untuk mengukur dan mengelola kinerja keamanan informasi, memastikan keselarasan dengan tujuan bisnis dengan tetap dapat dimengerti oleh para eksekutif senior dan karyawan.

2.4. Prior Literature in IS Security Balanced Scorecard

T. Herath et al. (2010)	Development of a conceptual framework of an information security BSC based on the traditional BSC and an IT BSC by Martinsons et al. (1999)
Bachlechner et al. (2014)	BSC perspective to look at the security and compliance challenges focusing on IT outsourcing arrangements
Goldman and Ahuja (2011)	Integration of COBIT and BSC for information security management
Tallau et al. (2010)	Justification and comparison of IT security investments
Hamdan (2013)	Arguing that existing governance frameworks do not provide an inclusive mechanism to evaluate performance of information security, presents conceptual BSC framework
Atoum and Otoom (2016)	Modification of T. Herath et al.'s (2010) information security BSC framework to apply it at the country level
Kong et al. (2012)	Identification of key performance indicators for information security investments through literature and investigation of the relationship among the KPIs using data collected through a survey
Tu et al. (2018)	Empirical evaluation of antecedents of information security management performance (ISMP) – ISMP captured through the lens of a BSC
de Oliveira Alves et al. (2006)	Recommends BSC – suggests that the BSC works as an interpreter for the business goals, meeting vision requirements, mission and strategical planning, while CobiT works as a bridge for business processes, considering business objectives and being controlled by the BSC.

Literatur Sebelumnya dalam InfoSec BSC

Integrasi kerangka kerja *Balanced Scorecard* (BSC) ke dalam manajemen keamanan informasi telah menarik perhatian para peneliti. Berbagai penelitian telah mengeksplorasi penerapannya, mulai dari kerangka kerja konseptual hingga implementasi praktis dalam pengaturan organisasi yang berbeda.

Peneliti seperti Herath et al. (2010) dan Bachlechner et al. (2014) telah mengusulkan model BSC yang secara khusus dirancang untuk implementasi strategi keamanan informasi dan mengelola tantangan keamanan dalam pengaturan outsourcing TI yang kompleks. Yang lainnya, seperti Goldman dan Ahuja (2011), telah menganjurkan untuk mengintegrasikan COBIT dengan BSC untuk menyediakan mekanisme komprehensif yang menyelaraskan strategi bisnis, TI, dan keamanan.

Namun, artikel ini memperkenalkan pendekatan baru dengan mengintegrasikan lima kerangka kerja kontrol keamanan dan tata kelola dengan BSC khusus keamanan untuk mengidentifikasi seperangkat tujuan strategis keamanan informasi. Artikel ini menggunakan skenario dunia nyata dalam lingkungan universitas untuk mengembangkan ukuran kinerja, memfasilitasi identifikasi target dan inisiatif untuk implementasi strategi keamanan informasi.

Kerangka kerja BSC muncul sebagai alat yang cocok untuk mengukur kinerja keamanan informasi karena meningkatnya ancaman *cyber* yang dihadapi organisasi. Fleksibilitasnya memungkinkan organisasi untuk menyelaraskan tujuan TI dan keamanan dengan tujuan organisasi yang lebih luas. Selain itu, kerangka kerja ini menyediakan metode terstruktur untuk menyajikan metrik keamanan informasi kepada manajemen eksekutif, yang sangat penting dalam menghadapi sistem TI yang tidak berwujud dan kesulitan dalam mengukur tujuan keamanan.

Artikel ini menegaskan pentingnya mematuhi pedoman yang telah ditetapkan dalam mengadaptasi BSC untuk tujuan keamanan, dengan mengutip kerangka kerja Kaplan dan Norton dan pendekatan Microsoft TechNet sebagai contoh. Ini membahas peningkatan berbagai tata kelola TI dan metodologi kontrol menggunakan BSC, dengan mencontohkan templat kartu skor berdasarkan ISO 17799 sebagai dasar untuk strategi keamanan. Pendekatan ini menggunakan model *Event-Asset-Impact* untuk memetakan kategori ISO 17799 ke perspektif BSC tradisional, yang memberikan pandangan komprehensif tentang manajemen keamanan informasi.ikasi target dan inisiatif untuk implementasi strategi keamanan informasi.

3. Information Technology/Security Governance and Control Frameworks

Banyak sekali framework yang dapat digunakan dalam mengembangkan Teknologi Informasi, Sekuritas dan Kontrol dalam Organisasi, contohnya ada COBIT, ITIL, ISO, ISG, SABSA, dan masih banyak kerangka kerja lainnya yang dapat digunakan sebaik mungkin.

Saat ini, ada dua model yang berada di garis depan dan digunakan sebagai standar untuk teknologi dan keamanan sistem informasi organisasi. *The National*

Institute of Standards and Technology (NIST) dan *International Organization for Standardization* (ISO). Pada sub-bab selanjutnya akan dijelaskan secara singkat mengenai macam-macam framework yang umum digunakan, mulai dari COBIT, ITIL, ISO, ISG, dan SABSA.

3.1. Control Objectives for Information Technology (COBIT)

[1] "The current version is COBIT 5, which is the leading business framework for governance and management of enterprise IT (ISACA). COBIT 5 builds on the previous versions of COBIT (and Val IT and Risk IT), and without loss of information in this article, we focus on COBIT 4.1. COBIT 5 goals cascade stakeholder needs into specific actionable and customized goals within the context of enterprise, IT-related goals and enabler goals. The enterprise goals have been developed using the BSC dimensions and the list is not exhaustive (ISACA). COBIT 5 separates IT governance (evaluate stakeholder needs, set direction through prioritization, and monitor performance, compliance, and progress) and IT management (plan, build, run, and monitor activities with direction set by governance).

