**Engineering And Technology International Journal**
**Juli 2023 | Vol. 5 | No. 2**
**E-ISSN : 2714-755X**
**DOI: 10.556442**

# Penerapan Manajemen Risiko Keamanan Smartphone Menggunakan ISO/IEC 270005 Di Organisasi

**Fingki Marwati*[1]**
[1,]Sistem Informasi, Fakultas Ilmu Komputer Universitas Pamulang

e-mail : dosen02817@unpam.ac.id

***Abstrak***

*Teknologi smartphone mengalami tingkat pertumbuhan yang mencengangkan. Seperti yang umumnya dipahami, smartphone adalah alat serbaguna yang memungkinkan pengguna untuk menangani berbagai macam tugas sehari-hari dan yang berhubungan dengan pekerjaan. Namun, kemudahan ini telah menyebabkan pengabaian potensi kerentanan keamanan pada perangkat ini saat digunakan sebagai perangkat pribadi dan kantor. Kerentanan ini dapat dimanfaatkan oleh entitas jahat yang ingin mencuri informasi sensitif organisasi, yang merupakan aset penting. Seringkali, organisasi kekurangan sumber daya untuk mengelola beragam smartphone secara efisien, terutama ketika tidak ada personel tambahan yang tersedia. Meskipun smartphone memperluas jangkauan kemungkinan bisnis, risiko keamanan dan privasi harus dipertimbangkan dengan cermat.*

*Diperlukan upaya untuk memitigasi risiko yang terkait dengan penggunaan ponsel cerdas, yang memerlukan tindakan pencegahan untuk meminimalkan terjadinya risiko tersebut. Panduan untuk mengelola risiko keamanan pada telepon pintar dikembangkan dan dianalisis dalam penelitian ini. Panduan ini berkaitan dengan pengembangan dan pemanfaatan aplikasi seluler. ISO/IEC 27005 adalah metode yang digunakan untuk melakukan studi ini, dan langkah-langkah manajemen risiko diterapkan menggunakan metode ini di Lemsaneg. Dengan memanfaatkan temuan penelitian ini, diantisipasi bahwa desain sistem manajemen risiko dapat dikembangkan, yang melibatkan identifikasi dan pengukuran risiko dengan tujuan memitigasinya.*

***Kata kunci****— Smartphone, ISO/IEC 27005, Manajemen Risiko*

***Abstract***

*Smartphone technology is experiencing an astonishing rate of growth. As commonly understood, smartphones are versatile tools that enable users to handle a wide variety of everyday and work-related tasks. However, this convenience has led to neglect of potential security vulnerabilities in these devices when used as personal and office devices. This vulnerability could be exploited by malicious entities looking to steal an organization's sensitive information, which is a critical asset. Often, organizations lack the resources to efficiently manage multiple smartphones, especially when no additional personnel are available. Although smartphones expand the range of business possibilities, security and privacy risks must be carefully considered.*

*Efforts are needed to mitigate the risks associated with smartphone use, requiring precautions to minimize the occurrence of these risks. Guidelines for managing security risks on smartphones were developed and analyzed in this study. This guide deals with the development and utilization of mobile applications. ISO/IEC 27005 is the method used to carry out this study, and risk management measures are implemented using this method in Lemsaneg. By utilizing the findings of this study, it is anticipated that a risk management system design can be developed, which involves identifying and measuring risks with the aim of mitigating them.*

***Keywords****: Smartphone, ISO/IEC 27005, Risk Management*

## PENDAHULUAN

Perkembangan smartphone saat ini berkembang sangat pesat sering dengan perkembangan TIK. Menurut laporan tertulis Ericsson dari riset berjudul Ericsson Mobility, diprediksi pada tahun 2025 jumlah total pengguna perangkat mobile akan melebihi jumlah penduduk dunia. Dimana hasil riset lain yang diungkap oleh Ericsson adalah 75 persen dari semua perangkat mobile yang terjual di kuartal pertama 2023 merupakan perangkat smartphone. Namun perlu diketahui bahwa smartphone android merupakan target utama malware. FBI juga pernah mengeluarkan warning terhadap smartphone android pada tahun 2020.

Laporan Alcatel-Lucenttahun 2022 menunjukkan terdapat kenaikan serangan malware pada perangkat dan jaringan yang berisiko terhadap privasi dan tempat kerja. Laporan Motive Security Lab report (Alcatel-Lucent) menyebutkan bahwa :

- Tingkat infeksi terhadap perangkat mobile pada tahun 2020 adalah 0,68%. Berdasarkan ini Alcatel-Lucent memperkirakan bahwa di seluruh dunia, sekitar 26 juta perangkat mobile terinfeksi oleh malware.
- Malware pada perangkat mobile (smartphone) meningkat secara signifikan dengan perintah yang lebih kuat dan protokol kontrol.
- 60% perangkat yang terinfeksi malware adalah smartphone android, 40 % adalah PC Windows.
- Spyware pada smartphone, digunakan untuk memata-matai pemilik ponsel, juga meningkat. Hal tersebut digunakan untuk melacak lokasi telepon, memonitor panggilan masuk dan keluar, pesan teks, e-mail dan melacak web browsing.
- Tingkat infeksi bulanan keseluruhan di jaringan broadband tetap perumahan hanya di bawah 14%. Hal ini secara substansial meningkat 9% dari tahun 2021. Hal ini sebagian besar disebabkan peningkatan infeksi oleh iklan.
- Ancaman tingkat tinggi seperti 'bots', 'rootkit', dan 'trojan perbankan' tetap stabil di sekitar 5%

