JURNAL SITEKNIK
Sistem Informasi, Teknik dan Teknologi Terapan
Volume 1, No.2, Juni 2024, hal. 76-89
E-ISSN: 3032-3991 | P-ISSN: xxxx.xxxx

Analisis Jaminan Kualitas Sistem Keamanan Siber pada Sistem Informasi : sebuah Studi Literatur

Nenden Eva[1]✉, Rahma Karina[2], Septiya Mutiara[3], RD. Rohmat Saedudin[4]

[1] S2 Sistem Informasi, Rekayasa Industri, Universitas Telkom, Indonesia
[2] S2 Sistem Informasi, Rekayasa Industri, Universitas Telkom, Indonesia
[3] S2 Sistem Informasi, Rekayasa Industri, Universitas Telkom, Indonesia
[4,] Rekayasa Industri, Universitas Telkom, Indonesia

Abstrak

Perkembangan teknologi informasi saat ini yang semakin pesat, diiringi dengan serangan siber yang semakin marak terjadi pada sektor publik atau pemerintahan. Serangan tersebut mengakibatkan sejumlah kerugian materi maupun kerusakan infrastruktur atau informasi suatu organisasi, untuk mencegah ancaman siber tersebut, dibutuhkan penjaminan kualitas untuk melindungi informasi dengan melakukan penjagaan terhadap data agar tidak mudah diakses oleh orang yang tidak berkepentingan atau informasi yang disimpan masih terjaga keaslian dan kerahasiaannya. Penjagaan serangan siber dilakukan dengan menggunakan arsitektur TISA (Trust Information Security Architecture) yang terdiri dari tahapan perlindungan data, aturan keamanan informasi, dan prosedur keamanan. Penerapan arsitektur tersebut diselaraskan dengan kriteria kualitas pada sistem untuk menjamin keamanan yang baik berdasarkan framework penjaminan keamanan yang disesuaikan dengan permasalahan keamanan yang terjadi.

Abstract

Abstract written in Indonesian or English with Times New Roman typeface, font size 10 pt, space 1 (single), one column, left and right margins protruding 10 mm from the main margin limit. If the manuscript is in English, the abstract must be translated into Indonesian. The content of the abstract consists of important points from the background, research objectives, methods used, as well as research results. The number of words in the abstract is at least 100 words and a maximum of 150 words.

Riwayat Artikel :	**Kata Kunci :**	***Keywords:***
Diserahkan : 01-06-2024 Direvisi :06-06-2024 Diterima :11-06-2024	Analisis, Jaminan, Kualitas, Keamanan, Siber,	*Analysis, Assurance, Quality, Security, Cyber,.*

Corresponding Author :
Nenden Eva
S2 Sistem Informasi, Rekayasa Industri, Universitas Telkom, Indonesia
Jl. Telekomunikasi. 1, Terusan Buahbatu - Bojongsoang, Telkom University, Sukapura, Kec. Dayeuhkolot, Kabupaten Bandung, Jawa Barat 40257
Email : nendeneva@gmail.com

PENDAHULUAN

Perkembangan teknologi saat ini dalam berbagai bidang seperti bidang sosial, data, infrastruktur teknologi semakin cepat dan masif. Tujuan perkembangan teknologi tersebut untuk meningkatkan efisiensi dan produktifitas pada perusahaan atau organisasi. Akan tetapi, dalam penerapan digitalisasi dalam suatu organisasi tersebut, sering kali terjadi kejahatan siber yang bertujuan untuk merusak data atau mencuri informasi, yang menyebabkan kerugian materi dan kerusakan infrastruktur teknologi informasi (Radicic & Petković, 2023). Berdasarkan artikel yang ditulis oleh Nivedita pada Web GetAstra, kejadian tentang kejahatan keamanan terjadi sebanyak dua ribu dua ratus serangan per hari dengan kerugian sebesar sembilan koma empat puluh empat miliar dolar, dengan kejahatan berupa serangan ransomware dan pencurian dana(Nivedita James, 2023). Terdapat beberapa kategori serangan siber lain di negara Amerika Serikat pada tahun 2021,

yaitu dengan kasus tertinggi penipuan, dan faktor lain yang terdiri dari pembelanjaan daring, hadiah dan lotre, pelayanan internet, lowongan pekerjaan, layanan telepon, kesehatan, investasi keuangan, travel dan hiburan, serta pemalsuan check(Md Haris Uddin Sharif & Mehmood Ali Mohammed, 2022). Dengan adanya berbagai tindak kejahatan siber, diperlukan suatu penjaminan kualitas dalam keamanan sistem informasi, agar data dan informasi terjaga kerahasiaan dan integritasnya.

Jaminan keamanan informasi dilakukan agar sistem dapat terhindar dari ancaman keamanan dan memenuhi persyaratan keamanan, dengan melakukan analisis terhadap kerentanan, uji penetrasi, audit dan penentuan skor(Shukla et al., 2022). Subyek utama dari perlindungan informasi bagi keamanan informasi yaitu informasi dan sistem informasi, sedangkan jaminan keamanan merupakan bisnis secara keseluruhan(Cherdantseva & Hilton, 2013). Oleh sebab itu, keamanan informasi harus berdasarkan atau selaras dengan tujuan strategis suatu organisasi. Penjaminan strategis tersebut dilakukan dengan melakukan analisis pada struktur jaringan, penentuan dan pengolahan data, manajemen akses yang tidak sah, serta manajemen risiko dari serangan siber. Untuk melakukan penanggulangan serangan, dapat dilakukan dengan beberapa jenis kerangka kerja untuk menjamin keamanan informasi perusahaan.

STUDI DAN KEBUTUHAN TERKAIT PENELITIAN

Jaminan keamanan informasi dilakukan untuk memastikan sistem yang digunakan aman dan terhindar dari serangan siber yang terjadi. Serangan siber tersebut dapat dicegah dengan melakukan sistem security quality assurance. Menurut Ankur, Basel, Livinus, Prosper, dan Goitom memberikan definisi jaminan kualitas keamanan yaitu memastikan sistem memenuhi persyaratan keamanan dan terhindar dari kerentanan(Shukla et al., 2022). Pada saat ini, hanya tersedia sedikit penelitian yang menjelaskan studi literatur tentang kualitas keamanan informasi. Penelitian mengenai kualitas keamanan menurut ahli harus memuat beberapa hal penting.