The Control Objectives for Information Technology (COBIT) diterbitkan oleh Systems Audit and Control Association (ISACA) pada tahun 2011. COBIT adalah sebuah Kerangka kerja kontrol tata kelola TI yang membantu organisasi memenuhi dan mengelola kerentanan dan memastikan kepatuhan, mengevaluasi dan mengoptimalkan risiko perusahaan, mengawasi dan mengelola keamanan informasi, dan menangani kepatuhan terhadap peraturan dan tata kelola TI perusahaan dengan menyelaraskan tujuan TI dan tujuan bisnis strategis. COBIT didasarkan pada prinsip berikut: Untuk menyediakan informasi yang dibutuhkan perusahaan untuk mencapai tujuannya, perusahaan perlu berinvestasi dan mengelola serta mengendalikan sumber daya TI menggunakan serangkaian proses terstruktur untuk menyediakan layanan yang memberikan informasi perusahaan yang dibutuhkan.

Pengendalian menggunakan framework COBIT memberikan syarat-syarat supaya seluruh objektif dari sebuah organisasi bisa terlaksana, ciri-ciri framework COBIT adalah:

- sebuah pernyataan tindakan manajerial untuk meningkatkan nilai atau mengurangi risiko
- terdiri dari kebijakan, prosedur, praktik, dan struktur organisasi
- dirancang untuk memberikan jaminan yang wajar bahwa tujuan bisnis akan tercapai dan kejadian yang tidak diinginkan akan dicegah atau dideteksi dan diperbaiki.

3.2. Information Technology Infrastructure Library (ITIL)

Information Technology Infrastructure Library (ITIL) dikembangkan oleh Central Computer and Telecommunication Agency (CCTA). ITIL adalah seperangkat kode etik yang komprehensif dan Kode latihan yang terkait dengan TI untuk manajemen layanan TI. Ini sangat berguna dalam hal mencapai dukungan yang efisien dan memberikan layanan TI yang berkualitas tinggi dan hemat biaya. Lebih lanjut Secara khusus, ITIL adalah kumpulan panduan latihan terbaik tentang pengelolaan layanan TI. Hal ini ditawarkan sebagai "kerangka kerja yang komprehensif dari mana organisasi, atau agen, dapat memperoleh struktur untuk merancang dan mengimplementasikan prosedur mereka sendiri." tujuan utama dari manajemen layanan ITIL adalah untuk memastikan dan mendukung keselarasan layanan TI dengan kebutuhan bisnis.

3.3. International Organization for Standards (ISO)-ISO 27000 Family: 2013

Rangkaian standar ISO 27000 Series dirancang untuk menjaga keamanan aset informasi. Secara lebih spesifik, standar ini membantu organisasi mengelola aset keamanan seperti informasi keuangan, kekayaan intelektual, data karyawan, dan pihak ketiga informasi. ISO/IEC 27001 adalah standar dalam keluarga yang menyediakan persyaratan untuk Information Security Management System (ISMS). ISMS menyediakan pendekatan sistematis untuk mengelola dan mengamankan informasi perusahaan yang sensitif, melalui manajemen risiko yang yang mencakup orang, proses, dan sistem TI. ISO/IEC 27000 dimaksudkan untuk menyediakan semua informasi yang diperlukan yang diperlukan untuk merencanakan, mengimplementasikan, dan mengoperasikan Information Security Management System (ISMS).

Berikut beberapa perubahan dari ISO 27000 tahun 2005 ke tahun 2013.

Table 2 Comparison of ISO 27000 Security Control Categories

ISO 27000:2013 Categories (14 in Total)	ISO 27000:2005 Categories (11 in Total)
1 Information Security Policies	Security Policy
2 Organization of Information Security	Organization of Information Security
3 Human Resource Security	Human Resource Security
4 Asset Management	Asset Management
5 Access Control	Access Control
6 Cryptography	
7 Physical and Environmental Security	Physical and Environmental Security
8 Operations Security	Communications and Operations Management
9 Communications Security	
10 System Acquisition, Development, and Maintenance	Information Systems Acquisition, Development, and Maintenance
11 Supplier Relationships	
12 Information Security Incident Management	Information Security Incident Management
13 Information Security Aspects of Business Continuity Management	Business Continuity Management
14 Compliance	Compliance

3.4. Information Security Governance (ISG)

IT Governance Institute (ITGI) didirikan pada tahun 1998 dengan tujuan untuk memajukan pemikiran dan standar internasional dalam internasional dalam mengarahkan dan mengendalikan teknologi informasi perusahaan. Menurut ITGI, Information Security Governance (ISG) membahas mengenai perlindungan informasi, kerahasiaan, ketersediaan, dan integritas di seluruh siklus hidup informasi dan penggunaannya di dalam organisasi. Tata kelola untuk program keamanan informasi harus disediakan dari puncak organisasi ke bawah untuk memastikan bahwa tujuan organisasi dapat terpenuhi dengan tepat. Informasi kebijakan dan prosedur harus dapat diterima dan disediakan dalam berbagai media yang mengakomodasi semua karyawan. Lima hasil yang diinginkan dari tata kelola keamanan informasi menurut ISG meliputi:

1. strategic alignment;
2. risk management;
3. resource management;
4. performance measurement;
5. value delivery.

3.5. Sherwood Applied Business Security Architecture (SABSA)

SABSA adalah metodologi untuk mengembangkan keamanan informasi perusahaan yang berbasis risiko, arsitektur jaminan informasi, dan untuk memberikan solusi infrastruktur keamanan yang mendukung inisiatif bisnis yang penting. SABSA melakukan pekerjaan yang sangat baik dalam menggabungkan kebutuhan bisnis dengan teknologi. Menurut SABSA Institute, SABSA digunakan secara luas untuk Arsitektur Jaminan Informasi dan Kerangka Kerja

Manajemen Risiko serta untuk menyelaraskan dan mengintegrasikan keamanan dan manajemen risiko ke dalam Arsitektur TI.