. Kaspersky security bulletin 2022 menyebutkan bahwa ledakan pertumbuhan malware pada smartphone dimulai pada tahun 2011 dan berkembang terus. Tahun 2023 dilaporkan lebih dari 248.427 modifikasi malware dalam 777 keluarga malware. Sebagian besar terfokuskan pada Android sebanyak 98,05% dari malware pada smartphone yang ditemukan tahun 2023. Platform Android banyak digunakan oleh kejahatan cyber untuk melakukan penyerangan. Dengan mudah penjahat cyber membuat aplikasi untuk perangkat android dan banyak orang dengan mudah mendownload program-program (termasuk malware) dari mana pun mereka mendownload. Selain itu terdapat aplikasi android seperti PlaceRaider yang merupakan malware canggih yang dapat merekam secara diam-diam seluruh aktivitas smartphone target dan merekontrusinya dalam bentuk grafis 3 dimensi.

Laporan-laporan global di atas secara umum menjelaskan tentang ancaman serius terhadap celah-celah yang ditimbulkan oleh smartphone. Celah-celah keamanan yang dapat digunakan musuh untuk mencuri informasi penting di dalam smartphone, dimana informasi merupakan salah suatu aset penting dan sangat berharga bagi kelangsungan hidup organisasi dan disajikan dalam berbagai format berupa : catatan, lisan, elektronik, pos, dan audio visual.

Berkaitan dengan risiko-risiko yang ditimbulkan dari smartphone, Lemsaneg sendiri belum mempunyai kebijakan secara khusus yang mengatur tentang penggunaan smartphone dan langkah-langkah strategis untuk mitigasi risiko keamanan smartphone di lingkungan kerja untuk mengantisipasi berbagai macam serangan terhadap celah-celah keamananan pada smartphone.

Manajemen risiko merupakan bagian penting dalam Tata Kelola Keamanan Informasi. Manajemen risiko akan menganalisa apa yang bisa terjadi dan apa konsekuensi yang mungkin bisa, sebelum memutuskan apa yang harus dilakukan dan kapan, untuk mengurangi risiko ke tingkat yang dapat diterima. Penelitian ini dilakukan di Lembaga Sandi Negara (Lemsaneg).

Manajemen risiko secara umum merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja (Deni Ahmad Jakaria, R. Teduh Dirgahayu, Hendrik:2019).

## TINJAUAN PUSTAKA DAN LANDASAN TEORI

### 2.1 Penelitian Terkait

a. Menurut Blaž Markelj et.al (2020) pada publikasi Mobile Devices and Corporate Data Security menyatakan bahwa saat ini memastikan perlindungan terhadap data perusahaan menjadi fokus utama dalam industri Teknologi Informasi dan Komunikasi (TIK). Dalam dua tahun terakhir penggunaan perangkat mobile untuk mengakses data menjadi jauh lebih sering, Oleh karena itu keamanan data sekarang menjadi tantangan baru bagi pengguna dan manajer informasi dan sistem komputer, dimana mereka semua harus menyadari akan ancaman cyber, dan langkah-langkah yang harus apa yang harus dilakukan untuk mempertahankan tingkat keamanan terhadap informasi yang memadai. Software untuk perangkat mobile yang dikombinasikan dengan internet, sekarang ini menyediakan akses yang mudah dan cepat ke data dan informasi. Teknologi yang relatif baru ini mendukung pengambilan keputusan dengan cepat. Perangkat lunak yang canggih memungkinkan pengguna untuk mengelola data dan melaksanakan berbagai tugas secara online. Keamanan data perusahaan pada saat perangkat mobile digunakan untuk mengakses sistem informasi hanya dapat dicapai, jika pengguna mengikuti langkah-langkah keamanan tertentu yang sudah dibuat.

b. Menurut Prashant Kumar Gajar et.al (2019) dalam publikasinya Bring Your Own Device (Byod): Security Risks And Mitigating Strategies, bahwa pertumbuhan teknologi mobile berkaitan dengan ketersediaan layanan 3G/4G dan perangkat seperti smartphone telah menciptakan fenomena baru untuk komunikasi dan kemampuan pengolahan data untuk melakukan bisnis. Salah satu fenomena seperti adalah muncul dalam lingkungan bisnis BYOD (Bring Your Own Device), yang berarti bahwa karyawan menggunakan perangkat pribadi mereka untuk mengakses sumber daya perusahaan untuk bekerja, di dalam atau di luar lingkungan organisasi. Fenomena baru ini dengan sendiri membuat peluang baru tapi juga memiliki banyak risiko yang terkait dengan hal tersebut. Menggunakan perangkat mobile untuk bekerja pribadi maupun profesional dengan sendirinya menimbulkan risiko. Risiko tersebut dapat dikurangi dengan membuat berbagai strategi mobilitas, pertahanan dan tindakan, aspek kontrol, manajemen dan aspek tata kelola untuk melihat bagaimana menerapkan strategi BYOD dalam sebuah organisasi.