Menurut Guo (Choi & Yoo, 2009; Guo, 2013)yaitu membahas tentang pengembangan konsep dan kebiasaan untuk keamanan dengan konsep yang berbeda berdasarkan kebiasaan. Menurut choi dan yoo(Choi & Yoo, 2009) yaitu terdiri dari kualitas sistem dan ancaman keamanan yang berkaitan dengan perangkat. Menurut Bijani dan Robertson (Bijani & Robertson, 2014)yaitu jika melakukan studi literatur maka harus menjelaskan tentang teknik untuk menghindari serangan siber. Sedangkan menurut Oueslati harus melakukan identifikasi isu yang terjadi tentang keamanan.

Pada studi literatur yang akan dilakukan tentang menentukan kualitas dari perangkat lunak, kriteria, metode, persyaratan dan *kerangka kerja* dalam penjaminan kualitas keamanan. Akan tetapi, dalam penelitian ini tidak menjelaskan karakteristik keamanan pada suatu sistem dan hanya menjelaskan secara umum. Dalam hal tersebut, jurnal ini memiliki kekurangan tentang kualitas keamanan yang spesifik terhadap sistem informasi.

METODE PENELITIAN

Penelitian ini menggunakan beberapa pendekatan dalam melakukan tinjauan studi literatur mengenai kualitas sistem keamanan data. Tahap awal yaitu melakukan pengumpulan jurnal yang berkaitan dengan penelitian tentang jaminan kualitas keamanan. Tujuan pengumpulan jurnal tersebut yaitu untuk mengetahui hal – hal yang harus diperhatikan tentang kualitas keamanan, yang harus dipatuhi atau terpenuhi untuk menjamin keamanan suatu sistem.

Tahap selanjutnya yaitu penelitian harus memenuhi pertanyaan penelitian yang terdiri dari:

1. Apa saja fungsi dari jaminan keamanan informasi?
2. Aspek apa saja yang harus terpenuhi untuk menjamin keamanan komputer?
3. Bagaimana sistem dapat dikatakan berkualitas?
4. Apa saja kriteria yang harus dipenuhi untuk menjamin kualitas keamanan?
5. Pada kualitas keamanan terdapat ancaman yang dapat mengganggu sistem dan bagaimana cara untuk identifikasi risiko keamanan siber tersebut?

6. Persyaratan keamanan apa saja yang harus terpenuhi di dalam sistem?
7. Metode apa saja untuk menjamin keamanan suatu sistem?
8. Kerangka kerja apa saja yang dapat digunakan untuk menjamin kualitas keamanan suatu sistem dan bagaimana implementasi kualitas keamanan tersebut?

Setelah menentukan hal – hal yang harus ada di dalam penelitian tentang kualitas keamanan, maka peneliti melakukan seleksi jurnal untuk studi literatur antara tahun 2000-2022. Jurnal yang dibahas hanya berfokus pada pertanyaan penelitian tentang keamanan siber dan kualitas keamanan sistem. Setelah melakukan pengumpulan jurnal, peneliti melakukan penyeleksian jurnal yang sesuai dengan pertanyaan penelitian. Hasil akhir yaitu berupa studi literatur tentang kualitas keamanan yang sistematis.

HASIL DAN PEMBAHASAN

Jaminan Keamanan Informasi

Keamanan informasi sangat penting karena informasi dapat memiliki nilai dan kepentingan yang tinggi bagi suatu organisasi atau individu. Keamanan informasi juga diperlukan untuk melindungi informasi dari berbagai ancaman yang terjadi. Menurut Ankur, Bael, Livinus, Prosper dan Goitom, jaminan keamanan informasi yaitu sistem dapat terhindar dari ancaman keamanan dan memenuhi persyaratan keamanan dengan menentukan persyaratan keamanan, melakukan analisis terhadap kerentanan, uji penetrasi, audit dan penentuan skor. Tipe jaminan keamanan dapat berupa operasi, keberlangsungan, optimal, kegunaan, orientasi layanan, dan level inti(Shukla et al., 2022). Fungsi jaminan informasi menurut Raiganj, Bhuimali, Sreeramana, Rajesh,(Paul et al., n.d.) yaitu:

1. Informasi harus tersedia untuk pengguna yang tepat dan terhindar dari pengguna yang tidak memiliki hak akses.
2. Melindungi privasi, jaringan, infrastruktur dan memastikan teknologi aman.
3. Strategi manajemen risiko penanggulangan serangan.

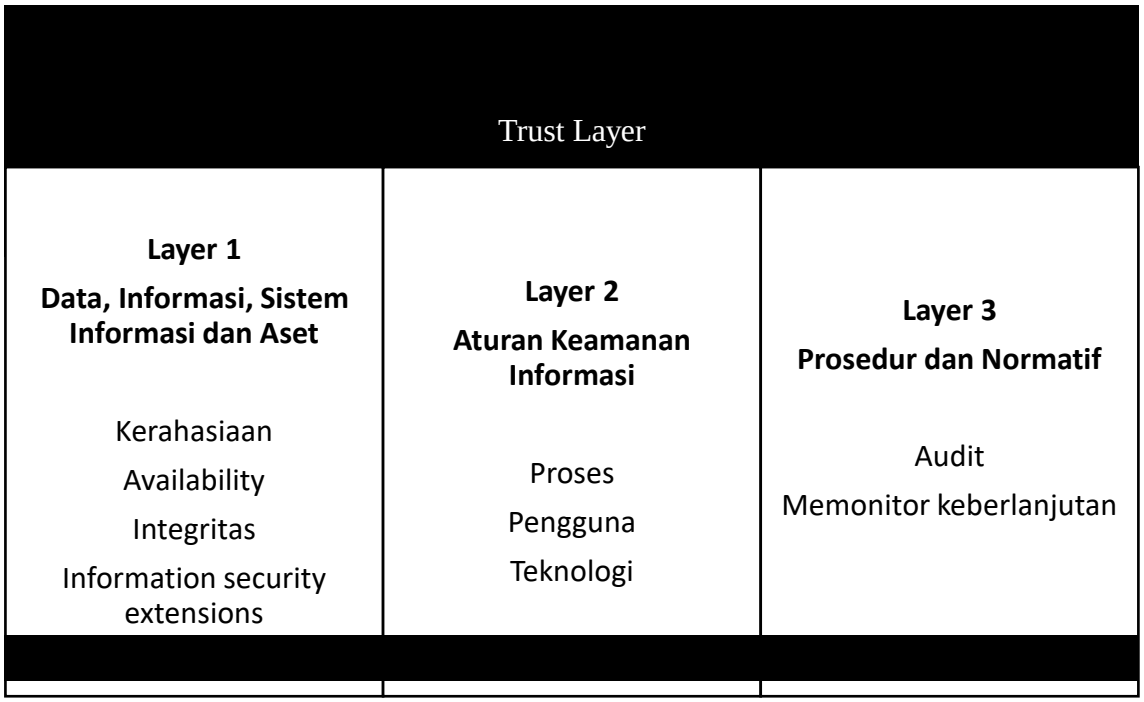
Jaminan keamanan informasi dan keamanan informasi menurut Yulia dan Jeremy (Cherdantseva & Hilton, 2013)memiliki perbedaan, yaitu:

