Terakreditasi SINTA Peringkat 4
Surat Keputusan Direktur Jenderal Pendidikan Tinggi, Riset, dan Teknologi, Nomor: 158/E/KPT/2021
masa berlaku mulai Volume 5 Nomor 2 Tahun 2018 sampai Volume 10 Nomor 1 Tahun 2023

Terbit online pada laman web jurnal: **https://jurnal.plb.ac.id/index.php/tematik/index**

T E M A T I K
Jurnal **Teknologi Informasi Komunikasi (e-Journal)**
Vol. 10 No. 2 (2023) 216 - 226 ISSN Media Elektronik: 2443-3640

Smart Security Risk Management pada Bali Smart Island menggunakan OSINT, OTGv4.2, dan ISO 31000:2018

Smart Security Risk Management at Bali Smart Island Using OSINT, OTGv4.2, and ISO 31000:2018

I Putu Agus Eka Pratama
[1]Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana
[1]eka.pratama@unud.ac.id

Abstract

The integration of web-based services and information on Bali Smart Island, on the one hand, provides convenience, but on the other hand raises issues of threats and risks related to system, data, and information security. Current security testing only uses OWASP and OSINT but is not accompanied by risk assessment and risk management. This research conducted security testing on the Bali Smart Island domain using a combination of OSINT and OWASP Testing Guide (OTGv4.2) accompanied by ISO 31000:208 risk assessment and risk management. The research uses experimental methodology with Proof of Concept (PoC) using the Harvester tool in the target domain. The test results measure the level of risk, accompanied by recommendations. The final results of the research show that the combination of OSINT, OTGv4.2, and ISO 31000:2018, can provide the best and most effective solution for information technology security risk management guidelines on the Bali Smart Island, through security testing, assessing security test results, evaluation, and providing recommendations post-evaluation system improvements. In the future, this research can be continued by using a combination of other tools and methods for web security.

Keywords: ISO 31000:2018, OWASP Testing Guide version 4.2 (OTGv4.2), risk management, risk assessment, web security.

Abstrak

Integrasi layanan dan informasi berbasis web pada Bali Smart Island, di satu sisi memberikan kemudahan, namun di sisi lain menimbulkan isu ancaman dan risiko terkait dengan keamanan sistem, data, dan informasi. Pengujian keamanan saat ini hanya menggunakan OWASP dan OSINT namun belum disertai dengan risk assesment dan risk management. Penelitian ini melakukan pengujian keamanan pada domain Bali Smart Island menggunakan kombinasi OSINT dan OWASP Testing Guide (OTGv4.2) disertai dengan risk assesment dan risk management ISO 31000:208. Penelitian menggunakan metodologi eksperimental dengan Proof of Concept (PoC) menggunakan tool Harvester pada domain target. Hasil-hasil pengujian diukur tingkat risiko di dalamnya disertai dengan pemberian rekomendasi. Hasil akhir penelitian menunjukkan bahwa kombinasi OSINT, OTGv4.2, dan ISO 31000:2018, mampu memberikan solusi terbaik dan efektif untuk pedoman manajemen risiko keamanan teknologi informasi pada Bali Smart Island, melalui pengujian keamanan, penilaian hasil pengujian keamanan, evaluasi, dan pemberian rekomendasi perbaikan sistem pasca evaluasi. Ke depannya penelitian ini dapat dilanjutkan dengan penggunaan kombinasi tool dan metode lainnya pada web security.

Katakunci: ISO 31000:2018, OWASP Testing Guide version 4.2 (OTGv4.2), risk management, risk assessment, web security.

1. Pendahuluan

Smart City (kota pintar) merujuk kepada konsep kota atau daerah untuk menyelesaikan permasalahan yang terjadi maupun untuk mengelola potensi-potensi yang terdapat pada kota atau daerah tersebut berbasiskan teknologi informasi[1]. Smart City telah banyak diterapkan di seluruh dunia, termasuk juga pada sejumlah kota dan daerah di Indonesia. Di Indonesia, gerakan 100 kota Smart City telah dicanangkan per tahun 2017 oleh pemerintah (melalui Kementerian Komunikasi dan Informatika Republik Indonesia) pada sejumlah kota dan daerah, salah satunya di Provinsi Bali[2].

Pemerintah Provinsi Bali menerapkan Smart City dalam bentuk Bali Smart Island. Teknologi Informasi (TI) berperan penting di dalam mewujudkan proses

Diterima Redaksi: 18-10-2023 | Selesai Revisi: 07-12-2023 | Diterbitkan Online: 07-12-2023

integrasi data dan layanan, penyediaan data dan informasi, serta penyediaan layanan publik kepada masyarakat secara lebih baik melalui program Smart City. Salah satu media digital yang digunakan oleh Pemerintah Provinsi Bali di dalam mewujudkan program Bali Smart Island melalui penyediaan layanan berbasis TI adalah berupa website pada domain https://baliprov.go.id[3].

