CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 1, No. 1, Mei 2018, hlm. 28-38

MEMBANGUN PROFIL RISIKO PADA PEMBUATAN PETA DIGITAL

Koes Wiyatmoko [1], Bambang Sugiantoro [2], Yudi Prayudi [3]
[1,3]Magister Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
[2]Magister Informatika UIN Sunan Kalijaga Yogyakarta
Email: [1]koesmoko@gmail.com, [2]bambang.sugiantoro@uin-suka.ac.id, [3]prayudi@uii.ac.id

Abstrak

GPS (*Global Positioning System)* merupakan perangkat penting dalam merekam data lokasi suatu obyek berdasarkan titik koordinat. Perekaman lokasi tersebut tujuannya digunakan diantaranya untuk pembuatan peta digital dan keluarnya menjadi peta rupa bumi. Peta digital dan peta rupa bumi yang sudah disahkan oleh pemerintah melalui lembaga yag berwenang akan menjadi rujukan dalam melakukan bermacam kegiatan seperti penentuan lokasi obyek, batas batas wilayah. Akurasi dan keaslian data koordinat hasil *survey* dengan GPS sangat penting untuk hasil peta yang memiliki akurasi tinggi, namun peta digital juga rawan terjadi pengeditan, penggandaan, penghapusan untuk tujuan tertentu, karena itu diperlukan sebuah manajemen pengawasan dalam proses pembuatanya yang menjadi sebuah model untuk membantu mempermudah dalam membangun profil pembuatan peta digital. Acuan dalam mengelola menajemen risiko untuk membangun profil tersebut diantarnya adalah *Framework NIST*.

Kata kunci: *gps, profil framework, peta digital, akurasi survey, way point, fake location, NIST, framework*

DEVELOPE RISK PROFILE AT DIGITAL MAP WORKMANSHIP

Abstract

GPS (Global Positioning System) is the main device that record location based on coordinate . The purpose of location recording is making digital maps and the output are printed-maps. Digital maps and printed-maps that have been authorized by the government will become reference for every activities like terminating the location objects or borderline. The Accuracy and authenticity of coordinate data from GPS is essential for high-accuracy maps, but digital maps are also vulnerable from editing, duplication, or deleted for a particular purpose. Because of that, supervisory management in the manufacturing process is needed to help facilitate in building a digital map-making profile. The reference in managing risk management to build the profile is NIST Framework.

Keywords: : *gps, framework profile, digital map, accuracy,i survey, way point, fake location, NIST, framework*

1. PENDAHULUAN

GPS (*Global Positioning System*) merupakan perangkat yang sangat vital untuk mendapatkan titik koordinat sebagai bahan dalam pembuatan peta digital. Peta digital adalah representasi fenomena geografik yang disimpan dan dianalisis oleh komputer digital atau yang sekarang kita sebut sebagai sistem informasi geografis. Sistem Informasi Geografis (SIG)merupakan sistem informasi khusus untuk mengelola data yang memiliki informasi spasial. SIG juga merupakan perangkat lunak yang dapat digunakan untuk pemasukan, penyimpanan, manipulasi, menampilkan dan keluaran informasi geografis berikut atributnya(Prahasta, 2009). Data SIG pada dasarnya adalah sebuah titik titik yang disebut *waypoint* dimana kumpulan titik titik yang di ambil pada saat *survey* dengan GPS akan membentuk *polyline* atau garis dan membentuk *polygon* atau area. Setiap titik atau *waypoint* akan direkam didalam sebuah koordinat dan disimpan dalam perangkat GPS tersebut. Keunggulan peta digital adalah mudah untuk di edit, dihapus, dicopy dengan hasil yang sama seperti aslinya.

Gambar 1.1 Contoh Perangkat GPS

Namun keunggulan tersebut juga menimbulkan kerentanan terhadap manipulasi data yang berpotensi terjadi kesalahan pembuatan peta digital. Risiko terjadinya manipulasi merupakan ancaman terhadap hasil dan kualitas peta digital. Untuk menghindari ancaman risiko dan kerentanan terhadap kualitas hasil akhir peta digital, maka seharusnya ada sebuah memanajemen yang mengatur system pengolahan data digital. Sistem ini perlu di bangun mengingat pentingnya sebuah peta dan aktivitas ini melibatkan beberapa fihak seperti bagian peralatan (*logistic*), pelaku *survey* (*surveyor*), penerima dan pengolah data (*operator*) dan admi*NIST*rator sebagai pengolah akhir peta digital sekaligus *team leader*. Melihat hal tersebut maka diperlukan sebuah manajemen risiko untuk melindungi aset informasi dari risiko kejahatan maipulasi data digital atau diperlukan sebuah kerangka kerja untuk melindungi , mengelola dan mengantisipasi ancaman kejahatan digital (Stoneburner Gary , Goguen Alice, 2002).

Manajemen risiko diterapkan untuk mengelola risiko, mengingat bahwa suatu peristiwa akan terjadi dan menghasilkan dampak negatif. Dengan manajemen ini, organisasi dapat menentukan tingkat risiko yang dapat diterima, sebagai toleransi risiko mereka (Purbo Onno W, 2017). Beberapa contoh dari proses manajemen risiko, *cybersecurity* / *IT Security* termasuk *International Organization for Standardization* (ISO) 31000: 2009, ISO / IEC 27005: 2011, *National Institute of Standards and Technology (NIST) Special Publications (SP) 800-39 serta NIST 800-30, dan Guidelines Electricity Subsector Cybersecurity Risk Management Process* (RMP). Diantara beberapa *framework* tersebut, *NIST* SP800-30 merupakan *framework* standart untuk mitigasi risiko yang dikembangkan oleh National Institute of Standards and Technology (*NIST*) yang mana merupakan tindak lanjut dari tanggung jawab hukum didalam undang undang Computer Security Act tahun 1987 dan the Information Technology Management Reform Act tahun 1996 (Stoneburner Gary , Goguen Alice, 2002).

Framework NIST SP 800-30 akan memetakan aktifitas sebuah sistem mulai dari keberadaan *hardware, software, brainware* serta aturan atau kebijakan untuk mengontrol sistem yang berjalan sehingga akan ada gambaran kapan, bagaimana, dimana dan ancaman risiko seperti apa yang akan terjadi, kerangka kerja ini akan membantu memberikan gambaran terhadap ancaman seperti apa yang akan terjadi dengan memebrikan sebuah matrik nilai pembobotan terhadap suatu ancaman risiko.