c. Menurut Poornima Mahesh et.al (2018) pada publikasi Smartphone Security: Review of Attacks, Detection and Prevention, dalam beberapa tahun terakhir smartphone telah menjadi perangkat mobile yang paling khas dan populer. Smartphone bertindak sebagai komputer portabel dan fungsi yang sama dengan unit pengolahan, unit komunikasi, unit penyimpanan data seperti PC biasa. Smartphone juga menyediakan banyak layanan layaknya komputer, seperti web browser, portable media player, video call, GPS, Wi-Fi dan banyak aplikasi lainnya. Karena kebijakan kontrol akses yang tidak memadai dan kurangnya informasi tentang pengamanan perangkat mobile perlu untuk mempelajari tantangan penyediaan dan pengelolaan keamanan di lingkungan smartphone. Namun, keamanan komunikasi mobile telah menduduki puncak daftar kekhawatiran bagi pengguna ponsel. Kerahasiaan, otentikasi, integritas dan nir sangkal diperlukan untuk keamanan dalam layanan komunikasi mobile. Penelitian ini menyoroti berbagai aspek keamanan yang memerlukan fokus ekstra ketika menggunakan perangkat mobile dan juga melakukan penilaian terhadap keamanan berbagai smartphone.

d. Menurut Muneer Ahmad Dar et.al (2018) pada publikasi Evaluating Smartphone Application Security: A Case Study onAndroid, bahwa saat ini smartphone sangat diperlukan untuk memenuhi harapan masyarakat untuk selalu tetap terhubung dan kebutuhan untuk meningkatkan produktivitas menjadi penyebab meningkatkan penggunaan smartphone. Salah satu pemimpin pasar dari evolusi

smartphone adalah sistem operasi Android dari Google. Hal ini sangat mungkin bahwa Android akan terinstall di jutaan smartphone dalam waktu dekat. Dengan popularitas smartphone Android, semua orang merasakan kenyamanan untuk melakukan transaksi melalui smartphone ini karena keterbukaan aplikasi Android. Serangan malware juga signifikan. Keamanan Android adalah merupakan sesuatu yang kompleks, oleh karena itu perlu dilakukan evaluasi terhadap lingkungan pengembangan aplikasi yang rentan terhadap serangan malware sehingga dapat melakukan transaksi secara aman di smartphone berbasis Android.

**2.2 Keamanan Informasi**

Menurut Duane E. Sharp dalam buku Information Security Management Handbook, informasi merupakan aset tunggal yang bernilai amat berharga bagi organisasi. Informasi menjadi aset yang mempunyai nilai bagi organisasi seperti aset usaha berharga lainnya dan sebagai akibatnya butuh untuk dilindungi secara tepat dan layak. Keamanan informasi dapat memproteksi informasi dari ancaman sehingga dapat menjamin keberlangsungan usaha suatu organisasi, memperkecil dan mengurangi rugi/ risiko suatu organisasi dan memaksimumkan laba, investasi, peluang dan kesempatan usaha.

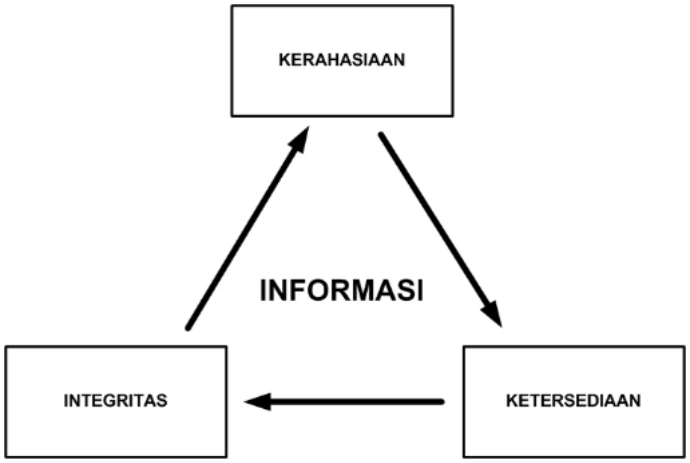
Menurut ISO/IEC 17799, keamanan informasi adalah suatu hal penting bagi dua sektor, baik publik maupun privat. Keamanan informasi dianggap penting karena saat ini setiap organisasi dan sistem informasi yang dimiliki dihadapkan pada ancaman keamanan seperti penipuan, penyadapan aktivitas *hacking, cracking*, sabotase, bencana alam serta ancaman lainnya.

Menurut Harris dalam buku *All-in-One Exam Guide,* keamanan informasi dapat dicapai melalui penerapan prinsip perlindungan dan aspek terhadap aspek-aspek berikut, yang biasa disingkat menjadi *CIA Triangle* (*Confidentiality-Integrity-Availability)*:

1. Kerahasiaan *(Confidentiality)* yaitu aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan. Usaha yang dapat dilakukan untuk mencegah hilangnya kerahasiaan ialah dengan teknik kriptografi, misal dengan mengenkripsi data baik yang disimpan maupun ditransmisikan, dengan menerapkan kontrol akses, klasifikasi data dan sebagainya.
2. Integritas *(Integrity)* yaitu aspek yang menjamin bahwa data tidak dirubah tanpa ada izin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi . Hal ini dapat dilihat dari dua sisi yaitu:
3. Integritas data, yaitu data tidak dirubah sewaktu disimpan, diproses, maupun dikirim
4. Integritas sistem, yaitu kualitas dari sistem pada waktu enjalankan beberapa fungsi, terhindar dari manipulasi yang tidak diizinkan

Salah satu contoh ancaman yang dapat mempengaruhi integritas data ialah ketika ada serangan virus kedalam sebuah sistem, maka sistem tersebut kehilangan integritasnya. Cara untuk mengatasi hal tersebut ialah dapat menerapkan kontrol akses, pendeteksi intrusi, fungsi hash dan sebagainya.