Penyediaan layanan publik terintegrasi berbasis web, memberikan kemudahan akses bagi masyarakat dan kemudahan pengelolaan bagi Pemerintah Provinsi Bali. Namun terdapat sejumlah risiko yang harus diketahui dan dikelola dengan baik oleh pihak Pemerintah Provinsi Bali.

Berbicara mengenai risiko maka perlu untuk diketahui mengenai definisi risiko. Risiko (risk) merupakan peluang (probabilitas) dan kemungkinan terjadinya hal-hal yang tidak dapat diprediksi terkait dengan ketidakpastian akan sesuatu yang mungkin terjadi di masa depan[4]. Dengan demikian, sebuah risiko harus dihindari dan dicegah sejak awal.

Untuk mencegah terjadinya risiko, maka perlu dilakukan manajemen risiko (risk management). Manajemen risiko memerlukan adanya pengendalian internal, evaluasi, dan hasil evaluasi terhadap proses dan kegiatan yang dilakukan oleh organisasi, untuk mencegah timbulnya kerugian finansial dan non finansial[5].

Risiko dan manajemen risiko juga dapat terjadi pada organisasi dan instansi yang menerapkan teknologi informasi di dalamnya. Salah satunya adalah sejumlah risiko yang berkaitan dengan keamanan sistem, data, dan informasi. Dengan demikian, di dalam mewujudkan Bali Smart Island dengan menggunakan teknologi informasi di dalamnya, juga perlu dilakukan manajemen risiko.

Untuk itu, pada penelitian ini, dilakukan pengujian keamanan sistem, data, dan informasi pada domain website Pemerintah Provinsi Bali yang digunakan untuk mewujudkan Bali Smart Island, diikuti dengan pengukuran dan penilaian risiko serta penyusunan dan pemberian rekomendasi perbaikan pasca pengukuran tingkat risiko. Hasil akhir penelitian, diharapkan dapat membantu pihak Pemerintah Provinsi Bali di dalam mewujudkan Bali Smart Island yang lebih baik serta peningkatan kualitas layanan publik berbasis teknologi informasi.

Usulan solusi pada penelitian ini adalah smart security risk management menggunakan metode Open Source Intelligence (OSINT), untuk mengumpulkan informasi mengenai domain target (information gathering) sesuai dengan aturan pada OWASP Testing Guide versi 4.2[6]. Proof of Concept (PoC) dilakukan dengan menggunakan tool OSINT Harvester pada sistem operasi Linux Ubuntu[7]. Selain itu, pada information gathering, juga dilakukan reconnaissance untuk mengumpulkan data-data penting terkait dengan domain target[8][9]. Hasil dari information gathering, digunakan untuk melakukan penilaian dan pengukuran tingkat risiko keamanan sistem sesuai dengan framework ISO 31000:2018, serta penyusunan dan pemberian rekomendasi perbaikan.

Rumusan masalah dalam bentuk pertanyaan penelitian berikut: 1.) Bagaimana cara melakukan information gathering pada domain target sesuai pedoman OTGv4.2 menggunakan tool OSINT Harvester? 2.) Bagaimana cara melakukan penilaian risiko berdasarkan hasil information gathering? 3.)Bagaimana cara menyusun rekomendasi perbaikan pasca penilaian risiko?

Tiga batasan masalah pada penelitian ini, yaitu 1.)Penelitian hanya fokus menggunakan framework ISO 31000:2018 untuk penilaian risiko, 2.)Penelitian hanya menggunakan metode OSINT, pedoman OTGv4.2, dan tool OSINT Harvester untuk melakukan information gathering pada domain target, 3.)Studi kasus penelitian hanya fokus pada domain web Pemerintah Provinsi Bali (https://baliprov.go.id) yang menyediakan layanan publik terintegrasi.

Terdapat sepuluh penelitian sebelumnya yang menjadi state of the art pada penelitian ini. Penelitian pertama menjelaskan mengenai peranan kecerdasan buatan (Artificial Intelligence), khususnya Artificial Neural Network, pada bentuk keamanan Smart City di bagian Smart Government, ditinjau dari sisi pemanfaatan software dan risikonya[10]. Penelitian kedua menguraikan tentang prinsip-prinsip dasar di dalam membangun sebuah sistem perlindungan keamanan digital pada Smart City, meliputi: perangkat, kontrol akses, integritas data, dan segmentasi Smart Network, serta upaya-upaya pencegahan dari ancaman serangan oleh attacker[11]. Penelitian ketiga menjelaskan mengenai adanya berbagai kemungkinan Smart Service pada Smart City dengan menggunakan pendekatan adaptasi arsitektur berbasis microservice, dengan mempertimbangkan sisi keamanan dan privasi[12]. Penelitian keempat memaparkan tentang hasil analisa terhadap syarat-syarat penilaian risiko keamanan informasi pada Smart City serta model penilaian risiko keamanan informasi pada Smart City dengan menggunakan algoritma Decision Tree[13].