Dari uraian diatas dapat disimpulkan bahwa *Framework NIST* SP 800-30 melalui langkah langkah yang digunakan sebagai acuan kerja sebuah sistem maka seharusnya langkah langkah kerangka kerja *NIST* 800-30 dapat dijadikan sebagai sarana untuk mendapatkan fakta fakta obyektif serta model deteksi yang tepat sebagai acuan untuk mengetahui adanya *fake* data *survey* sehingga aktifitas manipulasi peta digital dapat terdeteksi lebih cepat.

1.1 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut :

1) Bagaimana membangun profil ancaman risiko *Geodata* menggunakan *framework NIST*
2) Bagaimana detail identifikasi ancaman dan kerentanan pada geodata
3) Bagaimana mengatasi ancaman risiko dan kerentanan *geodata*

1.2 Batasan Masalah

Batasan masalah dalam penelitian ini adalah :

1) Pembuatan profil ini hanya mengacu pada *framework NIST SP 800-30*
2) Detail analisa data dengan tehnik digital forensik yang hanya mengacu *Vulnerability Identification* pada *Framework NIST*
3) Perangkat GPS yang digunakan untuk proses penitikan *waypoint* adalah produk dari GARMIN seri GPS Map 76 CSx
4) Lokasi penelitian dilakukan pada Konsultan CV. Rickomputer Kota Banjarbaru

1.3 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah :

1) Membangun profile ancaman risiko *Geodata* menggunakan *framework NIST*..
2) Mendapatkan fakta fakta ancaman risiko akibat kerentanan sistem sehingga dapat melakukan antisipasi lebih dini.
3) Membangun profil pencetakan peta digital untuk acuan antisipasi tindakan pemalsuan data hasil *survey*

1.4 Manfaat Penelitian

Dari uraian yang telah dipaparkan pada latar belakang dan rumusan masalah, maka manfaat yang ingin di capai dalam penelitian ini adalah sebagai berikut :

1) Untuk Penulis, penelitian ini diharapkan dapat meningkatkan kualitas akademis dan non akademis, serta wawasan baik secara teori dan praktek
2) Untuk Pengembangan keilmuan dan teknologi, diharapkan proses ini dapat memberikan gambaran tentang penggunaan GPS untuk mendapatkan data yang akurat dan obyektif
3) Dengan adanya pola metadata log maka akan meminimalisir kesalahan penetapan lokasi yang disebabkan *fake location waypoint.*

4) Profile yang dibuat ini diharapkan menjadi sebuah sistem yang akan membantu penanganan pembuatan peta digital.

1.5 *Literature Review*

Pada bagian ini akan di ulas tentang penelitian terkait yang telah dilakukan sebelumnya dengan topik GPS, *Framework* manajemen risiko.

Literature Review ini diawali dengan penelitian (Daryono, 2017). Penelitian ini merupakan pengembangan dari penelitian sebelumnya yang dilakukan oleh Yong-dal Shin,yaitu tentang *framework* tahapan penanganan kasus cyber crime. Dalam penelitian Pengembangan *Framework* pelaporan Cybercrime metode yang digunakan adalah Metode Zachman *Framework* yang merupakan salah satu metode EAP, yaitu membuat *framework* pelaporan cybercrime dengan membangun sistem informasi. Tujuan dari membangun membangun sistem informasi cybercrime report agar masarakat akan cepat dan mudah dalam melaporkan apabila menjadi korban cyber,begitu pula pihak kepolisian cepat merespon

(Fabian Bustamante, Walter Fuertes, Paul Diaz, 2017), yang membahas tentang peningkatan keamanan sistem informasi dan *system control industry*. Studi ini menjelaskan tentang penyesuaian dan peningkatan metodologi untuk menyelaraskan proposal untuk pengelolaan keamanan informasi yang tepat untuk tujuan strategis. Penelitian ini terbagi dalam tiga tahap yang berbeda. Pertama, menginduksi artikulasi PMI-PMBOK v5 dan ITIL v3 baik untuk pengelolaan proyek dan mengurangi penyaluran dana ke dalam layanan PELUANG. Kedua, penerapan serangkaian strategi mitigasi risiko berdasarkan standar internasional sebagai *NIST* 800-82 dan 800-30. Ketiga, mengkombinasikan dua tahap yang disebutkan di dalam Panduan untuk instruksi dan kebijakan keamanan berbasis standar, yang sebelumnya telah didorong pada *NIST* 800-82, 800-53 dan 800-12. Hasilnya menunjukkan perbaikan telah berfungsi seperti yang diharapkan, terutama dalam konteks ketersediaan dan integritas informasi, yang menghasilkan nilai tambah bagi perusahaan.

Penelitian yang dilakukan oleh (Ucu Nugraha, 2016) Penelitian ini membahas tentang penerapan manajemen risiko pada sistem informasi dengan menggunakan *Framework SP 800-30*. Tujuan penelitian ini menganalisa tentang keamanan data dan informasi dalam menerapkan sistem informasi. Dengan melakukan analisa manajemen risiko maka diharapkan hasilnya dapat mengurangi risiko ancaman pencurian data dan informasi yang berpotensi disalah gunakan.

(Nurdiati Sri, Barus Baba, 2015) mengembangkan penelitianya tentang Sistem Informasi Geografis Tindak Kejahatan Multilevel berbasis Web. Penelitian ini membahas tentang pemetaan wilayah kejahatan untuk tindakan antisipasi. System ini memetakan tindak kejahatan dari aspek kapan terjadi ,dimana , motifnya apa , dalam rangka apa. Sistem juga dapat memberikan saran sebagai masukan kepada aparat penegak hukum dalam hal ini kepolisian dalam pengambilan keputusan. Pemetaan wilayah kejahatan ini juga menampilkan grafik yang dapat digunakan untuk menagnalisa tingkat kerawanan wilayah dan segera mengambil keputusan berikutnya.

Penelitian (Widyantara, Agus, & Warmayana, 2015) kali ini membahas tentang Adapun fokus penelitiannya membahas tentang penerapan teknologi GPS, Seluler dan database Sistem Informasi Geografis. Topik bahasan pada paper ini adalah bagaimana mengidentifikasi trafik lalu lintas dengan menggunakan variabel data kecepatan, koordinat dan heading yang diperoleh dari perangkat GPS Tracker. Mekanisme yang digunakan adalah merealisasikan sebuah server GPS untuk mencapture data GPS secara real time. Dari server teknologi ini memberikan layanan *real t*ime tentang kondisi lalulintas seperti kemacetan, kepadatan dan kelancaran lalulintas. Penelitian ini diharapkan dapat membantu menemukan solusi mengatasi kemacetan akibat kepadatan di jalan raya.