1. Subyek utama dari perlindungan informasi bagi keamanan informasi yaitu informasi dan sistem informasi, sedangkan jaminan keamanan merupakan bisnis secara keseluruhan.
2. Tujuan utama dari perlindungan informasi yaitu ketersediaan (otentik, dapat diperhitungkan, tidak repudasi dan ketersediaan ketika informasi dibutuhkan), rahasia dan integritas, sedangkan jaminan informasi adalah perlindungan terhadap bisnis secara menyeluruh.
3. Tujuan utama untuk perlindungan informasi yaitu aspek teknis, pengguna, sedangkan jaminan keamanan meliputi perlindungan secara menyeluruh.
4. Fungsi utama dalam bisnis untuk perlindungan informasi yaitu sebagai bagian pendukung, sedangkan untuk jaminan keamanan merupakan fungsi utama.
5. Anggota organisasi yang bertanggung jawab untuk keamanan informasi yaitu teknis, sedangkan jaminan informasi secara menyeluruh.
6. Alur dari keputusan keamanan untuk jaminan informasi yaitu berdasarkan tim teknis yang berpengalaman, lalu merekomendasikan ke manajemen puncak, sedangkan untuk jaminan keamanan

Arsitektur Keamanan Informasi

Robson, Luis, Ana dan Fabio(de Oliveira Albuquerque et al., 2014), mengembangkan arsitektur keamanan informasi untuk mempertimbangkan seluruh aspek keamanan yang bernama TISA

(*Trust Information Security Architecture*) yang terdiri dari tiga layer. Berikut ini merupakan sebuah ilustrasi untuk diagram TISA terdapat pada Gambar 1.



Gambar 1. TISA (Trust Information Security Architecture)

Layer pertama yaitu tentang data, informasi, sistem informasi dan aset yang terdiri dari kerahasiaan, keamanan, integritas, dan tambahan keamanan infromasi. Layer kedua yaitu aturan tentang keamanan informasi yang terdiri dari proses, orang dan teknologi. Layer terakhir yaitu prosedur dan normatif yang terdiri dari audit, dan monitor terus menerus.

Data, Informasi, Sistem Informasi dan Aset

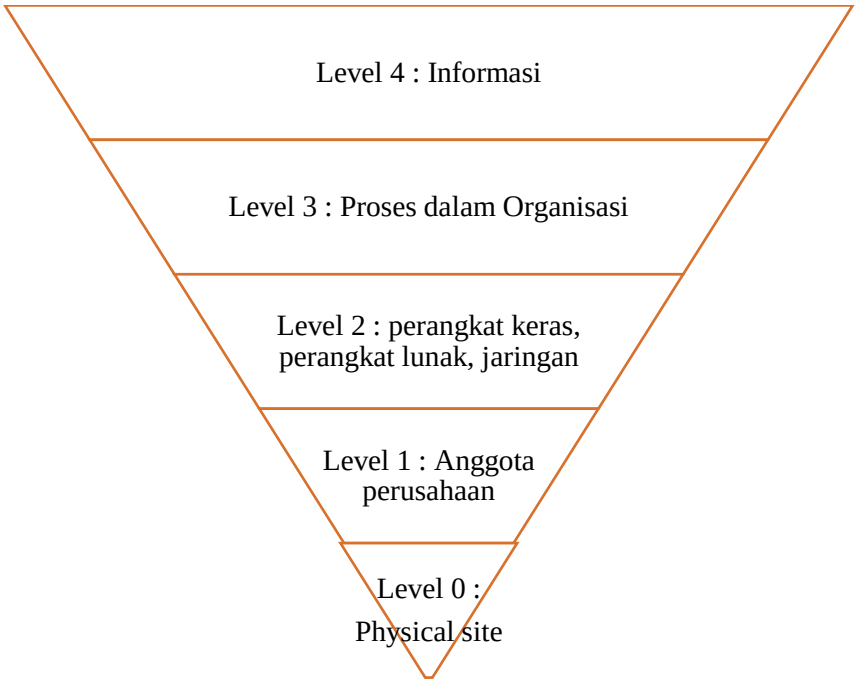
Berikut ini merupakan faktor – faktornya, yaitu:

1. Kerahasiaan

Kerahasiaan yaitu membatasi hak akses sistem atau informasi hanya kepada pihak yang berwenang.(de Oliveira Albuquerque et al., 2014) Hak akses tersebut dapat berupa proses, pengguna dan perangkat sistem.(Cherdantseva & Hilton, 2013)

2. Ketersediaan

Ketersediaan yaitu informasi pada sebuah sistem hanya tersedia untuk pengguna yang memiliki akses kepada sistem(Cherdantseva & Hilton, 2013). Suatu informasi pada sistem tidak tersedia apabila tidak memiliki akses atau informasi tersebut dihapus(de Oliveira Albuquerque et al., 2014). Menurut Suhail (Qadir & Quadri, 2016), ketersediaan pada suatu organisasi terdiri dari 4 level yaitu level nol dengan physical site, level site anggota di dalam perusahaan, level dua yaitu perangkat keras, perangkat lunak dan jaringan. Level ketiga yaitu proses dalam organisasi, dan level keempat atau level terakhir yaitu informasi.