4. Development and Implementation of InfoSec BSC – Information Security Measurement Program (ISMP) by the National Institute of Standards and Technology (NIST)

Implementasi dari InfoSec BSC memiliki banyak manfaat yang selaras dengan kerangka kerja keamanan *cyber National Institute of Standards and Technology (NIST)*. Contoh dari manfaatnya adalah meningkatkan akuntabilitas yang mana organisasi dapat menangani akuntabilitas untuk keamanan informasi mereka. Meningkatkan efisiensi pada aktifitas yang berhubungan dengan keamanan informasi. Menunjukkan kepatuhan kepada regulasi dan juga hukum. Yang terakhir yaitu menyajikan hasil yang terukur, hasil yang terukur ini memfasilitasi aktivitas pengelolaan dan memungkinkan hubungan yang jelas antara hasil kegiatan kemanana dan investasi dalam kontrol dan inisiatif keamanan.

4.1. NIST Guidelines for Developing Security Performance Measures and Implementation of an ISM – NIST Risk Management Framework (RMF)

The risk management framework (RMF) yang dijelaskan dalam NIST *Special Publication 800-37* adalah proses tersturktur dan disiplin yang mengintegrasikan aktivitas keamanan informasi dan manajemen risiko ke dalam siklus hidup pengembangan sistem atau *Software Development Life cycle* (SDLC). Langkah-langkah dalam RMF tersebut dapat berguna saat membuat sistem pengukuran kinerja untuk keamanan informasi menggnakan InfoSec BSC. Secara garis besar, langkah-langkahnya meliputi:

1. Kategorisasi. Mengidentifikasi dan mengelompokkan sistem informasi dalam organisasi untuk memahami potensi kerentanan masing-masing sistem.
2. Analisis Dampak. Mengukur dampak yang ditimbulkan jika suatu sistem gagal berfungsi.
3. Pemilihan dan Implementasi Kontrol Keamanan. Berdasarkan hasil kategorisasi dan analisis dampak, memilih dan menerapkan kontrol keamanan yang sesuai untuk memitigasi risiko pada setiap sistem.
4. Penilaian. Memastikan bahwa kontrol keamanan yang diterapkan berfungsi dengan baik dan mencapai tujuan yang diinginkan.
5. Otorisasi. Menerima konfirmasi resmi untuk mengoperasikan sistem informasi dengan kesadaran akan risiko yang ada dan pemahaman dari tim keamanan bahwa risiko tersebut dapat diterima.
6. Pemantauan dan Penilaian Ulang Berkelanjutan. Melakukan pemantauan dan penilaian ulang terhadap sistem informasi secara

berkala untuk memastikan tidak ada masalah yang muncul sejak sistem tersebut diterapkan. Pemantauan sangat penting karena teknologi berubah dan berkembang setiap detiknya.

4.2. Security Performance Measure Characteristics

NIST menguraikan berbagai faktor yang harus dipertimbangkan organisasi ketika mengembangkan dan menerapkan pengukuran kinerja keamanan (Chew et al., 2008). Faktor-faktor tersebut meliputi:

1. Informasi yang Terukur.
2. Konsistensi dan Pengulangan
3. Kemudahan dalam Mendapatkan Data
4. Tren dan Tindakan Korektif

Karakteristik ini dapat diterapkan saat mengembangkan ukuran kinerja untuk perspektif dan tujuan InfoSec BSC. Hal ini untuk memastikan bahwa materi yang dihasilkan akan mmeberikan informasi terukur yang berguna unutk pengambilan keputusan. Mengembangkan dan menerapkan program pengukuran keamanan informasi membutuhkan banyak waktu. Biaya pengukuran cenderung menurun seiring dengan otomatisasi pengumpulan data. Namun, volume data yang besar dapat menimbulkan masalah tambahan dalam mengidentifikasi data yang paling berguna dan menyajikannya dengan cara yang bernilai.

Kerangka NIST juga membedakan beberapa jenis ukuran kinerja dan proses pengembangannya. Jenis ukuran kinerja yang efektif terkait langsung dengan kematangan portofolio dan aktivitas keamanan informasi organisasi. Semakin matang portofolio keamanan informasi, semakin mungkin memiliki kebijakan dan prosedur terperinci yang terdokumentasi dengan baik, dapat diulang, dan karenanya dapat diukur. Tiga jenis ukuran yang relevan dengan kemanan informasi menurut panduan manajemen kinerja NIST adalah:

1. Ukuran Implementasi (*Implementation Measure*). Untuk mendemonstrasikan progres pada implementasi menganai kontrol keamanan, program, kebijakan, dan prosedur.
2. Efisiensi Kontrol (*Effectiveness/Efficiency Measure*). Untuk memonitor, mengukur efektifitas dan efisiensi kontrol dalam mencapai tujuan keamanan.
3. Ukuran dampak (*Impact measure*). Mengukur kualitas dan melihat dampak dari program keamanan informasi pada organisasi.

Mengembangkan pengukuran kinerja keamanan informasi memerlukan beberapa pertimbangan penting menurut NIST, yaitu pemilihan ukuran yang cermat dengan perhatian khusus pada sesuatu yang memengaruhi misi organisasi dan prioritas keamanan informasi, menerima masukan dan edukasi kepada semua pemangku kepentingan yang relevan, dan memastikan infrastruktur keamanan informasi yang memadai, seperti alat pengumpulan data, analisis, dan pelaporan. Setelah program pengukuran keamanan informasi dipilih dan dikembangkan,

program tersebut harus diterapkan. InfoSec BSC berperan sebagai alat analisis dan penilaian untuk memahami portofolio keamanan informasi yang ada dan mengidentifikasi aktivitas bernilai tambah serta potensi tindakan perbaikan. Ini hanyalah bagian dari keseluruhan proses implementasi program pengukuran keamanan informasi.