(Prayudi Yudi, 2014) pokok bahasan penelitian ini adalah tentang analisis bukti digital berupa database GPS di smartphone Android, dan teknik *acquisition, extraction, conversion* dan *presentation.* Adapun penekanannya pada prinsip kerja penggunaan tool untuk proses *acquisition* dan ekstraksi database GPS sehingga menemukan bukti digital yang dapat digunakan untuk bukti dipengadilan.

(Guntur Bagus Pamungkas, Bambang Sudarsono, 2014) dalam penelitiannya membuat analisis pembatasan daerah antara Kabupaten Sukoharjo dengan Kabupaten Karanganyar. Pokok permasalahan yang menjadi bahasan utama adalah bagaimana letak batas daerah tersebut sudah sesuai dengan SNI 19-6724-2002 atau Permendagri no.76/2012 dan bagaimana perbandingan antara pengukuran dengan ikatan orde-2 (pengukuran sebelumnya) dan pengukuran dengan orde-1 (pengukuran sekarang) ?. Penelitian ini juga menekankan bagaimana penentuan titik titik batas begitu penting dengan pengikatan ke orde-1 sebagai pengikatan kerangka pengukurannya, sementara hasil pengukuran sebelumnya dengan orde-2.

(Last David, 2014), meneliti tentang GPS Forensik dimana fokusnya pada perangkat GPS *Mobile Navigator Satelite* yang banyak digunakan saat ini. Beberapa kendaraan yang memiliki navigator tersebut diantaranya digunakan untuk tujuan criminal. GPS Mobile Navigator Satelite memiliki semua rekaman yang catatan dapat diinvestigasi dengan teknik teknik forensik yang baru dikembangkan yang menggunakan alat ini

untuk menginvestigasi berbagai jenis kendaraan. Beberapa informasi di antaranya adalah tentang pergerakan kendaraan, kondisi real time terjadinya penyimpangan route .

(Ibnu, 2013) melakukan penelitian tentang bagaimana merancang dan membangun teknologi untuk pelacakan lokasi menggunakan perangkat GPS. Pada penelitian ini alat pelacak hasil rancangannya di tempatkan di dalam HELM, dimana helm sebagai media pengganti kendaraan bermotor dengan cara menanamnya. GPS dapat dijadikan sebagai jawaban dari permasalahan bagaimana cara melacak lokasi tersebut.

(Kramer, 2013) peneliti dari Iowa State University pada tahun 2013 melakukan penelitian tentang Droid Spooter : A Forensic tool for Android Location Data Collection and Analysis. Penelitian ini menitik beratkan pada pembuatan alat yang dinamakan DROID SPOOTER, yang berfungsi untuk membantu penyidik dalam mengidentifikasi lokasi data penting yang tersimpan pada perangkat android dan alat ini memudahkan penyidik melakukan analisa forensik, serta kecepatan dalam menyelesaikan banyak kasus.

(J Kiyoshi, 2013) dan William Bradley Glisson University of South Alabama dan L. Milton Glisson Ret. N.C. A&T State University menyelidiki sejauh mana perangkat GPS digunakan dalam kasus perkara pidana dan perdata melalui pemeriksaan database hukum Lexis Nexis, Westlaw. Penelitian ini mengidentifikasi 83 kasus yang melibatkan bukti GPS dari dalam Inggris dan Eropa untuk periode waktu dari 1 Juni 1993 sampai 01 Juni 2013. Analisis empiris awal menunjukkan bahwa bukti GPS dalam kasus pengadilan meningkat dari waktu ke waktu dan mayoritas tentang kasus pidana.

(Lestari & Kristiyana, 2013) tentang rancang bangun suatu alat yang digunakan untuk melacak obyek bergerak. Alat tersebut berupa rangkaian module D-GPS508 yang dilengkapi dengan modul Development System untuk aplikasi GSM/GPRS/GPS yang telah dilengkapi dengan beberapa fitur tambahan seperti open collector output 3A, atmel microcontroller pada ISP Port, Onboard Power Regulator dan Extra I/O port. Rangkaian modul tersebut akan di kombinasikan dengan perangkat handphone. Tujuan dari penelitian ini adalah untuk melacak dan mendapatkan posisi obyek atau koordinat maka handphone akan digunakan untuk mengirim posisi koordinat obyek bergerak tersebut melalui fasilitas SMS

2. TINJAUAN PUSTAKA

2.1 Manajemen Risiko

Manajemen risiko adalah proses yang berkelanjutan untuk mengidentifikasi, menilai, dan menanggapi risiko. Untuk mengelola risiko, organisasi harus memahami kemungkinan bahwa suatu peristiwa akan terjadi dan dampak yang dihasilkan, sehingga organisasi dapat menentukan tingkat risiko yang dapat diterima untuk pengiriman layanan dan dapat mengekspresikan ini sebagai toleransi risiko (Purbo Onno W, 2017).

Contoh dari proses manajemen risiko *cybersecurity* termasuk Organisasi Internasional untuk Standardisasi (ISO) 31000: 2009, ISO / IEC 27005: 2011, *Institut Nasional Standar dan Teknologi* (*NIST*) Publikasi Khusus (SP) 800-39, dan Pedoman *Electricity Subsector Cybersecurity Risk Management Process* (RMP).

2.2 Bukti Digital

Undang – undang No.11 Tahun 2008 Pasal 5 Tentang Informasi dan Trasaksi Eletronik Ayat 1, 2 yang intinya bahwa dokumen elektronik dan hasil cetakan merupakan alat bukti hukum yang sah dan perluasanya. Sedangkan pada Pasal 44 Huruf b UUD No.11 Tahun 2008 Tentang ITE bahwa informasi eletronik dan dokumen eletronik merupakan alat bukti lain, selain alat bukti yang sebagaimana dimaksud dalam ketentuan perundang – undangan.