Gambar 2. Level Ketersediaan didalam Organisasi.

3. Integritas

Integritas yaitu menjamin informasi yang terdapat didalam sistem akurat dan konsisten, dan tidak dapat diubah oleh pihak yang berwenang(de Oliveira Albuquerque et al., 2014).

4. Keamanan tambahan

Pada ekstensi keamanan informasi terdiri dari otentik (data harus ter verifikasi), kontrol akses (pembatasan hak akses), non-repudasi (pencegahan penyangkalan terhadap keaslian suatu informasi yang telah diserahkan sebelumnya), keaslian (validasi informasi yang diberikan), anonimitas (seseorang yang tidak bisa ditelusuri dan dapat berinteraksi dengan pihak lain), dan otorisasi (pemberian hak akses)(de Oliveira Albuquerque et al., 2014).

Aturan Keamanan Informasi

Berikut ini merupakan faktor – faktornya(de Oliveira Albuquerque et al., 2014), yaitu:

1. Proses yaitu tata cara untuk melakukan identifikasi dan pengelolaan risiko keamanan, dan harus terkait dengan persyaratan bisnis, dengan melakukan pertimbangan terhadap perubahan persyaratan yang dilakukan di masa depan.
2. Pengguna, yaitu cara pengguna mengamankan dan memelihara sistem, serta menentukan teknologi yang harus digunakan.
3. Teknologi merupakan aspek teknis dalam sistem seperti infrastruktur informasi, aplikasi dan mekanisme pertahanan untuk menghindari serangan.

Prosedur dan Normatif

Berikut ini merupakan faktor – faktornya,(de Oliveira Albuquerque et al., 2014) yaitu:

1. Audit, yaitu proses untuk penilaian keamanan informasi yang terdiri dari kriteria tertentu dengan penilaian yang bersifat kualitatif dan kuantitatif.
2. Memonitor keberlanjutan yaitu pemantauan pada keamanan teknologi yang sedang berlangsung, tata cara proses pengamanan, prosedur yang digunakan dan pengetahuan keamanan bagi pengguna sistem.

Definisi Kualitas Perangkat Lunak

Kualitas perangkat menurut Ming, yaitu suatu proses untuk melakukan evaluasi dan mendokumentasikan kualitas dari aplikasi pada setiap pengembangan aplikasi, berdasarkan

standar yang telah ditetapkan pada aplikasi tersebu(Lee, 2014)t. berikut ini manfaat penjaminan kualitas dalam aplikasi menurut Kishu, yaitu:

1. Loyalitas pelanggan
2. Mengurangi pengulangan pekerjaan akibat dari sistem yang tidak sesuai dengan kriteria
3. Proses yang sesuai akan menghasilkan aplikasi yang baik
4. Meningkatkan pengetahuan karyawan tentang peraturan dan tujuan bisnis perusahaan
5. Efisiensi didalam perusahaan.

Kriteria Kualitas Jaminan Keamanan

Kriteria dalam kualitas Jaminan Keamanan berbeda - beda antara setiap individu atau suatu organisasi, tetapi terdapat kategori umum yang sering digunakan. Kriteria yang digunakan, yaitu operasional, keberlanjutan, optimal, kegunaan, layanan oriental dan level inti dari keamanan(Shukla et al., 2022). Masing - masing faktor tersebut mempunyai definisi atau standar yang harus dipatuhi, yaitu:

1. Operasional dalam keamanan yaitu dengan mekanisme perlindungan kripto serta kontrol akses untuk melindungi perangkat keras dan perangkat lunak Perlindungan tersebut harus selalu dipantau untuk satu siklus hidup ase dengan melakukan pengelolaan, pengubahan dan manajemen patch yang aman dengan firewalls, sandboxing dan manajemen patch(Al-Kasasbeh, 2022).
2. Keberlanjutan, yaitu memastikan perencanaan untuk masa dean secara keberlanjutan melaui *Redundant Array of Inexpensive Disks* (RAID) dan *Service Level Agreements*(Conrad et al., 2023).
3. Optimal yaitu dengan memperhatikan faktor kerahasiaan dan ketersediaan serta sistem harus terhindar dari masalah integritas(Ioannidis et al., 2012).
4. Kegunaan, yaitu dengan memperhatikan pengguna yang akan menggunakan sistem informasi, permasalahan yang terjadi yaitu kata sandi, tanda tangan digital dan pengukuran biometrik(Schultz et al., 2001).
5. Service oriented yaitu ditingkatkan dengan melakukan interoperabilitas, usabilitas dan fleksibilitas, salah satunya dengan menggunakan metode SiSOA dengan mengalaisis tingkat arsitektur yang dipadukan dengan basis pengetahuan.(Jung et al., 2011)
6. Level inti dari keamanan, yaitu tentang kepatuhan dan fungsionalitas keamanan yang diharapkan.