Ketersediaan *(Availability) yaitu* aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan hanya pengguna yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan). Contoh ancaman yang berkaitan dengan aspek ketersediaan ialah serangan *Denial of Service(DOS).* Untuk mengatasi hal tersebut, dapat menerapkan IDS *(Intrusion Detection Systems),* memasang 3.firewall, mengkonfigurasi router, menyediakan layanan data cadangan dan sebagainya.




Gambar 2.1 CIA Triangel

Keamanan informasi bisa dicapai melalui beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi satu dengan yang lain. Strategi keamanan informasi masing-masing memiliki fokus dan dibangun pada setiap kekhususannya. Berikut ini merupakan contoh sebuah tinjauan pengamanan informasi.

1. *Physical Security.*
   Pengamanan ini berfokus pada strategi untuk pengamanan para pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman seperti kebakaran, akses tanpa otorisasi, dan bencana alam.
2. *Personal Security*
   Pengamanan ini dilakukan secara overlap dengan '*physical security'* untuk melindungi orang-orang dalam organisasi.
3. *Operation Security*
   Pengamanan ini memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan agar dapat bekerja tanpa gangguan.
4. *Communications Security*
   Pengamanan ini bertujuan untuk mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat-alat yang ada untuk mencapai tujuan organisasi.
5. *Network Security*
   Pengamanan ini memfokuskan pengamanan pada perangkat jaringan, sistem jaringan berikut isinya, serta kemampuan untuk menggunakan jaringan itu untuk memenuhi fungsi komunikasi data organisasi.

Masing-masing komponen di atas berkontribusi dalam program keamanan informasi secara keseluruhan. Secara ringkas, keamanan informasi adalah perlindungan informasi termasuk sistem dan perangkat yang digunakan, menyimpan, dan mengirimkannya.

Selain beberapa hal yang telah disebutkan diatas, Harris menyebutkan beberapa istilah yang terkait dengan keamanan informasi didalam bukunya yang berjudul *All-in- One Exam Guide,* diantaranya *vulnerability, threat,* dan *risk.* Lawrie Brown dalam buku karangan Budi Raharjo, yakni Keamanan Sistem Informasi Berbasis Internet menyatakan bahwa pengelolaan terhadap keamanan dapat dilihat dari sisi pengelolaan risiko (*risk management*). Disarankan menggunakan "*Risk Management Model*" untuk menghadapi ancaman (*managing threats*). Ada tiga komponen yang memberikan kontribusi kepada *Risk* (risiko), yaitu *Asset* (aset), *Vulnerabilities* (kerawanan), dan *Threats* (ancaman). Berikut ini merupakan penjelasan dari *vulneralbility, threat,* dan *risk.*

1. Kerawanan (*vulneralbility*) : merupakan kelemahan yang dapat berasal dari perangkat keras, perangkat lunak, atau prosedur yang menyediakan kesempatan bagi pihak luar atau penyerang untuk melakukan tindakan yang dapat menimbulkan kerugian

2. Ancaman (*threat*) : merupakan segala hal yang berpotensi menimbulkan bahaya dan dapat terjadi pada informasi maupun sistem. Bahaya tersebut dapat disebabkan oleh bencana, kesalahan sistem atau kesalahan manusia.
3. Risiko (*risk*) : merupakan segala kemungkinan terjadinya ancaman yang disebabkan oleh adanya kelemahan. Risiko merupakan hal yang pasti terjadi dan dapat dikurangi atau dikontrol dengan mengurangi faktor ancaman dan kelemahan.

Sehubungan dengan hal yang telah disebutkan di atas, yaitu kerawanan, ancaman dan risiko, maka perlu diperhatikan bahwa terdapat beberapa kemungkinan serangan menurut William Stalling dalam bukunya cryptography and network security:

1. Interupsi (*Interruption*) : perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada aspek ketersediaan (*availability*). Contohnya ialah serangan *denial of service.*
2. Penyadapan (*Interception*) : pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contohnya ialah penyadapan (*wiretapping*)
3. Pengubahan *(Modification*) : pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi juga mengubah asset. Contohnya mengubah isi *website* dengan isi pesan yang dapat merugikan pemilik *website.*
4. Penyisipan *(Fabrication).* Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya ialah email palsu dalam jaringan komputer.

Menurut Jim Appleard dalam *Information Security Management Handbook*, suatu organisasi perlu mengklasifikasikan informasi yang ada untuk mendapatkan perlindungan yang sesuai. Klasifikasi informasi ini ditentukan sendiri oleh organisasi tersebut dengan memperhatikan risiko dan keuntungan yang ditimbulkan dari pengolahan informasi tersebut. Pengklasifikasian informasi tersebut bermanfaat untuk menentukan teknik, level keamanan, kontrol serta tindakan yang tepat diterapkan. Tipton dalam bukunya *Handbook of Information Security Management* membuat secara umum klasifikasi informasi yang berlaku dibanyak organisasi menjadi tiga level.yaitu:

1. Publik : informasi yang dapat diketahui oleh semua pihak.
2. Terbatas : informasi yang tidak bersifat sensitif, namun jika terungkap akan menggangu jalannya suatu organisasi
3. Rahasia : informasi yang bersifat sensitif dan dibatasi akses untuk memperolehnya.