4.3. Information Security Measurement Program (ISMP) Implementation Process

The Information Security Measurement Program (ISMP) memiliki 6 langkah proses implementasi yang berdasarkan kerangka NIST [(Chew et al., 2008), 35-40]:

1. Persiapan Pengumpulan Data. Merencanakan aktivitas yang diperlukan untuk membuat program IS yang komprehensif, seperti mengenali, memilih, dan mengembangkan metrik IS yang berguna.
2. Pengumpulan Data dan Analisis Hasil. Memastikan bahwa semua metrik yang dikumpulkan digunakan untuk memahami sistem keamanan informasi dan mengidentifikasi peluang perbaikan yang efektif.
3. Identifikasi Tindakan Korektif. Mengembangkan strategi untuk menutup kesenjangan implementasi yang teridentifikasi pada langkah 2.
4. Pengembangan Kajian Bisnis. Menganalisis risiko dan biaya terkait dengan mempertahankan keadaan saat ini sebagai dasar untuk dibandingkan dengan alternatif investasi lainnya.
5. Perolehan Sumber Daya. Mengatasi siklus penganggaran untuk memperoleh sumber daya yang diperlukan untuk menerapkan tindakan korektif yang diidentifikasi pada langkah 3.
6. Penerapan Tindakan Korektif. Menerapkan tindakan korektif yang dipilih dalam program IS atau dalam area operasional, manajemen, atau kontrol keamanan teknis.

Selain itu, menurut publikasi khusus NIST pada juli 2008 berjudul "*Performance Measurement Guide for Information Security*", program pengukuran keamanan informasi harus terdiri dari empat komponen saling bergantung untuk mencapai keberhasilan. Komponen tersebut meliputi:

1. Dukungan Manajemen Tingkat Atas yang Kuat. Dukungan ini penting untuk implementasi dan keberhasilan jangka panjang program keamanan informasi.
2. Kebijakan dan Prosedur Keamanan Informasi yang Praktis. Kebijakan dan prosedur yang jelas diperlukan untuk mengukur dan mendokumentasikan kemajuan program secara akurat. Prosedur

tersebut juga harus dapat menyediakan data yang dapat digunakan untuk pengukuran.

3. Pengembangan Ukuran Kinerja yang Terukur. Mengembangkan ukuran kinerja yang terukur untuk menghasilkan data kinerja yang berarti dan terkait dengan tujuan keamanan informasi. Ukuran tersebut harus dapat diulang karena tren kinerja sering berubah dari waktu ke waktu.
4. Analisis Ukuran Berorientasi Hasil. Analisis ini menekankan pengukuran dan analisis data yang dikumpulkan secara konsisten dan berorientasi pada hasil. Hasil ini digunakan untuk "menerapkan pembelajaran, meningkatkan efektivitas kontrol keamanan yang ada, dan merencanakan implementasi kontrol keamanan di masa depan" [(Chew et al., 2008), 4].

Dengan menerapkan InfoSec BSC, organisasi dapat memperoleh hasil analisis ukuran yang berarti dan dapat memberikan justifikasi yang signifikan untuk keputusan yang secara langsung memengaruhi aktivitas keamanan informasinya.

5. Mapping Security Control and Governance Frameworks and Developing InfoSec BSC in Case Application

Untuk mengembangkan ukuran kinerja untuk manajemen keamanan, beberapa poin perlu diperhatikan. Banyak kerangka kerja keamanan mungkin mencakup sebagian besar aspek tata kelola TI dengan beberapa duplikasi dan tumpang tindih ketika digunakan secara kolektif. Sebaliknya, sebuah kerangka kerja tata kelola dan kontrol tunggal mungkin tidak mencakup semua hal.

Dalam pertimbangan pengembangan ukuran kinerja keamanan, kritik utama terhadap ukuran seperti ROSI dan ALE adalah bahwa mereka cenderung hanya memperhitungkan aspek keuangan dan oleh karena itu juga disebut sebagai ukuran tertinggal atau umum. Ukuran pemimpin adalah penggerak kinerja yang penting untuk mencapai hasil yang diinginkan atau ukuran tertinggal (peningkatan laba organisasi atau pertumbuhan penjualan melalui keamanan informasi yang lebih baik). Karena tidak ada strategi bisnis yang identik, penting bagi organisasi untuk mengembangkan ukuran unik untuk keamanan informasi yang sejalan dengan strategi bisnis mereka sendiri, dan kerangka kerja InfoSec BSC umum adalah alat yang berguna untuk tujuan ini. Desain InfoSec BSC untuk digunakan oleh manajer senior adalah untuk mengidentifikasi tujuan keamanan informasi yang berkaitan dengan masing-masing dari empat perspektif InfoSec BSC yang dibahas selanjutnya.

5.1. Research Methodology, Analysis and Findings

5.1.1. Phase 1

Pada tahap pertama, standar dipetakan menggunakan coding manual dengan bantuan mahasiswa tingkat akhir. Codebook disiapkan untuk mengidentifikasi empat perspektif InfoSec BSC dan kategori tambahan "tidak ada" untuk menghilangkan kemungkinan memasukkan kerangka kerja secara paksa ke dalam kategori InfoSec BSC. Para coder terlebih dahulu diinstruksikan untuk memahami sepenuhnya protokol coding. Untuk menguji reliabilitas antar coder, kami menggunakan metode persentase agreement sederhana, menilai kesepakatan antara coder dari 0 (tidak ada kesepakatan) hingga 1 (kesepakatan sempurna) (Lombard et al., 2002)

Item yang dipetakan secara konsisten ke dalam keempat perspektif InfoSec BSC dipertahankan, sementara item yang tidak cocok atau dianggap tidak termasuk dalam keempat perspektif tersebut dianggap tidak cocok. Tinjauan ahli terhadap pemetaan ini menghasilkan penyesuaian tambahan untuk memindahkan beberapa item ke area yang dipetakan. Lima kerangka kerja utama yang dipertimbangkan dalam penelitian ini telah dipetakan. Hasilnya disajikan dalam Lampiran sebagai berikut:

1. Pemetaan tujuan IT generik COBIT 4.1 terhadap perspektif InfoSec BSC (Tabel Lampiran 6) menunjukkan sifat menyeluruh dari kerangka kerja tersebut. Tabel Lampiran 7 menyajikan proses IT COBIT yang secara khusus terkait dengan keamanan informasi yang dipetakan ke perspektif InfoSec BSC.
2. Pemetaan konsep, proses, dan aktivitas yang berkaitan dengan tahapan siklus hidup layanan ITIL ke perspektif InfoSec BSC ditunjukkan pada Tabel Lampiran 8.
3. Pada Tabel Lampiran 9, ISO 27001-2:2013 dan SecSDLC dipetakan ke perspektif InfoSec BSC.
4. Pemetaan hasil yang diinginkan, manfaat, dan program ISG ke perspektif InfoSec BSC disajikan pada Tabel Lampiran 10.
5. Sebagian besar Atribut Bisnis telah dipetakan ke perspektif InfoSec BSC pada Tabel Lampiran 11.

5.1.2. Phase 2

Pada tahap penelitian ini, studi kasus digunakan untuk mengkaji penilaian strategi keamanan IS secara lebih mendalam. Universitas Amerika Utara (NAU) dipilih untuk melihat penerapan InfoSec BSC. Studi kasus ini memberi kami kesempatan berharga untuk memahami masalah implementasi keamanan informasi serta memperluas pengetahuan kami tentang subjek dari perspektif praktis. Studi kasus dapat memberikan gambaran yang kaya tentang suatu fenomena (Baskerville et al., 2014) karena studi kasus menyelidiki suatu

fenomena dalam konteks kehidupan nyata dan berusaha memahami keunikan dan kompleksitasnya (Lin et al., 2014).

Pendekatan wawancara semi-terstruktur, Delphi, dan metode brainstorming kelompok digunakan untuk mengumpulkan data dan membangun konsensus. Metode Delphi (Woudenberg, 1991) dan metode brainstorming (Telem, 1988) direkomendasikan dalam perencanaan strategi.

Table 4 Composition of Panel of Experts

	Job title	Key responsibilities
Panel expert 1	Associate Vice-President, Information Technology Services	Oversee overall IT and Security function, Accountable to the Board
Panel expert 2	Information Security Specialist	Responsible for operational security activities, also part of tactical and strategic security activities
Panel expert 3	Director/Manager of IT Infrastructure	Responsible for key system, network administration
Panel expert 4	Manager of Client Services	Responsible for various client services including help desk and desktop services
Panel expert 5	Technical Analyst	Responsible for day-to-day operational assistance of client services

Untuk mendapatkan pandangan mereka, kami mewawancarai Associate Vice-President (AVP) layanan IT dan empat personel IT tambahan dari peran IT kunci. Personel yang diwawancarai adalah personel IT kunci atau pembuat keputusan dan profesional paling berpengetahuan dalam mengelola keamanan informasi di organisasi mereka. Perlu dicatat bahwa beberapa ahli ini, berdasarkan peran pekerjaan mereka, adalah karyawan baru universitas. Tabel 4 menyajikan jabatan dan tanggung jawab utama panel ahli

Tujuan kedua dari latihan ini adalah menggunakan tujuan tersebut sebagai dasar untuk mengidentifikasi serangkaian langkah-langkah kinerja tertentu sehingga manajer keamanan dapat menetapkan target untuk masing-masing tujuan dan membandingkan target tersebut dengan hasil aktual setelah strategi keamanan informasi diterapkan.

Penting untuk dicatat bahwa menerapkan strategi keamanan informasi organisasi membutuhkan sumber daya finansial dan non-finansial. Sumber daya tersebut terutama untuk inisiatif yang harus dilakukan untuk memastikan strategi keamanan informasi diterapkan dengan benar. Inisiatif membutuhkan waktu dan uang, dan diperlukan untuk lisensi perangkat lunak, pengembangan kemampuan firewall, perekrutan spesialis IT, pelaksanaan tes penetrasi, pelaksanaan audit jaminan keamanan IT secara berkala, program pelatihan karyawan, dan tindakan lain yang berfokus pada orang, proses, produk/teknologi, dan mitra/pemasok.

Karena inisiatif membutuhkan biaya, maka perlu untuk meyakinkan manajemen senior bahwa investasi dalam strategi keamanan informasi sangat penting. Lebih tepatnya, dengan menggunakan InfoSec BSC, organisasi secara tepat dapat membenarkan investasi tersebut. Seperti yang digambarkan dalam artikel ini, langkah pertama dalam mendesain InfoSec BSC untuk suatu organisasi adalah mengidentifikasi serangkaian tujuan keamanan informasi generik yang dapat dipahami oleh manajer senior dan kemudian mengembangkan serangkaian langkah-langkah kinerja yang spesifik untuk organisasi berdasarkan sistem IT yang ada.

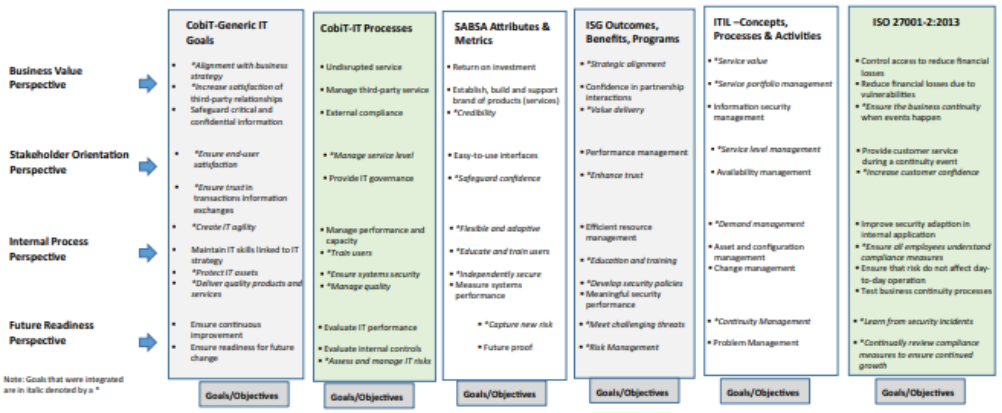


Fig. 2 High-Level Mapping of Information Security Governance and Control Frameworks to InfoSec BSC to Identify Goals and Objectives