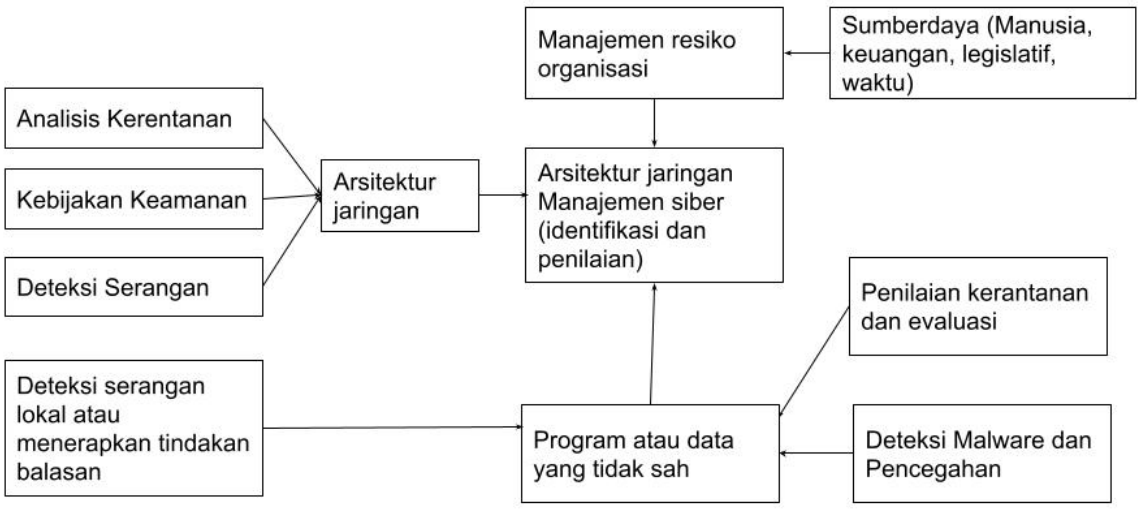
Siklus Security Development Lifecycle

Pada model siklus keamanan terdiri dai tahap persyaratan, desain, implementasi, verifikasi, dan pelepasan.(Kalaimannan & Gupta, 2017) Berikut ini merupakan penjelasan dari masing - masing faktor tersebut, yaitu:

1. Persyaratan yaitu konsultasi antara tim produk dengan tim keamanan mengenai rekomendasi kebijakan keamanan, dalam hal ini ancaman, dan syarat keamanan dipertimbangkan.
2. Desain yaitu identifikasi syarat yang harus dipenuhi dalam keamanan.
3. Implementasi yaitu sistem dipasang dan evaluasi dilakukan untuk kemungkinan ancaman siber yang terjadi.
4. Verifikasi yaitu pengujian sistem secara beta untuk menguji keamanan.
5. Pelepasan yaitu pemeriksaan keseluruhan sistem sebelum dirilis.

Metode untuk Identifikasi Resiko Cyber

Metode untuk melakukan identifikasi resiko cyber dapat dilakukan melalui dua cara yaitu menggunakan metode teknis dan bisnis (Klapkiv & Klapkiv, 2018). Metode teknis dilakukan dengan melakukan konsolidasi risiko siber, investigasi kejadian keamanan, melakukan visualisasi dan pemantauan, transmisi ke dalam informasi digital, dan melakukan pengamanan terhadap hak akses. Sedangkan untuk metode bisnis dilakukan dengan cara melakukan kalkulasi risiko siber, melakukan peramalan untuk risiko finansial di masa depan, melakukan simulasi terhadap



kerugian yang ditimbulkan, dan melakukan identifikasi terhadap risiko siber yang tersebar. Berikut ini merupakan ilustrasi untuk pengelompokan untuk risiko siber dan penilaian.

Klustering identifikasi resiko dan aktivitas penilaian menurut Lyubov dan Yurij (2018)

Persyaratan Keamanan

Persyaratan keamanan dapat dibagi ke dalam beberapa kategori yaitu fungsional, non fungsional, positif, dan negatif (Savola, 2009). Berikut ini melupakan penjelasan dari faktor - faktor tersebut, yaitu:

1. Persyaratan fungsional yaitu hal - hal yang harus dilakukan oleh sistem dan dapat menunjukkan persyaratan sistem telah terpenuhi.
2. Persyaratan non fungsional yaitu cara perangkat lunak melakukan tugasnya.
3. Persyaratan positif yaitu sistem harus melakukan hal tertentu.
4. Persyaratan negatif yaitu memastikan sesuatu tidak terjadi yang berdampak negatif terhadap sistem.

Metode Security Quality Assurance

Metode security quality assurance digunakan untuk memastikan sistem memiliki tingkat keamanan yang sesuai dengan tujuan untuk pencegahan kerentanan yang terdapat dalam pernagkat. Terdapat beberapa metode yang dapat digunakan, yaitu:

1. Pendekatan orientasi obyek, untuk melakukan evaluasi terhadap struktur berdasarkan orientasi obyek(Xu & Lin, 2009).
2. Model sekuriti Assurance yaitu melakukan evaluasi terhadap kesiapan sistem menghadap kerentanan(Shukla et al., 2022).
3. Deteksi kerentanan dengan melakukan pengembangan pendeteksi, penilaian dan mengembangkan kode sumber menggunakan machine learning(Shukla et al., 2022).

4. Pelatihan kerentanan yaitu pembuatan pelatihan berdasarkan skenario yang sesuai dengan keamanan perusahaan.(Somarakis et al., 2022)
5. Alat security assurance, yaitu membuat, menyediakan dan mengembangkan alat untuk pengamanan sistem(Shukla et al., 2022).
6. Deteksi serangan, yaitu untuk meningkatkan akurasi terhadap serangan sistem(Sakthivel et al., 2022).
7. Memantau yaitu dengan melakukan pengecekan telekomunikasi(Ouedraogo et al., 2008).
8. Deteksi anomali yaitu dengan melakukan analisa keamanan terhadap gangguan jaringan(Wawrowski et al., 2021).

Macam - Macam Framework dalam Security Quality Assurance

Kerangka keamanan siber digunakan untuk melindungi sistem dari serangan atau ancaman siber berdasarkan suatu standar yang berlaku. Berikut ini beberapa contoh kerangka keamanan menurut Hamed(Taherdoost, 2022), yaitu:

1. COBIT

COBIT merupakan kerangka kerja yang dikembangkan oleh ISACA untuk pengembangan dan pengontrolan informasi yang sesuai untuk perlindungan aset melalui tata kelola informasi(ISACA, 2012). Pada kerangka kerja ini, terdapat beberapa hal yang harus diperhatikan dalam keamanan sistem, yaitu:

a. Peraturan keamanan, prinsip – prinsip dan kerangka kerja.
b. Proses dalam menentukan detail aktivitas yang harus dilakukan dalam keamanan secara spesifik
c. Menggambarkan struktural organisasi secara spesifik
d. Dalam kesuksesan implementasi keamanan harus memperhatikan budaya dan kebiasaan perusahaan.
e. Informasi yang spesifik digunakan untuk proses tata kelola.
f. Kapabilitas di dalam layanan harus terdapat keamanan informasi yang terkait dengan rencana strategis organisasi.
g. Kemampuan dan kompetensi pengguna dalam mengamankan sistem.