Penelitian kelima mengemukakan pendekatan di sisi pengguna berbasiskan kepada reputasi dan kepercayaan publik, untuk melakukan penilaian terhadap permasalahan, tantangan, ancaman keamanan, dan potensi di masa depan dari implementasi Internet of Things (IoT) pada Smart City[14]. Penelitian keenam menguraikan tentang Application Security Control (ASC) pada Smart City, yang meliputi identifikasi, otomatisasi, anotasi, dan pelacakan, terkait manajemen aset-aset TI, ketersediaan layanan (availability), integritas, serta kehandalan layanan (reliability) pada jaringan

DOI: https://doi.org/10.38204/tematik.v10i2.1559

komputer dan lingkungan Cloud Computing[15]. Penelitian ketujuh mengemukakan tentang perancangan desain dan pengembangan aplikasi web untuk mendukung Smart City dengan mengikuti pedoman pada Open Web Application Security Project (OWASP) dengan mempertimbangkan bahwa keamanan web merupakan fokus utama bagi instansi atau organisasi di dalam penyediaan layanan publik[16]. Penelitian kedelapan menguraikan tentang pengujian keamanan sistem pada website Perusahaan X menggunakan pedoman OWASP dengan metode GET dan POST, di mana hasil pengujian menunjukkan bahwa keamanan website Perusahaan X perlu diperbaiki dan ke depannya perlu dilakukan manajemen risiko[17]. Penelitian kesembilan mengadopsi Scottish Smart City Maturity Model dengan menggunakan pendekatan kualitatif berupa teknik wawancara, observasi, dan analisis dokumen, untuk melakukan perhitungan bobot di dalam menentukan nilai penting dari dimensi-dimensi pada smart government, dengan menggunakan metode Entropy pada studi kasus implementasi Depok Smart City di Indonesia[18]. Penelitian kesepuluh menguraikan tentang risiko-risiko pada implementasi Smart Lighting di Kota Semarang terkait dengan Smart City[19].

Tabel 1. menunjukkan ringkasan hasil penelitian dari kesepuluh penelitian sebelumnya (state of the art) beserta dengan kaitannya terhadap penelitian ini:

Tabel 1.Ringkasan Penelitian Sebelumnya (State of the Art)

Paper	Ringkasan Hasil Penelitian	Kontribusi terhadap Penelitian
[10]	Penelitian ini menguraikan peranan Artificial Neural Network pada keamanan Smart Government dari sisi pemanfaatan software dan risikonya.	Penelitian ini memberikan kontribusi peranan TI (AI) pada Smart City serta sejumlah risikonya.
[11]	Penelitian ini menguraikan prinsip-prinsip dasar sistem keamanan digital pada Smart City (perangkat, kontrol akses, integritas data, segmentasi Smart Network) beserta upaya pencegahan dari ancaman serangan siber	Penelitian ini memberikan kontribusi berupa gambaran prinsip dasar keamanan digital pada Smart City beserta sejumlah jenis serangan siber di dalamnya
[12]	Penelitian ini menguraikan beberapa Smart Service menggunakan pendekatan adaptasi arsitektur microservice, dengan mempertimbangkan keamanan dan privasi	Penelitian ini memberikan kontribusi tentang Smart Service pada Smart City berbasis Microservice beserta keamanan dan privasi
[13]	Penelitian ini memaparkan analisa prasyarat penilaian risiko keamanan informasi pada Smart City beserta model penilaian risiko menggunakan algoritma Decision Tree	Penelitian ini memberikan kontribusi model penilaian risiko keamanan informasi pada Smart City berbasis Decision Tree
[14]	Penelitian ini menjelaskan pendekatan di sisi pengguna berbasis reputasi dan kepercayaan publik untuk penilaian terhadap ancaman keamanan pada Internet of Things (IoT) di Smart City	Penelitian ini memberikan kontribusi pendekatan yang dipakai terkait keamanan IoT pada Smart City
[15]	Penelitian ini menguraikan tentang Application Security Control (ASC) pada Smart City terkait manajemen aset TI, availability, integritas, dan reliability pada jaringan komputer dan Cloud Computing	Penelitian ini memberikan kontribusi dari sisi ASC pada Smart City dan Cloud Computing
[16]	Penelitian ini membahas tentang rancang bangun web Smart City berbasis Open Web Application Security Project (OWASP) untuk keamanan di dalam penyediaan layanan publik	Penelitian ini memberikan kontribusi metode OWASP dan OTG untuk keamanan website pada Smart City
[17]	Penelitian ini menguraikan tentang pengujian keamanan sistem pada website OWASP dengan metode GET dan POST serta manajemen risiko	Penelitian ini memberikan kontribusi tambahan dari sisi metode GET-POST dan manajemen risiko selain OWASP
[18]	Penelitian ini menguraikan adopsi Scottish Smart City Maturity Model (SSCMM) menggunakan pendekatan kualitatif untuk perhitungan bobot dan nilai penting dari dimensi pada Smart Government menggunakan Metode Entropy	Penelitian ini memberikan kontribusi metode SSCMM dan Entropy pada Smart Government
[19]	Penelitian ini menguraikan risiko-risiko pada implementasi Smart Lighting	Penelitian ini memberikan kontribusi risiko pada Smart Lighting