Untuk mengilustrasikan tujuan utama kedua yaitu mengidentifikasi serangkaian langkah-langkah kinerja spesifik untuk tujuan InfoSec BSC, kelima kerangka kerja kontrol dan tata kelola diintegrasikan pada sesi perencanaan strategi keamanan informasi aktual di NAU. Pertemuan ketiga adalah untuk sesi brainstorming dengan panel ahli untuk mengidentifikasi inisiatif keamanan informasi dan langkah-langkah kinerja yang terkait dengan tujuan InfoSec BSC dan untuk menetapkan target untuk setiap langkah kinerja.

Tujuan keamanan informasi generik berdasarkan pemetaan konvergensi dari kelima kerangka kerja kontrol dan tata kelola keamanan IT telah dikembangkan. Ini kemudian digunakan untuk membahas dan mengidentifikasi potensi inisiatif keamanan informasi, langkah-langkah kinerja, dan target untuk setiap tujuan .Tabel 5 menyajikan contoh langkah-langkah kinerja dan inisiatif yang teridentifikasi.

Mempertimbangkan persyaratan keamanan informasi untuk sub-unit seperti unit akademis dan unit administrasi yang bervariasi dan mungkin tidak tercakup secara detail dalam InfoSec BSC tingkat tinggi yang diusulkan, beberapa narasumber menyarankan kemungkinan penggunaan beberapa scorecard. Di organisasi yang diteliti, kelompok IT terbilang kohesif (padu).

Dalam proses pengembangan balanced scorecard, banyak tantangan yang dapat muncul seperti:

- Mengidentifikasi tujuan,
- langkah-langkah kinerja,
- inisiatif,
- target, dan
- memasukkan manfaat yang dirasakan dari InfoSec BSC untuk menerapkan strategi keamanan informasi TI.

Beberapa tantangan yang disebutkan dalam diskusi terkait manajemen TI dan keamanan informasi adalah:

- **Kekurangan SDM**

  Kelangkaan keterampilan TI, khususnya keamanan informasi, terus memengaruhi bisnis di wilayah dan nasional. Salah satu kutipan dari narasumber, "Kami akhirnya menemukan spesialis keamanan setelah

bertahun-tahun mencari" adalah bukti nyata dari realitas praktis kelangkaan SDM ini. Bukti anekdot dari diskusi kelompok CIO regional mengungkapkan kesulitan yang sama. Media populer juga berulang kali melaporkan kelangkaan tersebut secara nasional (Ireton, 2016).

- **Integrasi Teknologi Baru**
  Setiap tahun, inovasi membuat perangkat lunak perlu ditingkatkan atau bahkan diganti. Saat ini, manajer harus menggunakan sistem baru termasuk sistem keamanan sambil memastikan mereka menyediakan apa yang dibutuhkan karyawan agar produktif.
- **Kompleksitas Platform**
  Untuk beberapa platform seperti modul ERP atau sistem manajemen kursus yang memengaruhi banyak pengguna akhir, kompleksitas menjadi masalah utama. Selain itu, keamanan tidak dapat dianggap dan ditangani secara terpisah-pisah tetapi harus dipertimbangkan dari pandangan holistik tentang penyediaan layanan teknologi. Salah satu contoh anekdotnya adalah perubahan selama tahun lalu. Selama penguncian COVID, grup IT perlu menunjukkan kemampuan untuk mengakomodasi permintaan baru dengan cepat dan mengubah mode/platform untuk mendukung cara baru dalam mengajar, belajar, melakukan penelitian, dan bekerja.
- **Solusi dan Kontrol Komputasi Baru**
  Dengan banyak solusi, seperti penggunaan layanan cloud, universitas harus bergantung pada penyedia layanan eksternal. Dalam acara tersebut, Anda tidak memiliki kendali penuh atas manajemen keamanan dan privasi dan harus bergantung pada perjanjian level layanan (SLA).
- **Prioritas Proyek yang Bersaing**
  Seperti di organisasi besar lainnya, grup IT dan grup keamanan informasi bersaing untuk mendapatkan sumber daya yang terbatas. Beberapa solusi teknologi keamanan dicatat membutuhkan waktu bertahun-tahun untuk mendapatkan persetujuan anggaran dan sumber daya yang dibutuhkan.
- **Pengenalan Teknologi/Inisiatif Keamanan dan Manajemen Perubahan**
  Pengenalan teknologi dan inisiatif keamanan baru tidak pernah mudah. Pengenalan autentikasi multifaktor baru-baru ini membutuhkan upaya substansial untuk orientasi grup pengguna akhir yang berbeda.
- **Kepuasan Pengguna**
  Kepuasan pengguna akhir disebutkan dalam beberapa aspek diskusi yang berbeda. Di universitas, survei kepuasan pengguna akhir dari berbagai kelompok pemangku kepentingan seperti fakultas, staf, atau mahasiswa dilakukan secara berkala untuk mengetahui persepsi

pengguna akhir. Informasi ini digunakan untuk meningkatkan layanan IT.