2.3 Sistem Informasi Geografis

Berikut terminologi yang merujuk pada istilah SIG (Prahasta, 2009) :

Tabel 2. 1 : **Definisi Sistem Informasi Geografis**

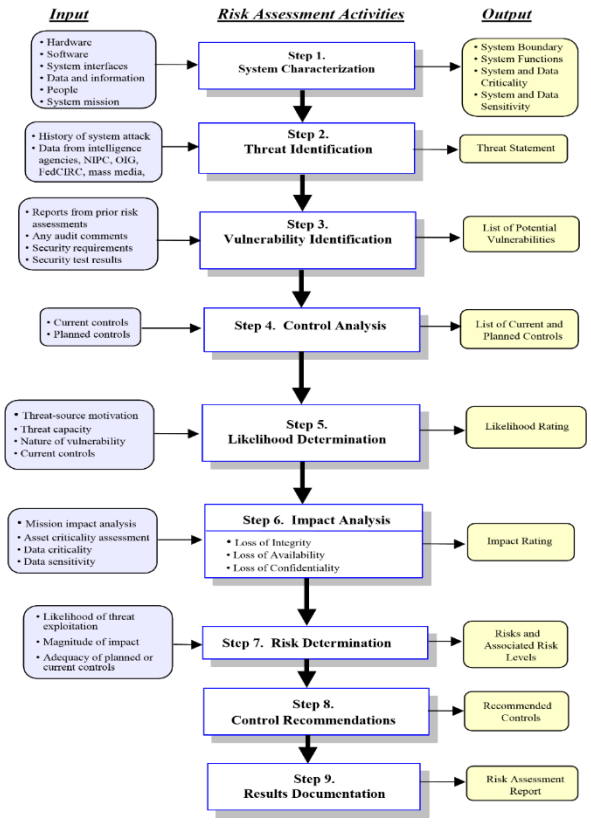
No	Definisi	Nama
1	Sistem komputer yang digunakan untuk memasukan (*captureing*), menyimpan, memeriksa, mengintegrasikan, memanipulasi, menganalisis dan menampilkan data yang berhubungan dengan posisi posisinyadi permukaan bumi	Rice
2	Kombinasi perangkat keras dan lunak sistem komputer yang memungkinkan pengguna nya untuk mengelola, menganalisa dan memetakan informasi spasial berikut data atributnya (data deskriptif) dengan akurasi kartografi.	Basic
3	Sistem yang berbasis komputer (CBIS) yang digunakan untuk menyimpan dan memanipulasi informasi-informasi geografis. SIG dirancang untuk mengum pulkan, menyimpan dan menganalisis objek-objek dan fenomena di mana lokasi geografis merupakan karakter ristik yang penting atau kritis untuk dianalisis. Jadi SIG merupakan sistem komputer yang memiliki 4 kemampuan berikut dalam menangani data yang bereferensi geografis: (a) masukan, (b) manajemen data (penyimpanan dan pemanggilan data), (c) analisis dan manipulasi data, dan (d) keluaran.	Aronoff

2.4 Peta Digital

Peta digital adalah representasi fenomena geografik yang disimpan dan dianalisis oleh komputer digital (Nuryadin, 2005:19). Peta digital memiliki kelebihan jika dibandingkan dengan peta analog atau peta rupabumi yang dicetak di kertas atau media lain.

2.5 *Framework NIST*

NIST (*National Institute of Standard and Technology*) merupakan panduan standar Pemerintah Federal US dalam melakukan penilaian Manajemen Risiko untuk Sistem Teknologi Informasi. Metodologi ini dirancang untuk menilai perhitungan kualitatif yang didasarkan pada analisa keamanan yang sesuai publik inginkan, sehingga secara teknis pada bagian sistem ini petu petugas teknis benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko pada sistem TI.



Gambar 2.1 Sembilan Langkah Utama Penilaian Risiko *Framework NIST*

3. METODOLOGI PENELITIAN

Dalam penelitian ini metode yang digunakan kualitatif, dengan mengambil lokasi studi kasus di Konsultan IT CV. Rickomputer Banjarbaru. Referensi untuk melengkapi dan mendukung analisa dan pembahasan terkait penelitian, bersumber dari pustaka berupa jurnal, buku, artikel, atau bahan tertulis lainnya, yang berupa teori, laporan hasil penelitian atau penemuan terdahulu, Informasi yang digali berupa data GPS , *Framework NIST* (Ucu Nugraha, 2016), skema kerangka kerja metode penelitian menggunakan *Framwork NIST*(Stoneburner Gary , Goguen Alice, 2002).

Selain dari sumber pustaka, juga dilakukan observasi baik yang di rencanakan, dengan langsung mengamati kelapangan dengan melakukan pencatatan pencatatan, mengamati individu maupun kelompok untuk dianalisa, serta observasi yang tidak direncanakan dengan tanpa menentukan obyek waktu dan lokasi. Cara ini dilakukan agar mendapatkan data yang lebih luas.

3.1 Penerapan *Framework NIST*

Acuan penilaian risiko keamanan teknologi informasi menggunakan *Framework NIST* (*National Institute of Standard and Technology*) Special Publication (SP) 800-30, yang merupakan standar Panduan Manajemen Risiko untuk Sistem Teknologi Informasi yang merupakan standar Pemerintah Federal US. Metodologi ini terutama dirancang untuk menjadi suatu perhitungan kualitatif dan didasarkan pada analisa keamanan yang benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko dalam sistem TI.

3.2 Penilaian Risiko *(Risk Assesment)*

Tujuannya untuk membantu mengidentifikasi bagaimana melakukan kontrol untuk meminimalisir atau menghilangkan risiko selama proses mitigasi. Ada 9 (Sembilan) langkah yang harus dipenuhi yaitu (Stoneburner Gary , Goguen Alice, 2002) :

Langkah 1 - Karakterisasi Sistem (*System Characterization),* mengidentifikasi sumber data dan potensi ancaman risiko untuk mendukung tapan berikutnya

Langkah 2 - Identifikasi Ancaman (*Threat Identification*), mengenali berbagai sumber gangguan yang akan terjadi pada sistem.

Langkah 3 - Identifikasi Kerentanan (*Vulnerability Identification),* langkah ini mengidentifikasi adanya berbagai kelemahan atau kekurangan yang dapat mengancam sistem.

Langkah 4 - Analisis Kontrol (*Control Analysis),* tujuan utama langkah ini untuk menganalisa kontrol yang akan dan telah diterapkan serta untuk meminimalisir terjadinya ancaman.

Langkah 5 - Penentuan Kemungkinan (*Likelihood Determination*), digunakan untuk mendapatkan nilai kecenderungan yang kemungkinan terjadi terhadap kelemahan sistem.

Langkah 6 – Analisa Dampak (*Impact Analysis*), langkah ini untuk menilai dampak serangan atas bagian lemah, akibat lemahnya sebuah sistem.