Terdapat tiga teknik dalam melindungi suatu informasi yaitu, secara:

1. Fisik misalnya menyimpan dalam suatu ruangan khusus yang dikunci, dalam lemari besi dan sebagainya.
2. Organisasi misalnya menunjuk personil khusus dengan regulasi yang jelas, melakukan pendidikan dan pelatihan masalah keamanan informasi untuk meningkatkan kesadaran karyawan tentang pentingnya pengamanan informasi yang baik.
3. Logik misalnya dengan menerapkan kriptografi, memasang antivirus dan sebagainya.

Harris menyebutkan dalam buku *All-in-One Exam Guide*, ada beberapa tipe risiko berkaitan dengan keamanan informasi yang harus diperhatikan oleh suatu organisasi yaitu:

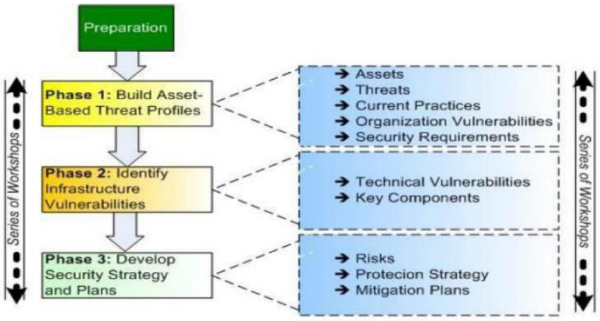
1. Pengrusakan secara fisik yang disebabkan bencana alam, api, kebakaran, air, pengrusakan secara senganja dan sebagainya.
2. Interaksi manusia yang dapat mengganggu produktivitas.
3. Kesalahan fungsi alat dan sistem.
4. Penyalahgunaan data meliputi penipuan, pencurian, dan sebagainya
5. Serangan aktif dan pasif meliputi penyadapan, modifikasi, fabrikasi, interupsi.
6. Eror pada aplikasi.

Dengan menerapkan keamanan informasi, sebuah organisasi selain dapat mengatasi hal tersebut diatas juga dapat menjaga kerahasiaan, integritas dan ketersediaan informasi secara kontinyu. Keamanan informasi dapat dicapai dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak. Namun banyak sistem informasi yang didesain secara tidak aman. Sehingga keamanan informasi harus diletakkan pada suatu kerangka pemikiran *(framework)* sebagai Sistem Manajemen Keamanan Informasi (SMKI).

## METODE PENELITIAN

### 3.1 Metode OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

Metodologi yang memungkinkan pengguna untuk mendapatkan pengetahuan tentang masalah keamanan dan mengembangkan perbaikan posisi keamanan organisasi tanpa bergantung pada Spesialis TI eksternal sehingga ketika Perusahaan memiliki banyak anak perusahaan di seluruh dunia, di mana risiko teknologi ada, dapat disesuaikan dengan kondisinya. Gambar 2.5.1. memberikan serangkaian lokakarya selama tiga fase yang organisasi harus menjalani menerapkan OCTAVE. Model ini menggabungkan seperangkat kriteria yang melibatkan prinsip-prinsip, atribut, dan output dan termasuk partisipasi karyawan di seluruh perusahaan dimana tingkat penting untuk data perusahaan tertentu ditentukan dan terkait ancaman di dalamnya dinilai. Tahap 1 melibatkan mengevaluasi strategi keamanan organisasi melalui karyawan mengidentifikasi kritis aset bisnis atau informasi yang membutuhkan perlindungan, dan kemudian meringkas ancaman diidentifikasi ke profil ancaman.

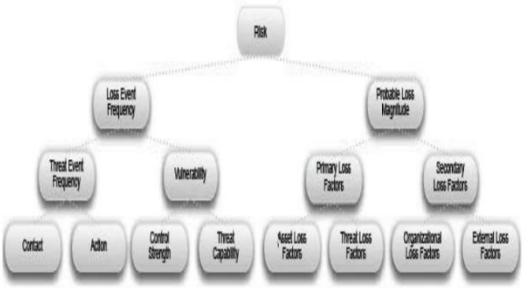



Gambar 3.1 Penerapan OCTAVE

Ancaman dianggap oleh model ini termasuk peristiwa yang tidak dapat dikendalikan seperti kebakaran atau banjir, kelalaian organisasi, kesalahan manusia, kesalahan teknologi dan kinerja yang disengaja berbahaya kegiatan. Tahap 2 tuntutan manajemen untuk meneliti komponen yang ada pada infrastruktur TI untuk menyelidiki kelemahan yang membuka organisasi risiko eksposur dan kerentanan. Analisis dilakukan untuk menilai risiko data kompromi dan kemungkinan bentuk serangan selama Tahap 3 di mana risiko manajemen dan rencana mitigasi dikembangkan. Untuk memerangi dan meminimalkan kemungkinan tindakan tersebut dari transpiring, beberapa tindakan pengamanan yang diusulkan oleh OCTAVE dapat digunakan, termasuk pertimbangan atas organisasi infrastruktur TI, kebutuhan staf, hardware dan software kebutuhan, komunikasi, dan cara untuk mempersiapkan untuk acara tak terduga. Kegiatan Penutup dari pendekatan OCTAVE memerlukan atas persetujuan manajemen dari strategi perlindungan dan kegiatan pasca-OCTAVE untuk mempertahankan rencana manajemen risiko yang efektif. Salah satu keuntungan menggunakan OCTAVE adalah bahwa hal itu dapat disesuaikan untuk menyesuaikan dengan kebijakan banyak entitas berbagai lingkungan bisnis. (Jitender Singh Yadav, Mohit Yadav, Ankit Jain:2019).