2. Seri Standar SP800

Seri Standar SP800 merupakan kerangka yang dikembangkan oleh Departemen Perdagangan Amerika Serikat atau NIST. Pada standar ini melakukan pengukuran keamanan yang terdiri dari standar dalam proses pengukuran keamanan, kualitas dan kesesuaian data, memastikan konsistensi dengan melakukan pemantauan perubahan, dan pengulangan proses(Yang Guo Ramaswamy Chandramouli et al., 2023).

3. Kerangka keamanan siber (CSF) NIST

Kerangka ini dikembangkan oleh Cybersecurity Enchancement Act (CEA) untuk melakukan pengendalian risiko keamanan dan identifikasi untuk infrastruktur. Pada standar ini terdiri dari identifikasi, perlindungan, deteksi, respons dan pemulihan, berikut ini merupakan penjelasan setiap faktor tersebut(U.S General Services Administration, 2023), yaitu:

a. Identifikasi yaitu melakukan identifikasi terhadap pengetahuan suatu organisasi tentang manajemen risiko keamanan, aset, data dan kapabilitas. Kategori dalam tahapan ini yaitu manajemen aset organisasi, ruang lingkup keamanan organisasi, sistem tata kelola, pengelolaan risiko terhadap keamanan yang terjadi dan strategi dalam menanggulangi risiko, dan risiko rantai pasok.

b. Proteksi yaitu melakukan pengembangan dan implementasi tentang standar yang aman untuk layanan infrastruktur. Kategori ini terdiri dari manajemen identitas, otentikasi dan kontrol akses, pelatihan, pengamanan terhadap data, informasi terhadap prosedur keamanan, tata cara pemeliharaan, serta proteksi teknologi.

c. Deteksi yaitu untuk melakukan pengembangan dan penerapan aktivitas untuk identifikasi terjadinya serangan siber sepeti anomali dalam sistem, deteksi dan pemantau yang secara berkelanjutan.

d. Respons yaitu untuk menanggapi kejadian keamanan siber yang terdeteksi dengan perencanaan respons, komunikasi, analisis, cara penanganan risiko, dan perbaikan.

e. Pemulihan yaitu aktivitas untuk mengambil tindakan dengan melakukan perencanaan respon, perbaikan dan komunikasi.

4. Kerangka manajemen risiko NIST (RMF)

Pada kerangka ini dilakukan dengan persiapan, kategorisasi, pemilihan dan penerapan, penilaian, pengesahan, dan pemantauan risiko privasi. Standar ini dapat dilakukan untuk penilaian IOT(Taherdoost, 2022). Berikut ini merupakan tahapan untuk manajemen keamanan infromasi(NIST, 2022), yaitu:

a. Persiapan untuk melakukan pengelolaan keamanan dan risiko privasi.

b. Kategorisasi dalam pemrosesan informasi, penyimpanan dan pendistribusian berdasarkan analisis akibat.

c. Pemilihan untuk melakukan perlindungan berbasis risiko dengan NIST SP 800-53.

d. Implementasi yaitu untuk melakukan pengontrolan implementasi.

e. Penilaian untuk melakukan kesesuaian pengontrolan, kesesuaian operasi dengan tujuan kesesuaian.

f. Hak akses yaitu manajemen tingkat atas untuk menentukan operasi sistem berdasarkan risiko.

g. Pengontrolan yaitu melakukan pengontrolan secara berkelanjutan.

5. Kerangka privasi NIST

Kerangka ini mencoba mengatasi permasalahan organisasi dengan cara pendeteksian dan penanganan masalah privasi dengan pembangunan layanan yang inovatif dengan melakukan perlindungan privasi antar individu.(NIST PRIVACY FRAMEWORK:, 2020) Pada kerangka ini terdiri dari tiga tahapan, yaitu:

a. Inti yaitu serangkaian proteksi dalam aktivitas yang memungkinkan untuk melakukan komunikasi berdasarkan prioritas yang terbagi antara kategori dan sub kategori untuk setiap fungsi.

b. Profil yaitu peninjauan kegiatan inti untuk menentukan kegiatan yang paling penting dalam bisnis, seperti peran ekosistem, jenis pemrosesan dalam data dan kebutuhan privasi dalam individu.

c. Tingkatan implementasi, yaitu tingkatan yang menjadi acuan untuk resiko privasi dan menentukan sumber daya untuk mengelola privasi tersebut.

6. NISTSP800-14

Kerangka ini bertujuan untuk perlindungan keamanan siber dari ancaman serangan didunia maya(Marianne Swanson & Barbara Guttman, 1996). Pada standar ini membahas tentang peraturan keamanan sistem, manajemen program, manajemen risiko, planning life cycle, isu personel, tata cara menghadapi permasalahan keamanan, prosedur menghadapi ancaman

keamanan, keamanan fisik, identifikasi dan otentikasi, manajemen kontrol akses, audit trail, dan kriptografi.

7. NIST SP 800-37

Standar ini digunakan dalam melakukan manajemen risiko dalam pengelolaan privasi dan tanggung jawab oleh manajemen puncak(Guide for Conducting Risk Assessments, 2012). Tujuan standar ini, yaitu:

a. Pengelolaan risiko keamanan sesuai dengan strategi bisnis organisasi.
b. Kontrol keamanan yang selaras dengan arsitektur perusahaan.
c. Menjamin keamanan yang konsisten dan berkelanjutan, transparansi dan pengelolaan risiko.
d. Sistem yang aman dengan pengelolaan risiko yang sesuai.

8. NIST SP 800-30

Pada standar ini digunakan untuk manajemen risiko berdasarkan sumber daya dan anggaran yang tersedia. Tahapan dalam prosedur ini terdiri dari penentuan risiko, penilaian, cara menghadapi risiko dan pemantauan. Pada standar ini organisasi melakukan pengontrolan tentang aktivitas untuk menghasilkan informasi yang terpercaya dan memenuhi keamanan dan privasi(NIST, 2012).