Langkah 7 - Penentuan Risiko (*Risk Determination*), untuk menilai tingkat risiko terhadap sistem, dengan mengacu kepada kemungkinan dan dampak risiko yang sudah ditentukan. Hasil penentuan risiko dapat dilihat ditabal di bawah ini (Stoneburner Gary , Goguen Alice, 2002)

Tabel 3.1 Matrik Level Risiko

Threat Likelihood	*Impact*		
	Low (10)	***Medium (50)***	***High (100)***
High (1.0)	*Low 10 x 1.0 = 10*	*Medium 50 x 1.0 = 50*	*High 100 x 1.0 = 100*
Medium (0.5)	*Low 10 x 1.0 = 5*	*Medium 50 x 1.0 = 25*	*Medium 100 x 0.5 = 50*
Low (0.1)	*Low 10 x 0.1 = 0.1*	*Low 0.5 x 0.1 = 5*	*Medium 100 x 0.1 = 10*

Tabel 3.1 Gambaran risiko dan tindakan yang di perlukan

Risk Level	*Risk Description and Necessary Actions*
High	*If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.*
Medium	*Medium If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.*
Low	*Low If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.*

Langkah 8 - Rekomendasi Kontrol (*Control Recommendations*), tujuannya untuk mengurangi level risiko pada sistem TI sehingga mencapai level yang bisa diterima. Inputnya adalah dari output dari tahapan sebelumnya yaitu risiko dan tingkat risiko, dari sini akan dihasilkan daftar rekomendasi kontrol.

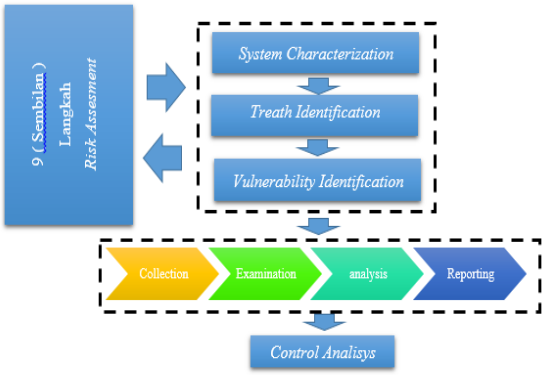
Langkah 9 - Dokumentasi Hasil (*Results Documentation), merupakan laporan atau dokumentasi hasil dari seluruh kegiatan yang telah dilakukan, dari langkah 1 - 8.

3.3 Simulasi Kasus

Terdapat 9 (Sembilan) tahapan didalam *Framework NIST*, posisi tahap ke 2, ke 3 dan ke 4 menjadi titik rawan berlangsungnya ancaman risiko yang muncul dari sebuah sistem informasi.

Tahap ke 2 adalah tentang identifikasi ancaman (*Threat Identification*), pada tahap ini diketahui ancaman apa saja yang akan menggangu system. Pada tahap ini juga akan mengenali berbagai sumber gangguan yang akan terjadi pada sistem. *Input* dari proses ini berupa daftar gangguan yang pernah terjadi dan yang akan terjadi, data dari berbagai pihak. *Output* dari tahap ini berupa daftar risiko risiko yang kemungkinan terjadi serta sumber risiko yang dapat menimbulkan kerentanan.

Tahap ke 3 tentang *Vulnerability Identification* yang merupakan step 3 dari 9 step *Framework NIST* SP 800-30 menjadi sangat penting untuk mengidentifikasi adanya risiko ancaman dari kerentanan sistem. *Input* langkah ini berupa laporan dari penilaian risiko terdahulu, atau serangan yang pernah terjadi, serta hasil pengecekan/pengetesan sistem. *Output* dari proses ini adalah *list vulnerability* atau kerentanan yang mungkin dan telah terjadi. Gambaran penanganan alur kasus yang nantinya untuk bahan masukan pada Langkah 4.



Gambar 3.1 Alur Penanganan *Vulnerability Identification* pada pembuatan Peta Digital

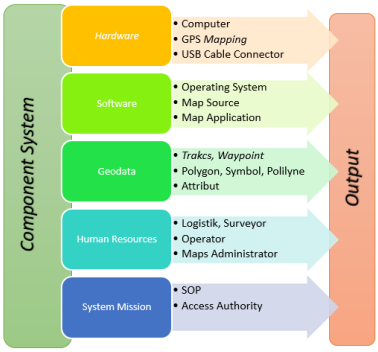
Tahap ke 4 merupakan tahap kontrol adanya ancaman risiko dan menjadi rekomendasi terhadap penentuan kemungkinan munculnya risiko.

4. IMPLEMENTASI PEMBUATAN PETA DIGITAL

4.1 Proses Implementasi

1) Karakter Sistem (*System Characterization*)

Pada tahap melihat kebutuhan system untuk pencetakan peta digital. Inisiasi dikategorikan dalam kelompok *hardware*, *software*, *interface*, Geodata, *Human Resource*, *System Mission. Output* dari step ini akan menjadi masukan pada step berikutnya



Gambar 4.1 *Step Process System Characterization*

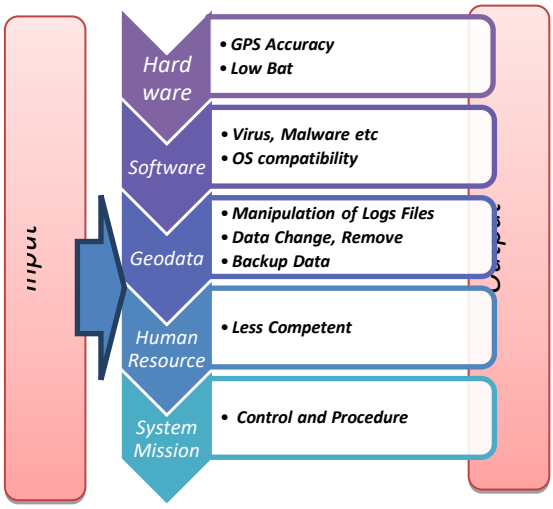
2) Identifikasi Ancaman (*Threat Identification*)

Hasil observasi di lapangan, teridentifikasi ancaman yang ada adalah penggunaan system OS yang terbatas pada Windows series , akurasi *data survey* yang *lost tolerance*, sumber daya yang melemah pada saat *survey* dilapangan jadi ancaman terhadap penerimaan data dari satelit yang bisa *lost tolerance*. Tidak adanya alarm pada saat baterai lemah, file peta digital yang mudah diubah. Tabel berikut menunjukan aspek karakter system dan ancaman yang ditimbulkan.

Tabel 4.1 Ancaman yang muncul dari karakter system.