### 3.2 FAIR (Factor Analysis of Information Risk)

Tujuannya adalah untuk memberikan informasi biaya-efektif manajemen risiko melalui pemahaman, analisis, dan mengukur risiko ini. Ada empat tahap dan puluhan langkah dalam model analisis dasar FAIR, dan Gambar 3.2 menggambarkan komponen utama. Dua yang pertama langkah-langkah dalam Tahap 1 melibatkan identifikasi aset berisiko dan jelas mendefinisikan apakah komponen ancaman adalah manusia atau malware (misalnya programmer / engineer dan program firewall), internal dan atau eksternal. Selama Tahap 2, frekuensi kemungkinan serangan, tingkat kemampuan ancaman kuantitatif (misalnya "Top 2% saat dibandingkan dengan populasi ancaman keseluruhan "), diharapkan efektivitas pengendalian dan tingkat kerentanan (Yaitu probabilitas aset rentan terhadap dampak ancaman) dan kemungkinan bahwa ancaman akan menyebabkan aset kerusakan yang dinilai menggunakan beberapa set matriks terorganisir. Bentuk-bentuk kerugian yang mencakup dalam Model FAIR termasuk kehilangan produktivitas, membebankan waktu personil untuk memperbaiki kekurangan, aset biaya penggantian, denda hukum / peraturan, keunggulan kompetitif terganggu dan kerusakan reputasi. Tahapan 3 dan 4 menghitung estimasi kerugian moneter dan perkiraan kemungkinan dan frekuensi masa depan kerugian. Ketika memperkirakan kerugian, skenario buruk-kasus adalah variabel yang mutlak, bahwa probabilitas individu faktor ancaman yang mengarah ke skenario yang lebih buruk-kasus dikalikan untuk menemukan produk yang akan sama dengan kemungkinan terjadinya skenario yang lebih buruk-kasus. Sebagai contoh, jika sebuah program firewall berfungsi (Kemungkinan terjadinya = 10%) dan bypass otorisasi password (probabilitas terjadinya = 15%) merupakan dua faktor yang dibutuhkan untuk hacker untuk mencuri semua uang dari rekening bank organisasi, yang skenario yang lebih buruk-hal uang akan dicuri akan memiliki probabilitas 10% x 15% = 1,5%. Itu probabilitas 1,5% kemudian akan dikalikan terhadap taksiran rugi moneter kuantitatif untuk mendapatkan estimasi kerugian akhir. Faktor organisasi penting yang dapat memiliki konsekuensi yang merugikan akan menjalani formula ini, dan estimasi kerugian keuangan agregat akan dijumlahkan untuk mengidentifikasi besarnya dan frekuensi kerugian. Profil risiko perusahaan secara keseluruhan karena itu akan dibuat untuk menilai mana sumber daya yang paling diperlukan untuk melindungi aset perusahaan. Metode ini merupakan pendekatan yang lebih komprehensif untuk menilai dan mengukur potensi risiko karena sejumlah besar waktu dan sumber daya dapat dikeluarkan dibandingkan. Metode octave menggunakan pendekatan tiga fase untuk menguji isu-isu teknologi, menyusun sebuah gambaran komprehensif keamanan informasi yang dibutuhkan oleh organisasi (dalam gambar). Metode ini menggunakan lokakarya untuk melakukan diskusi dan pertukaran informasi mengenai aset, praktek keamanan informasi dan strategi keamanan informasi. Setiap fase terdiri dari beberapa proses dan setiap proses memiliki satu atau lebuh lokakarya yang dipimpin oleh tim analisis. Beberapa aktifitas persiapan juga diperlukan untuk menetapkan dasar yang baik untuk suksesnya evaluasi secara keseluruhan. (Jitender Singh Yadav, Mohit Yadav, Ankit Jain:2019)




Gambar 3.2 Tahapan FAIR

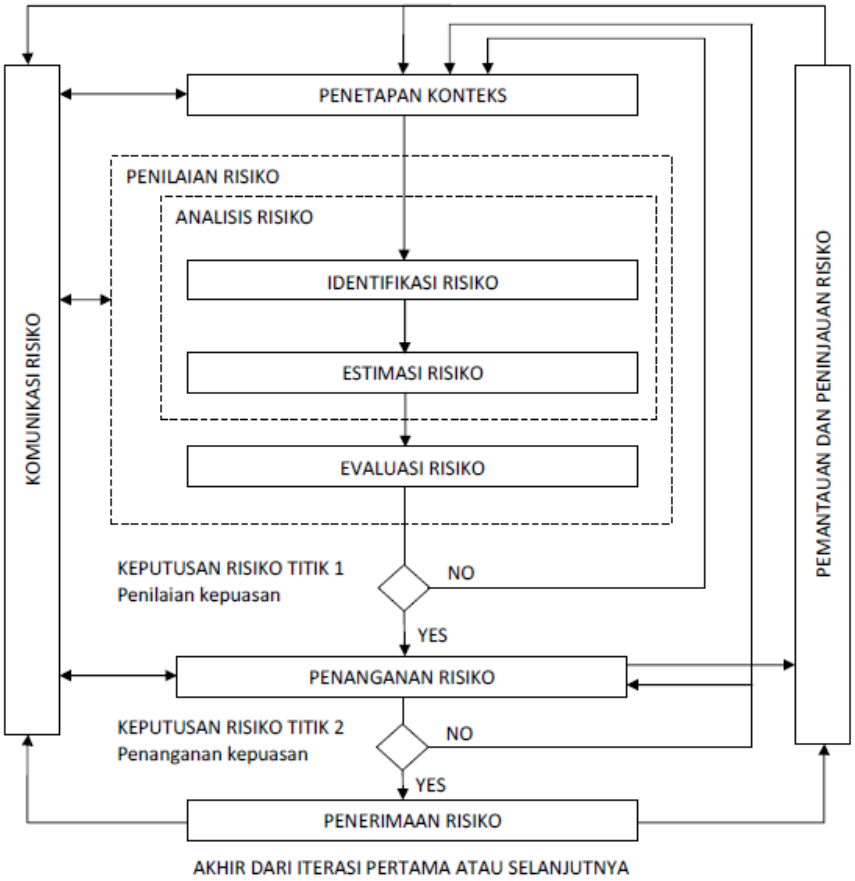
### 3.3 CRAMM (CCTA Risk Analysis and Management Method)