9. NIST SP 800-53

Standar ini digunakan untuk pengamanan terhadap aset, operasi dan individu dari serangan atau ancaman yang terjadi di dunia maya seperti kesalahan manusia, kegagalan infrastruktur, risiko privasi dan ancaman dari pihak lua(NIST, 2020)

10. NIST SP 800-12

Pada kerangka ini mengklasifikasikan peran keamanan dalam mendukung tujuan bisnis perusahaan dengan biaya yang hemat, akuntabilitas yang jelas, pertimbangan biaya, konsep dan hubungan antara pengontrolan keamanan yang berbeda(Nieles et al., 2017). Pada standar ini melakukan identifikasi jaminan keamanan dengan melakukan identifikasi otorisasi, teknis keamanan, jaminan operasional, interdepensi dan pertimbangan biaya yang dikeluarkan untuk menjamin keamanan.

Implementasi Security Quality Assurance Berdasarkan Standar ISO/IEC 270001

Berdasarkan kriteria dan standar ISO/IEC 27001(Ganji et al., 2019), terdapat beberapa kriteria dalam implementasi security quality assurance, yaitu:

1. Organisasi yaitu dengan mempertimbangkan permasalahan keamanan internal dan eksternal di dalam organisasi.
2. Pihak yang berkepentingan yaitu berbagai pihak yang terliat di dalam sistem informasi.
3. Ruang lingkup yaitu dengan menentukan batasan logis dan fisik.
4. Kepemimpinan yaitu komitmen manajemen puncak dalam penerapan rencana strategis organisasi.
5. Kebijakan yaitu dengan menentukan prosedur berdasarkan konteks organisasi.
6. Peran yaitu dengan tugas manajemen puncak dalam melakukan alokasi tanggung jawab dan pelaporan keamanan.
7. Risiko dan peluang yaitu menentukan risiko dan peluang yang diproyeksikan ke masa depan.
8. Tujuan keamanan informasi dengan menetapkan tujuan keamanan informasi di masa sekarang dan masa depan.

9. Sumber daya yaitu identifikasi pengguna, perangkat keras dan perangkat lunak pada keamanan sistem informasi.
10. Perencanaan operasional yaitu melakukan perencanaan, penetapan dan pengelolaan untuk memenuhi persyaratan dan tujuan keamanan.
11. Penilaian risiko keamanan untuk setiap ancaman yang terjadi.
12. Penanganan risiko terhadap ancaman.
13. Pemantau dengan melakukan evaluasi kinerja keamanan saat ini.
14. Audit internal yaitu dengan melakukan penilaian internal tentang efektivitas keamanan.
15. Tinjauan manajemen yaitu manajemen puncak melakukan penilai kesesuaian dan efektivitas tentang keamanan yang terjadi di dalam organisasi.
16. Perbaikan berkelanjutan yaitu dengan melakukan kesesuaian dan efektivitas sistem keamanan.

KESIMPULAN

Kesimpulan

Penjaminan kualitas sistem informasi yaitu dilakukan untuk menghindari pengguna yang tidak memiliki akses pada sistem, melindungi privasi, jaringan, infrastruktur dan memastikan teknologi aman, serta manajemen risiko untuk penanggulangan serangan siber. Risiko penangan an siber tersebut dilakukan dengan identifikasi keamanan menggunakan TISA (*Trust Information Security Architecture*) yang terdiri dari tiga layer. Layer pertama yaitu tentang data, informasi, sistem informasi dan aset yang terdiri dari kerahasiaan, keamanan, integritas, dan tambahan keamanan infromasi. Layer kedua yaitu aturan tentang keamanan informasi yang terdiri dari proses, orang dan teknologi. Layer terakhir yaitu prosedur dan normatif yang terdiri dari audit, dan monitor terus menerus. Setelah penentuan arsitektur perusahaan, maka dapat melakukan audit risiko keamanan informasi menggunakan kerangka kerja seperti COBIT, Kerangka keamanan siber (CSF) NIST, Kerangka manajemen risiko NIST (RMF), Kerangka privasi NIST, NISTSP800-14, NIST SP 800-37, NIST SP 800-53, dan NIST SP 800-12 Tujuan identifikasi keamanan siber tersebut digunakan untuk meningkatkan loyalitas pelanggan, mengurangi pengulangan pekerjaan akibat dari sistem yang tidak sesuai dengan kriteria, proses yang sesuai akan menghasilkan aplikasi yang baik, meningkatkan pengetahuan karyawan tentang peraturan dan tujuan bisnis perusahaan, dan efisiensi di dalam perusahaan.

REFERENSI

Al-Kasasbeh, B. (2022). Model of the information security protection subsystem operation and method of optimization of its composition. *Egyptian Informatics Journal*, *23*(3), 511–516. https://doi.org/10.1016/j.eij.2022.05.003

Bijani, S., & Robertson, D. (2014). A review of attacks and security approaches in open multi-agent systems. *Artificial Intelligence Review*, *42*(4), 607–636. https://doi.org/10.1007/s10462-012-9343-1

Cherdantseva, Y., & Hilton, J. (2013). Information security and information assurance: Discussion about the meaning, scope, and goals. In *Organizational, Legal, and Technological Dimensions of Information System Administration* (pp. 167–198). IGI Global. https://doi.org/10.4018/978-1-4666-4526-4.ch010

Choi, W., & Yoo, D. (2009). Software assurance towards better IT service. *Journal of Service Science*, *1*(1), 31–56. https://doi.org/10.1007/s12927-009-0003-1

Conrad, E., Misenar, S., & Feldman, J. (2023). Chapter 8 - Domain 7: Security Operations. In E. Conrad, S. Misenar, & J. Feldman (Eds.), *CISSP® Study Guide (Fourth Edition)* (Fourth Edition, pp. 361–457). Syngress. https://doi.org/https://doi.org/10.1016/B978-0-443-18734-6.00006-4

de Oliveira Albuquerque, R., García Villalba, L. J., Sandoval Orozco, A. L., Buiati, F., & Kim, T. H. (2014). A layered trust information security architecture. *Sensors (Switzerland)*, *14*(12), 22754–22772. https://doi.org/10.3390/s141222754

Ganji, D., Kalloniatis, C., Mouratidis, H., & Gheytassi, S. M. (2019). *Approaches to Develop and Implement ISO/IEC 27001 Standard-Information Security Management Systems: A Systematic Literature Review*. www.iaria.org

Guide for conducting risk assessments. (2012). https://doi.org/10.6028/NIST.SP.800-30r1

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. In *Computers and Security* (Vol. 32, pp. 242–251). Elsevier Ltd. https://doi.org/10.1016/j.cose.2012.10.003

Ioannidis, C., Pym, D., & Williams, J. (2012). Information security trade-offs and optimal patching policies. *European Journal of Operational Research*, *216*(2), 434–444. https://doi.org/10.1016/j.ejor.2011.05.050

ISACA. (2012). *COBIT 5 For Information Security*. ISACA.