Karakter Sistem			Ancaman	Keterangan
Hardware	Komputer GPS Maps Kabel USB Konektor		Akurasi GPS Maps, Baterai lemah	Lemahnya baterai selama initidak di ikuti dengan alarm pemberitahuan
Software	Operating System Map Source Maps Application		Windows Series	Aplikasi akuisisi data saat ini hanya bisa berjalan di OS Windows
Geodata	*Spacial*	*Waypoints Tracks*	File Digital yag mudah dirubah, dicuri, digandakan , bakup	-
	Tabular	*Longitude , Latitude*		
Human Resources	Kurang Kompetent		Kualitas peta digital	-
ystem mission	Aturan dan prosedur		Proses dan tanggung jawab kerja yang tumpang tindih	-

Pada table 4.1 dan gambar 4.2 menjelaskan tentang munculnya ancaman dari masing masing aspek yaitu , hardware dengan ancaman akurasi GPS, baterai lemah , software dengan ancaman virus , malware , OS hanya windows, dari sisi data adalah mudahnya dirubah menyebabkan data mudah di manipulasi, dihapus , bakup data, dari factor sumber

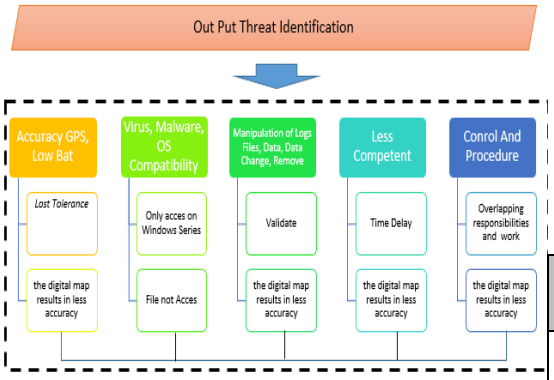


daya manusia adalah kurang kompeten dan yang terakir adalah dari sisi *system mission* belum ada aturan control prosedur.

Gambar 4.2 Jenis dan Sumber Ancaman

3) Identifikasi Kerentanan (*Vulnerability Identification)*

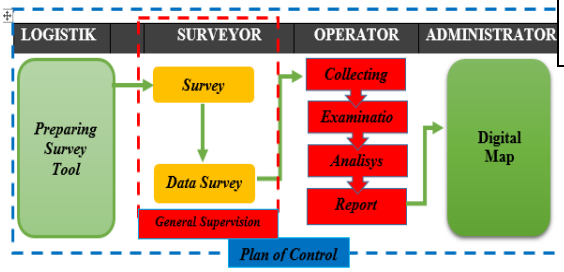
Kerentanan pada step ini adalah *output* dari *step 2*, dampaknya data *survey* tidak akurat, mudah di manipulasi, terhapus, digandakan dan file mudah di akses oleh siapa saja untuk tujuan tertentu.



Gambar 4.3 Identifikasi Kerentanan Proses

4) Analisa Kontrol (*Control Analisys)*

Gambar 4.4 memperlihatkan proses aktivitas penanganan ancaman risiko tiap bagian.

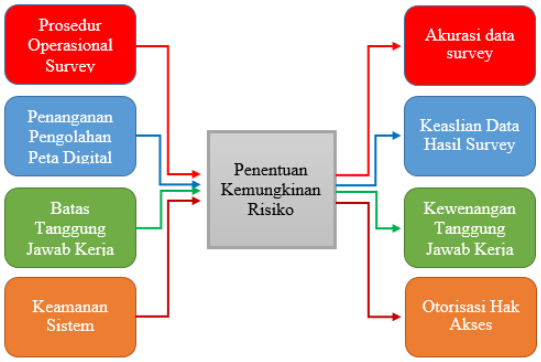


Gambar 4.4 *Control Activity* Pembuatan Peta Digital

Analisa dimulai dari mempersiapkan penggunaan alat, melakukan *survey* kemudian menyerahkan hasil *survey* ke bagian operator yang kemudian dianalisa dengan proses *collecting*, *examination*, *analisys*, *report* hasil report berupa data peta digital yang siap untuk dicetak.

5) . Penentuan Kemungkinan Risiko (*Likelihood Determination)*

Analisa kontrol yang memungkinkan dapat digunakan untuk penilaian risiko meliputi : 1. Prosedur operasional *survey*, 2. Penanganan pengolahan peta digital. 3. Batasan Tanggung jawab kerja. 4. Manajemen penangan system keamanan peta digital. Berdasarkan analisa kontrol tersebut, maka potensi ancaman yang bisa dieksploitasi menjadi sumber risiko adalah: 1. Akurasi data *survey*, 2. Keaslian data hasil *survey*, 3. Kewenangan tanggung jawab kerja, 4. Otorisasi hak akses.



Gambar 4.5 Penentuan Kemungkinan Risiko Pembuatan Peta Digital

6) Analisa Dampak (*Impact Analysis)*

Dampaknya dapat dilihat di tabel berikut :

Tabel 4.2 Dampak Risiko

Tipe Risiko	Skor Kemungkinan Ancaman	Skor Dampak	Skor Risiko	Predikat Level Rangking
Low Bat	1.0 (High)	100 (High)	100	High
Lost Tolerance	1.0 (High)	100 (High)	100	High
Otorisasi Hak Akses	1.0 (High)	100 (High)	100	High
Backup Data	0.5 (*Medium*)	50 (*Medium*)	25	*Medium*
Prosedur pengolahan data	0.5 (*Medium*)	50 (*Medium*)	25	*Medium*
Sumber Daya Manusia	0.1 (*Low)*	10 (*Medium*)	10	*Low*

Jenis Risiko	Dampak	Nilai Dampak
Low Bat	Kesalahan posisi koordinat	*High*
Lost Tolerance	Posisi koordinat berubah	*High*
Otorisasi Hak Akses	Rentan terhadap penggandaan file dan perubahan isinya oleh yang tidak berhak	*High*
Backup Data	Melakukan *survey* ulang jika file nya rusak atau hilang	*Medium*
Prosedur pengolahan data	Belum ada pembagian tanggung jawab pekerjaan hasil pekerjaan	*High*
Sumbe Daya Manusia	Tidak ada batasan tanggung jawab antar bagian	*Low*

7) Penentuan Risiko (*Risk Determination)*

Penilaian ini untuk mengukur tingkat risiko terhadap sistem, hal ini mengacu pada kemungkinan risiko dan dampak risiko yang telah ditentukan

Tabel 4.3 Besaran Definisi Dampak

8) Rekomendasi Kontrol (*Control Recommendation)*

Rekomendasi kontrol dapat dilihat pada tabel berikut ini:

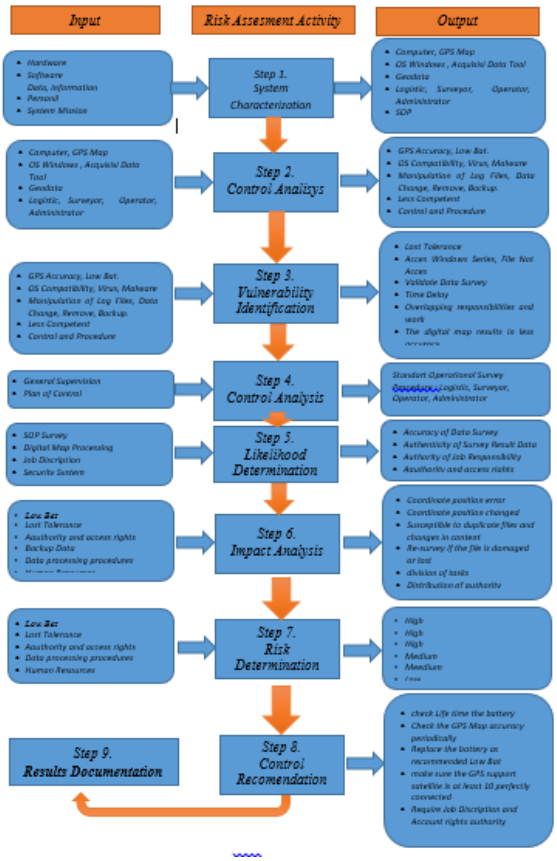
Tabel 4.4 Rekomendasi Kontrol

Jenis Risiko	Tingkat Risiko	Rekomendasi

Low Bat	*High*	Hitung masa hidup baterai jenis alkaline dari berbagai merek sehingga prediksi penggantian baterai dapat dilakukan
Lost Tolerance	*High*	1. Cek akurasi toleran GPS *Map* secara berkala 2. Ganti baterai sesuai rekomendasi *Low Bat* 3. Sebelum *survey* pastikan satelit pendukung GPS minimal 10 yang terkoneksi secara sempurna
Otorisasi Hak akses	*High*	1. Perlu adanya Job Discription 2. Akun yang mengatur hak otoritas

9) Dokumentasi Hasil (*Documentation Result)*

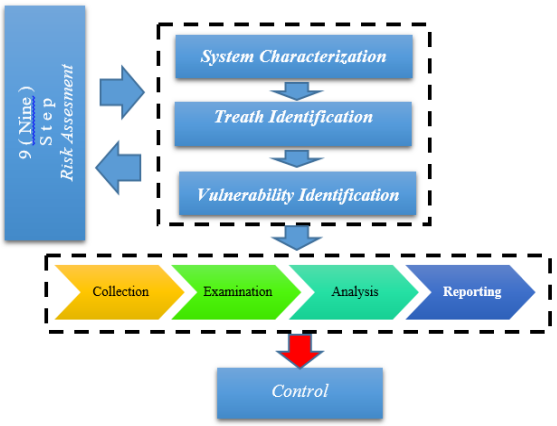
Tahap ini merupakan akhir dari *Risk Assesment* yang mendokumentasikan hasil dari penilaian risiko yang berupa profil risiko yang dapat mengancam keberlangsungan system proses pembuatan peta digital. Gambar 4.5 mendokumentasikan penanganan ancaman risiko serta rekomendasi penentuan kerentanan dan cara penanganan pembuatan peta digital. Dokumen hasil analisis mulai dari tahap 1 sampai tahap 8 menjadi profil penanganan pembuatan peta digital.



Gambar 4.6 ***Profile Digital Map With Framework NIST***

4.2 Analisis Ancaman Risiko dan Kerentanan

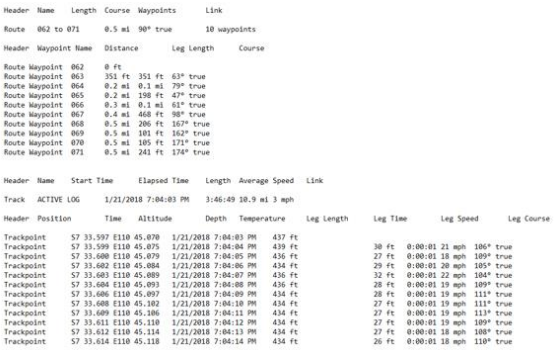
Pada tahap ini dilakukan analisa *survey* data *On location* dan *Fake Location.* Hasil dari analisa tersebut terlihat di gambar 4.9, dan dalam Tabel 4.5



Gambar 4.7 ***Vulnerability Identification Process***

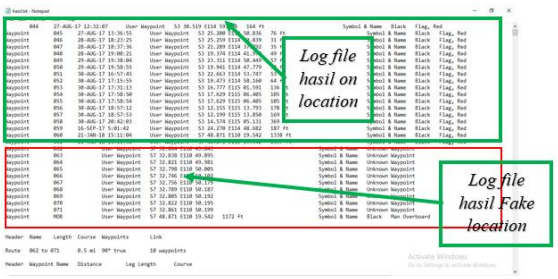
Pada gambar 4.5 memperlihatkan bagaimana ancaman muncul dan bagaimana menangani ancaman risiko. Berikut ini uraian gambar 4.5 :

1) Collection, proses pengumpulan data *survey*

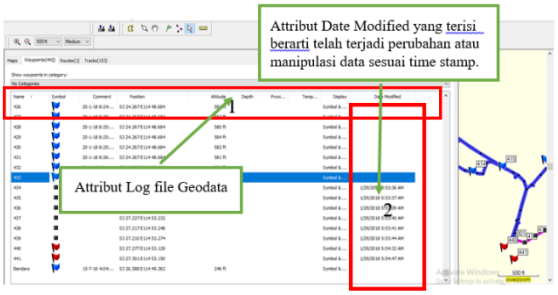


Gambar 4.8 Data ***Route waypoint*** **dan** ***Trackpoint***

2) ***Examination and Analisys,*** ditemukan pola pada data hasil *survey* lapangan (O*n Location)* dan yang tidak turun kelapangan (*Fake Location)*



Gambar 4.9 Identifikasi data yang pada ***log file waypoint***



Gambar 4.10 *Log file* Data *Survey* yang di Edit

Gambar 4.10 menunjukan properties *Tracks* dan *waypoint*. **Kotak merah 1** adalah atribut dari *trakcs* dan *waypoint*. "Kotak Merah 2 " pada attribute " Date Modified " terdapat rekod yang terisi *time stamp* artinya pada rekod tersebut telah terjadi perubahan. Jadi disimpulkan rekod hasil *survey* tidak valid**.**

3) *Reporting*, hasil dari pemeriksaan terhadap hasil *survey* maka dapat di sampaikan sebagai berikut,

Tabel 4.5 Laporan hasil identifikasi

No	Attribut	On Location	Fake
1	*Date Modified*	*Not Found*	*Found*
2	*Show Profile*	Aktif	Tidak Aktif
3	*Vertical Profile*	Ada	Not *Found*
4	*Properties*	*Tracks Properties*	*Route Properties*
5	Pada perbedaan pada type data	Sesuai dengan type data yg ada	Text semua

Tabel 4.6 Hasil Identifkasi Perbandingan attribut Data *survey* *On Location* dan *Fake Location*

No	Attribut	On Location	Fake
1	*Date Modified*	Not Found	Found
2	*Show Profile*	Active	Not Found
3	*Vertical Profile*	Found	Not Found
4	*Properties*	*Tracks Properties*	*Route Properties*

4.3 Analisa

Analisa dari hasil uji coba dan pengujian yang telah dilakukan menggunakan standart matrik pada tahapan *framework NIST*, dapat uraikan sebagai berikut, tahapan ini terbagi menjadi 4 (empat) bagian dimana tahap identifikasi terhadap ancaman risiko berada pada tahap 1- 4. Sedangkan tahap 5-7 adalah penentuan dari kerentanan akibat adanya ancaman risiko tersebut. Pada tahap tahap ini juga ditentukan bobot dampak risiko yang mengancam hasil dari pencetakan kualitas peta digital. Tahap 8 adalah rekomendasi dari hasil dari pelaksanaan tahap 1-7 dan tahp 9 adalah tahap pendokumentasian hasil.