- **Memperluas Perimetri Keamanan**
  Pengguna akhir, baik mahasiswa, staf, atau fakultas, tidak lagi hanya menggunakan satu komputer khusus di meja di ruang kantor atau lab yang dikelola. Hampir semua menggunakan banyak perangkat seperti laptop, tablet, ponsel, dll. dari jaringan rumah atau jaringan publik, yang membawa tantangan dalam memberikan dukungan tanpa risiko keamanan.
- **Lingkungan Ancaman Dinamis dan Mengimbangi**
  Di atas semua kesulitan yang disebutkan di atas, yang memperumit gambaran tersebut adalah ancaman yang sama sekali baru mengejutkan semua orang. Serangan ransomware yang membatasi beberapa universitas pada 2018-2019 (McGinn, 2017; McKenzie, 2021) adalah contoh utama dari lingkungan ancaman yang dinamis.Memerlukan upaya berkelanjutan untuk mengintegrasikan strategi kesadaran agar pengguna akhir lebih terinformasi, kebijakan dan prosedur yang sesuai, serta teknologi keamanan untuk mengurangi beban pengguna akhir. Pelatihan personel IT dan keamanan informasi untuk mengikuti kemajuan juga disebutkan dalam sesi tersebut.

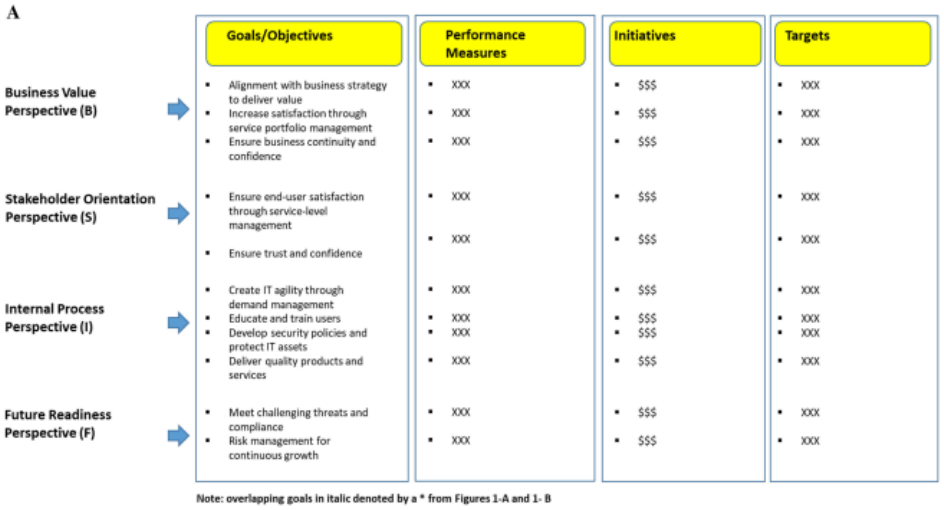


Fig. 3 Generic InfoSec BSC for Implementing Information Security Strategy at a University

B

BSC Perspective	Goals/Objectives	Performance Measures	Initiatives	Targets*
Business Value Perspective (BV)	BV1: Alignment with business strategy to deliver value	# of service-level agreements % savings in IT security cost due to cloud-based services such as ORION # of in-house-developed security tools % of open source software use to total software use	Using open source, consortium, and collaborative software strategies and strategic partnerships with other universities ($XXX)	
	BV2: Increase satisfaction through service portfolio management	# of IT Tickets % stakeholders who are satisfied Average response time in minutes	Expand service catalogue and service portfolio ($XXX) Conduct stakeholder satisfaction surveys ($XXX)	
	BV3: Ensure business continuity and confidence	# of IT system lockdowns Response time in minutes from detection to lockdown	Information security incidence response ($XXX)	
Stakeholder Orientation Perspective (SO)	SO1: Ensure end-user satisfaction through service-level management	# of positive stakeholder responses # of IT tickets handled Average response time in minutes	Conduct stakeholder satisfaction surveys ($XXX) Design and review service offerings ($XXX)	
	SO2: Ensure trust and confidence	# of internal spot audits # of penetration tests # of security patch installations # of times scanning filters are enabled	Planned and proactive security management ($XXX)	
Internal Process Perspective (IP)	IP1: Create IT agility through demand management	# of portable IT security devices (campus store in mall having firewall protection)	Provide agility through cloud computing infrastructure ($XXX)	
	IP2: Educate and train users	# of issues covered (mobile computing , IoT, traditional IS measures) # of workshops/training offered to stakeholders # of faculty and staff attended # of departments visited by IT security training staff	Information security awareness month (workshops, poster competitions, information security quizzes) ($XXX) Security blogs to inform and educate stakeholders ($XXX)	
	IP3: Develop security policies and protect IT assets	# number of intrusions # of false negatives	Establishment of a university-wide information security policy ($XXX) Install IDS ($XXX)	
	IP4: Deliver quality products and services	# of internal spot audits # of penetration tests # of security patch installations # reach and attack simulation # of times scanning filters are enabled	Periodic security testing and review ($XXX) Establish best practice guidelines ($XXX)	
Future Readiness Perspective (FR)	FR1: Meet challenging threats and compliance	# training workshops offered to IT security staff # of penetration tests # of advanced persistent threats (APTs)	Learning and self-awareness training for IT security staff ($XXX)	
	FR2: Risk management for continuous growth	% of IT migrated to Cloud % assets insured	Cloud initiative-IDS capacity planning for growth and risk management ($XXX) Information security insurance strategies ($XXX)	

6. Diskusi

InfoSec BSC membantu menyelaraskan strategi keamanan informasi dengan strategi bisnis. Sebuah organisasi tidak boleh hanya fokus pada satu perspektif tetapi menunjukkan bagaimana strategi keamanan informasi mempengaruhi organisasi internal dan pihak eksternal ke pelanggan, regulator, pemasok, dan lainnya. Karena organisasi berbeda, tujuan dan ukuran kinerja InfoSec BSC harus disempurnakan dan ditafsirkan dalam konteks kebutuhan individu organisasi mereka sendiri. Jadi InfoSec BSC harus diadaptasi sesuai kebutuhan organisasi.