Jung, C., Rudolph, M., & Schwarz, R. (2011). Security evaluation of service-oriented systems with an extensible knowledge base. *Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011*, 698–703. https://doi.org/10.1109/ARES.2011.109

Kalaimannan, E., & Gupta, J. N. D. (2017). The Security Development Lifecycle in the Context of Accreditation Policies and Standards. In *IEEE Security and Privacy* (Vol. 15, Issue 1, pp. 52–57). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/MSP.2017.14

Klapkiv, L., & Klapkiv, Y. (2018). METHODS FOR THE IDENTIFICATION OF CYBER RISKS: AN ANALYSIS BASED ON PATENT DATA. *CBU International Conference Proceedings*, *6*, 241–246. https://doi.org/10.12955/cbup.v6.1163

Lee, M.-C. (2014). Software Quality Factors and Software Quality Metrics to Enhance Software Quality Assurance. In *Original Research Article British Journal of Applied Science & Technology* (Vol. 4, Issue 21). www.sciencedomain.org

Marianne Swanson, & Barbara Guttman. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems* (14th ed.). U.S. GOVERNMENT PRINTING OFFICE .

Md Haris Uddin Sharif, & Mehmood Ali Mohammed. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, *15*(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security*. https://doi.org/10.6028/NIST.SP.800-12r1

NIST. (2012). *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. (2022, July 13). *NIST Risk Management Framework RMF*. July 13. https://csrc.nist.gov/Projects/risk-management

NIST PRIVACY FRAMEWORK: (2020). https://doi.org/10.6028/NIST.CSWP.01162020

Nivedita James. (2023, May 2). *160 Cybersecurity Statistics 2023 [Updated]*. Security Audit. https://www.getastra.com/blog/security-audit/cyber-security-statistics/

Ouedraogo, M., Khadraoui, D., De Remont, B., Dubois, E., & Mouratidis, H. (2008). Deployment of a Security Assurance Monitoring Framework for Telecommunication Service Infrastructures on a VoIP Service. *2008 New Technologies, Mobility and Security*, 1–5. https://doi.org/10.1109/NTMS.2008.ECP.38

Paul, P. K., Aithal, S., Profile, S., Bhuimali, A., & Rajamony, R. (n.d.). *Cyber Security to Information Assurance : An Overview Ideal Systems View project Image Analysis View project*. www.jrrset.com

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, *07*(03), 185–194. https://doi.org/10.4236/jis.2016.73014

Radicic, D., & Petković, S. (2023). Impact of digitalization on technological innovations in small and medium-sized enterprises (SMEs). *Technological Forecasting and Social Change*, *191*, 122474. https://doi.org/https://doi.org/10.1016/j.techfore.2023.122474

Sakthivel, R. K., Nagasubramanian, G., Al-Turjman, F., & Sankayya, M. (2022). Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry. *Transactions on Emerging Telecommunications Technologies*, *33*(4). https://doi.org/10.1002/ett.3947

Savola, R. M. (2009). Software security assurance of telecommunication systems. *2009 International Conference on Multimedia Computing and Systems*, 138–143. https://doi.org/10.1109/MMCS.2009.5256713

Schultz, E. E., Proctor, R. W., Lien, M.-C., & Salvendy, G. (2001). Usability and Security An Appraisal of Usability Issues in Information Security Methods. In *Computers & Security* (Vol. 20, Issue 7).

Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: A systematic literature review. In *Computer Science Review* (Vol. 45). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2022.100496

Somarakis, I., Smyrlis, M., & Fysarakis, K. (2022). *Model-driven Cyber Range Training: A Cyber Security Assurance Perspective Multi-scale Balance Hypermodel towards early diagnostic Evaluation and efficient Management plan formulation (EMBalance) (EU F7, 1/12/2013-31/1/2017) View project Holobalance View project Model-driven Cyber Range Training: A Cyber Security Assurance Perspective*. http://www.sphynx.ch

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. In *Electronics (Switzerland)* (Vol. 11, Issue 14). MDPI. https://doi.org/10.3390/electronics11142181

U.S General Services Administration. (2023). *NIST Cybersecurity Framework (CSF)*. U.S GEneral Services Administration. https://www.gsa.gov/technology/technology-products-services/it-security/nist-cybersecurity-framework-csf

Wawrowski, Ł., Michalak, M., Białas, A., Kurianowicz, R., Sikora, M., Uchroński, M., & Kajzer, A. (2021). Detecting anomalies and attacks in network traffic monitoring with classification methods and XAI-based explainability. *Procedia Computer Science*, *192*, 2259–2268. https://doi.org/https://doi.org/10.1016/j.procs.2021.08.239

Xu, C., & Lin, J. (2009). An object-oriented information system security evaluation method based on security level distinguishing model. *2009 International Conference on Web Information Systems and Mining, WISM 2009*, 497–500. https://doi.org/10.1109/WISM.2009.106

Yang Guo Ramaswamy Chandramouli, Antwan Clark, Aron Warren, Catherine Hinton, Purushotham Bangalore, Lowell Wofford, Andrew Prout Albert Reuther, Erik Deumens, Rickey Gregg Gary Key, Ryan Adamson, & Csilla Farkas. (2023). *High-Performance Computing (HPC) Security: Architecture, Threat Analysis, and Security Posture* (Gina M. Raimondo, Ed.; 223rd ed.). U.S. Department of Commerce .