Penerapan *Framework NIST SP 800-30* dalam penanganan proses system pembuatan peta digital terbukti mampu mengidentifikasi ancaman risiko dan mengidentifikasi kerentanan yang terjadi. Kesimpulan itu di kemukakan setelah dilakukan uji coba penerapan *Risk Assesment* dari *Framework NIST SP 800-30* yang dilakukan tahap demi tahap dan menghasilkan fakta fakta adanya ancaman risiko dimana uraiannya telah dibahas di tahap 1 – 4, hasil dari pembahasan tersebut telah menjawab rumusan masalah yang ada yaitu "Bagaimana detail identifikasi ancaman dan kerentanan pada geodata". Selain itu juga uraian bahasan pada tahap 5 – 7 telah menjawab rumusan masalah tentang "Bagaimana detail identifikasi ancaman dan kerentanan pada geodata".

Mengacu pada peneilitan sebelum yang terlihat pada *literature review* bahwa *Framework* telah terbukti membantu dalam mengatasi masalah masalah sitem informasi sesuai dengan kontek *framework* dan masalahnya, dengan adanya *framework* dapat mengurangi ancaman risiko dan kerentanan, memudahkan dalam mendeteksi kelemahan system, mendapatkan solusi atas kelemahan dan kerentanan sistem tersebut

5. KESIMPULAN

Framework NIST Special Publication 800- 30 dalam menilai step step pembuatan peta digital sesuai 9 step, terbukti mampu menguraikan profil ancaman risiko yang berpotensi dan sudah mengganggu pelaksanaan system pembuatan peta digital, memberi mitigasi risiko sebagai solusi tindakan peringanan risiko dan pengawasanya dengan mengevaluasi pelaksanaan manajemen risiko secara menyeluruh.

Penerapan *framework NIST* dapat dijadikan profile dalam rangka menilai kegiatan pembuatan peta digital. Ancaman risiko dan kerentanan mudah teridentifikasi karena adanya profile yang telah bangun ini

DAFTAR PUSTAKA

DARYONO, B. S. (2017). Pengembangan Pelaporan Framework Cyber Crime. *JISKa*, *Vol 1 No.*, 133–147. Retrieved from https://www.researchgate.net/publication/316510836_PENGEMBANGAN_FRAMEWORK_PELAPORAN_CYBER_CRIMEFRAMEWORK_PELAPORAN_CYBER_CRIME

FABIAN BUSTAMANTE, WALTER FUERTES, PAUL DIAZ, T. T. (2017). Methodology for Management of Information Security in Industrial Control Systems: A Proof of Concept aligned with EnterpriseObjectives. *Advances in Science, Technology and Engineering Systems Journal*, *Vol. 2*, *No*, 88–99. Retrieved from https://www.researchgate.net/publication/317138094_Methodology_for_Management_of_Information_Security_in_In-

dustrial_Control_Systems_A_Proof_of_Concept_aligned_with_Enterprise_Objectives

GUNTUR BAGUS PAMUNGKAS, BAMBANG SUDARSONO, S. K. (2014). Verifikasi Batas Wilayah Antara Kabupaten Sukoharjo Dan Kabupaten Karang Anyar. *Jurnal Geodesi Undip*, *Volume 3*,(Permasalahan Batas Daerah), 14–24.

IBNU, Z. (2013). Rancang Bangun Pelacak Lokasi Dengan Teknologi GPS. *Teknomatika*, *Vol. 3 No.*(Pelacakan Lokasi Kejahatan dengan GPS).

J KIYOSHI. (2013). Investigating the Impact of Global Positioning System Evidence.

KRAMER, J. (2013). *No DroidSpotter: A forensic tool for Android location data collection and analysis*. IOWA State Univercyti.

LAST DAVID. (2014). GPS Forensics, Crime and Jamming, (GPSJamming).

LESTARI, U., & KRISTIYANA, S. (2013). Rancang Bangun Mobile Tracking Application Module Untuk Pencarian Posisi Benda Bergerak Berbasis Short Massage Service (Sms). *Seminar Nasional Teknologi Informasi Dan Komputasi (SENASTIK 2013)*, 30–31.

NURDIATI SRI, BARUS BABA, P. D. (2015). Pengembangan Sistem Informasi Geografis Tindak Kejahatan Multilevel berbasis Web. Retrieved from http://download.portalgaruda.org/article.php?article=85662&val=235

PRAHASTA, E. (2009). *Sistem InformasiGeografis Konsep-Konsep Dasar* (Cetakan Pe). Bandung: Informatika.

PRAYUDI YUDI, S. S. (2014). Analisis Bukti Digital Global Positioning System (GPS) Pada Smartphone Android. *Konferensi Nasional Sistem Dan Informatika (KNS&I) 2014*, (bukti digital GPS).

PURBO ONNO W. (2017). Framework Cybersecurity. Retrieved January 13, 2018, from http://lms.onnocenter.or.id/wiki/index.php/Framework_Cybersecurity

STONEBURNER GARY , GOGUEN ALICE, AND F. A. (2002). Risk Management Guide for Information Technology Systems. *Cumputer Security*, (Reports on Computer System Technology). Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/admi*NIST*rative/securityrule/*NIST*800-30.pdf

UCU NUGRAHA. (2016). Manajemen Risiko Sistem Informasi Pada Perguruan Perguruan Tinggi Menggunakan Kerangka Kerja *NIST* SP 800-300. *Seminar Nasional Telekomunikasi Dan Informatika (SELISIK 2016)*, 2503–2844.

WIDYANTARA, I. M. O., AGUS, I. G., & WARMAYANA, K. (2015). Penerapan Teknologi GPS Tracker Untuk Identifikasi Kondisi Traffik Jalan Raya, *14*(1), 31–35.