CRAMM adalah software penilaian risiko yang pertama membutuhkan tim IT untuk mengidentifikasi semua fisik, perangkat lunak, data dan lokasi aset dalam informasi sistem, maka nilai mereka berdasarkan biaya pengganti untuk aset fisik dan dampak konsekuensial dari tidak tersedia, rusak, atau membocorkan informasi untuk data dan aset perangkat lunak. Ini meliputi software berbagai ancaman yang disengaja dan disengaja untuk sistem informasi seperti hacking, virus, kesalahan, dan peralatan dan perangkat lunak kegagalan dengan menilai tingkat risiko yang terkait. CRAMM software membandingkan ukuran risiko yang teridentifikasi selama tahap penilaian ancaman terhadap keamanan patokan untuk menentukan apakah risiko yang cukup untuk membenarkan pelaksanaan signifikan dari ukuran meja. Dari Gambar 3li, dapat dilihat bahwa ada dua analisis stages- berbeda dan manajemen-untuk memastikan bahwa pelaksanaan tidak terjadi sampai analisis mendalam adalah lengkap, menghindari biaya overruns dan alokasi sumber daya yang tidak efisien. Ada dua versi yang berbeda dari perangkat lunak CRAMM tersedia untuk menilai ancaman dan kerentanan, dan mereka CRAMM Express dan CRAMM Expert. The Express versi menyediakan alat penilaian risiko tingkat holistik namun dasar yang biasanya disukai oleh proyek IT atau sistem manajer baru yang bercabang keamanan TI mereka ketergantungan dari para ahli keamanan informasi eksternal. Versi Ahli dipasarkan ke organisasi melakukan analisis risiko yang komprehensif, termasuk berbagai peraturan kepatuhan dan global program sertifikasi dan itu termasuk alat penilaian risiko tingkat tinggi yang tersedia di ekspres versi. Perangkat lunak CRAMM digunakan oleh lebih dari 500 pengguna yang berbeda termasuk IBM dan Royal Air Force. (Jitender Singh Yadav, Mohit Yadav, Ankit Jain:2019)

## HASIL DAN PEMBAHASAN

Proses sistem mencakup pengelolaan risiko pada (Information Asset Register) sesuai dengan metode ISO 27001:2013, yaitu pemilihan data aset informasi (Information Asset Register) menjadi data risiko informasi (Information Risk Register). Dari hasil data risiko informasi (Information Risk Register) tersebut akan menghasilkan rencana pengelolaan risiko (Risk Treatment
Plan) yang dapat menjadi acuan organisasi dalam mengambil keputusan demi pengelolaan manajemen risiko. Dari hasil analisis kebutuhan ini didapatkan spesifikasi sistem yang akan dikembangkan
Kemudian sistem akan menampikan data-data yang telah di input. Data tersebut akan disaring berdasarkan klasifikasi dan nilai dari CIA asset tersebut yang bernilai "medium" dan "high". Pada saat pengguna (actor) memilih menu Information Risk Register maka pengguna (actor) akan mengisi informasi tentang ancaman dan kemungkinan yang terjadi pada setiap daftar risiko.

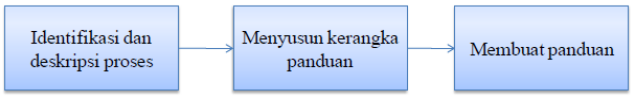
Kemudian sistem akan menampilakan daftar risiko tersebut beserta nilai tingkat risikonya dan kemudian akan sistem akan filter risiko yang akan diterima atau tidak. Daftar risiko-risiko yang akan diterima atau bernilai "medium" atau "high" akan masuk pada menu Risk Treatment Plan. Pada Menu ini pengguna (actor) akan mengisi bagaimana cara menanggulangi risiko tersebut berdasarkan ISO/IEC 27001:2013, rencana detail, divisi yang bertanggung jawab dan kapan rencana itu akan dikerjakan/selesai.
Implementasi penelitian merupakan metode yang lebih menekankan kepada aspek pemahaman secara mendalam terhadap suatu masalah daripada melihat permasalahan untuk penelitian generalisasi. Implementasi penelitian dalam jurnal ini menggunakan beberapa langkah sesuai dengan ISO/IEC 27005 yang dapat digambarkan pada diagram dibawah ini :