Organisasi yang mengadopsi praktik keamanan informasi yang baik dapat memperoleh manfaat dari sistem IT yang berkualitas. Selain itu, manfaat lain dari

mengadopsi praktik keamanan informasi yang baik adalah meningkatkan koordinasi dan komunikasi dalam organisasi, mengurangi duplikasi dan kompleksitas kerangka kerja tata kelola, meningkatkan kesadaran tentang keamanan informasi, mengurangi biaya IT dan meningkatkan kepercayaan dan pendapatan bisnis. Praktik terbaik IT adalah praktik yang telah terbukti berhasil dan terbukti efektif. Praktik terbaik IT dapat berasal dari berbagai sumber, termasuk kerangka kerja tata kelola dan kontrol IT seperti COBIT, SABSA, ISG, ITIL, dan ISO 27000, dan dari pengetahuan individu dan organisasi.

Organisasi mungkin harus mengikuti kerangka kerja yang direkomendasikan ini untuk alasan kepatuhan (Bachlechner et al., 2014; Chen & Benusa, 2017; Herath & Herath, 2014; Hohan et al., 2015) atau untuk mencapai 'kehati-hatian' 'uji tuntas' (Rastogi & von Solms, 2005). Namun, mereka bisa beragam dan bervariasi. Dalam hal itu, kami menunjukkan bahwa InfoSec BSC dapat menjadi alat yang berguna yang dapat membantu memanfaatkan praktik terbaik dari beberapa kerangka kerja kontrol dan tata kelola dengan mengintegrasikannya ke dalam balanced scorecard keamanan informasi tingkat tinggi.

Table 5 (continued)

BSC Perspective	Goals/Objectives	Performance Measures	Initiatives	Targets*
Future Readiness Perspective (FR)	FR1: Meet challenging threats and compliance	# training workshops offered to IT security staff	Learning and self-awareness training for IT security staff ($XXX)	
		# of penetration tests		
		# of advanced persistent threats (APTs)		
	FR2: Risk management for continuous growth			
	% of IT migrated to Cloud	Cloud initiative-IDS capacity planning for growth and risk management ($XXX)		
		% assets insured	Information security insurance strategies ($XXX)	

*Note: For confidentiality reasons, the cost of initiatives and targets are not listed

BSC menjadi salah satu alat tata kelola yang paling banyak digunakan dan dipahami dalam manajemen di seluruh dunia (Hasan & Chyi, 2017), InfoSec BSC dapat menjadi alat yang berguna untuk mengimplementasikan strategi keamanan informasi organisasi, meningkatkan koordinasi dan komunikasi dalam organisasi untuk menyediakan layanan IT yang berkualitas. Karena scorecard harus unik untuk memenuhi kebutuhan organisasi, proses yang dijelaskan dalam artikel ini dapat membantu manajer keamanan untuk melakukan aktivitas serupa untuk mengembangkan scorecard mereka sendiri.

InfoSec BSC tingkat tinggi adalah kerangka kerja yang cukup inklusif untuk tata kelola keamanan informasi karena memetakan beberapa kerangka kerja tata kelola dan kontrol yang dapat digunakan oleh manajer senior untuk mengimplementasikan strategi keamanan informasi dan mengukur kinerja. Dengan

menyederhanakan beberapa kerangka kerja tata kelola dan kontrol, banyak duplikasi, tumpang tindih, dan kompleksitas berkurang yang merupakan salah satu kelemahan utama ketika mencoba mengintegrasikan beberapa kerangka kerja ke praktik keamanan informasi dalam organisasi.

6.1. Avenues for Future Research

Penelitian eksploratif dan awal kami ini memiliki beberapa keterbatasan yang menjadi dasar untuk penelitian selanjutnya. Dalam penelitian ini kami menggunakan lima kerangka kerja yang dipilih, yaitu COBIT, SABSA, ISG, ITIL, dan ISO 27000, untuk dipetakan ke InfoSec BSC. Kami menggunakan kerangka ISMP NIST untuk memandu pengembangan InfoSec BSC. Namun banyak kerangka kerja lain, termasuk yang terkemuka seperti kerangka kontrol NIST, tidak dipertimbangkan dalam penelitian ini. Kerangka kerja terkemuka atau relevan lainnya dapat digunakan dalam pengembangan InfoSec BSC.

Keterbatasan lainnya mungkin terkait dengan tempat dan narasumber yang dipilih dalam studi kasus. Kasus yang digunakan dalam penelitian ini hanya melibatkan satu organisasi di sektor pendidikan tinggi. Kegiatan serupa dapat dilakukan pada industri yang berbeda atau beberapa organisasi yang dapat menjelaskan penerapan serta tantangan adaptasi InfoSec BSC untuk manajemen dan tata kelola keamanan informasi.

7. Kesimpulan

Kepatuhan keamanan informasi membutuhkan uji tuntas dari setiap individu dalam sebuah organisasi. Pengembangan dan implementasi program pengukuran keamanan informasi biasanya merupakan tugas yang berkelanjutan, yang memerlukan pembelajaran dan peningkatan terus-menerus. Jika program pengukuran keamanan informasi diterapkan dengan benar, baik manfaat nyata maupun tidak nyata dari penerapan InfoSec BSC dapat meningkat nilainya seiring berjalannya waktu. Manajer keamanan IT mungkin harus menunjukkan bahwa kinerja keamanan informasi selaras dengan tujuan strategis organisasi dan sesuai dengan berbagai persyaratan kepatuhan.

Balanced scorecard adalah alat tata kelola manajemen yang banyak digunakan dan dapat dengan mudah dipahami oleh manajer senior. Artikel ini membahas pengembangan program pengukuran keamanan informasi menggunakan konsep balanced scorecard yang memungkinkan integrasi praktik terbaik yang relevan. Lebih khusus lagi, artikel ini memetakan lima kerangka kerja tata kelola dan kontrol (COBIT, SABSA, ISG, ITIL, dan ISO 27000) dan menggambarkan fitur-fitur kritis dalam pengembangan program pengukuran keamanan informasi menggunakan konsep BSC.