Gambar 4.1 Langkah ISO/IEC 27005

Terdapat 6 langkah utama dalam ISO/IEC 27005 yang harus dilaksanakan yaitu :
a. Proses mengkomunikasikan risiko
b. Karakteristik sistem atau menentukan Kontek
c. Proses penilaian risiko, yang terdiri dari dua sub proses yaitu
    - Analisis risiko
    - Evaluasi risiko
d. Proses treatment risiko
e. Proses penerimaan risiko
f. Memonitor manajemen risiko dan mengkaji ulang proses

Hasil dari proses tersebut adalah draf panduan pelaksanaan manajemen risiko. Secara umum draf panduan pelaksanaan manajemen risiko disusun berdasarkan hasil identifikasi dan deskripsi proses yang digunakan sebagai acuan dalam membuat kerangka panduan serta pembuatan panduan.




Gambar 4.2 Langkah Pembuatan Panduan.

TEKNIK ANALISIS

Dari data yang didapatkan selanjutnya dilakukan analisis, yaitu dengan mengikuti proses manajemen risiko dari ISO/IEC 27005. aMelakukan Identifikasi Proses Identifikasi proses dilakukan dengan membandingkan tahapan-tahapan proses manajemen risiko yang digunakan dalam penelitian ini. bMelakukan Analisis Setiap proses yang diidentifikasi dalam tahap sebelumnya dianalisis kelebihan dan kekurangan terhadap standar yang digunakan dalam menyusun panduan manajemen risiko.

cMenentukan Urutan Proses Panduan Pelaksanaan Manajemen Risiko disusun berdasarkan sinergi proses pada hasil identifikasi dan analisis yang dilakukan pada tahap sebelumnya. dMelakukan Pengujian Pengujian dengan menyebar kuesioner mengenai draft panduan manajemen risiko keamanan smartphone kepada staf dan pejabat untuk mengetahui tanggapan serta pendapatnya.

Adapun metode pengambilan sample terhadap responden adalah menggunakan purposive sampling. Bouma Gary D. (2013: 2019) dalam bukunya The Research Process, edisi revisi menyatakan: pada purposive sampling, peneliti mempercayai bahwa mereka dapat menggunakan pertimbangannya atau intuisinya untuk memilih orang-orang atau kelompok terbaik untuk dipelajari atau dalam hal ini memberikan informasi yang akurat. Kelompok dengan sebutan “the typical and the best people” yang dipertimbangkan oleh peneliti untuk dipilih sebagai subjek penelitian oleh Williamson, at.al. (2018: 107) merupakan “respondents who are hard to locate and crucial to the study”, para responden yang dinilai akan banyak memberikan pengalaman yang unik dan pengetahuan yang memadai yang dibutuhkan peneliti. Kuesioner disebarkan menggunakan Google Docs untuk memudahkan dalam mengambil sample.

## SIMPULAN

Berdasarkan hasil penelitian yang telah dijelaskan maka dapat diambil kesimpulan bahwa :

1. Penerapan Manajemen Risiko Keamanan Smartphone sangat bermanfaat dan berguna dalam melindungi asset data di smartphone kita.
2. Dapat membantu menghitung tingkat risiko dan mengelompokkan daftar risiko yang sedang terjadi pada perusahaan. Karena hal tersebut maka akan dapat menanggulangi risiko terhadap klasifikasi aset yang bernilai risiko tinggi.

## SARAN

Berdasarkan hasil penelitian yang telah dijelaskan maka dapat diambil kesimpulan bahwa :

1. Penerapan Manajemen Risiko Keamanan Smartphone sangat bermanfaat dan berguna dalam melindungi asset data di smartphone kita.

2. Dapat membantu menghitung tingkat risiko dan mengelompokkan daftar risiko yang sedang terjadi pada perusahaan. Karena hal tersebut maka akan dapat menanggulangi risiko terhadap klasifikasi aset yang bernilai risiko tinggi.

## DAFTAR PUSTAKA

[1] Ahmed, Md. Z. (2019). Which one is better JavaScript or jQuery (Vols. 3). Hyderabad: Mahaveer Institute of Science and Technology, Department of SE.

[2]Bharthan, A. & Bharathan, D. (2019). International Journal of Computer Applications. RelationalJSON, An Enriched Method to Store and Query JSON Records (Vols. 98). India: Delhi

[3]Crockford, D (2008). JavaScript: The Good Parts VW————————————————HG

[4]Hidayat, M. N, (2017): "Kajian Tata Kelola Keamanan Informasi Berdasarkan Information Security Management System (ISMS) ISO 27001:2005 untuk Outsourcing Teknologi Informasi Pada PT. Kereta Api Indonesia (Persero)," Program Studi Magister Teknologi Informasi Fasilkom UI, Jakarta

[5]ISACA, in Certified Information Security Manager (2018) : Review Manual 200, USA, ISACA, pp. 38-29

[6]Zein, Afrizal (2018), Pendeteksian kantuk secara real time menggunakan pustaka opencv dan dlib python, Sainstech , Jakarta.

[7]Zein, Afrizal (2018), Pendeteksian Multi Wajah Dan Recognition Secara Real Time Menggunakan Metoda Principal Component Analysis (Pca) Dan Eigenface, ESIT 12 (1), 1-7, Jakarta