Dari kesepuluh penelitian tersebut, belum ada satupun penelitian yang menggunakan kombinasi OSINT, OTGv4.2, dan ISO 31000:2018 untuk melakukan security risk management dan risk assesment pada studi kasus tertentu. Penelitian ini menjadi penelitian pertama yang mengkombinasikan OSINT, OTGv4.2, dan ISO 31000:2018 untuk melakukan security risk management dan risk assesment pada studi kasus Bali Smart Island, disertai dengan penyusunan rekomendasi perbaikan.

2. Metode Penelitian

2.1. Alat dan Bahan

Di dalam penelitian ini, digunakan sejumlah software dan hardware pendukung. Hardware yang digunakan adalah notebook Dell dengan spesifikasi Dell Latitude E6440 (Intel i7-4610M (4) @ 3.700GHz, RAM 16GB). Untuk software digunakan sistem operasi Linux Ubuntu 20.04 LTS 64 bit, the Harvester 3.2.4, dan Python 3.9.5. Pemilihan sistem operasi Linux Ubuntu di dalam penelitian ini, bertujuan untuk memudahkan proses implementasi dan pengujian memanfaatkan repositori online dan kehandalan sistem

DOI: https://doi.org/10.38204/tematik.v10i2.1559

selama pengujian berlangsung. The Harvester memiliki nilai lebih dari sisi open source serta kemudahan instalasi berbasis repositori online dari GitHub dan penggunaan dari Terminal pada sistem operasi Linux Ubuntu. Penelitian dilakukan secara mandiri di masa pandemi Covid19 secara remote dan online melalui internet pada kurun waktu 2021-2022.

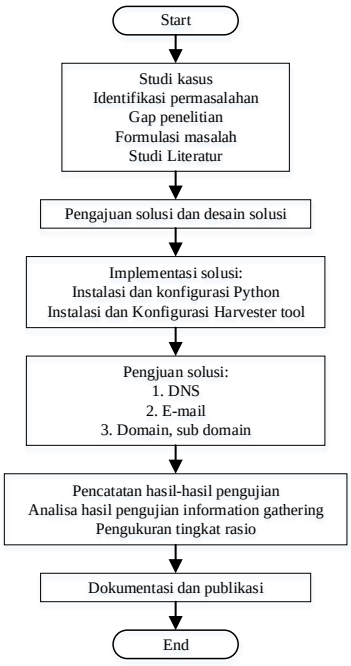
2.2 Metode Penelitian Kualitatif

Metode penelitian yang digunakan di dalam penelitian adalah metode penelitian kualitatif. Metode penelitian kualitatif pada penelitian ini menggunakan pendekatan studi kasus, di mana studi kasus yang diangkat adalah mengenai keamanan sistem, data, informasi, dan layanan terintegrasi Pemerintah Provinsi Bali pada domain Bali Smart Island di https://baliprov.go.id. Metode penelitian kualitatif studi kasus pada penelitian ini, memiliki karakteristik utama berupa penekanan solusi yang dapat diberikan terkait dengan kasus atau permasalahan pada ruang lingkup atau lokasi studi kasus penelitian terjadi (dalam hal ini domain Bali Smart Island).

Domain https://baliprov.go.id menjadi salah satu media untuk mewujudkan program Bali Smart Island secara online dan terintegrasi oleh Pemerintah Provinsi Bali. Hasil pengujian keamanan digunakan untuk melakukan pengukuran tingkat risiko pada manajemen risiko serta penyusunan dan pemberian rekomendasi perbaikan.

2.3. Flowchart Penelitian

Flowchart penelitian merupakan bagan yang memuat urutan-urutan langkah yang dilakukan pada sebuah penelitian. Gambar 1. menunjukkan flowchart penelitian ini:



Gambar 1. Flowchart Penelitian

Berdasarkan Gambar 1., urutan langkah di dalam penelitian ini meliputi enam tahapan, yaitu: 1.)Tahap awal, 2.)Tahap implementasi, 3.)Tahap pengujian, 4.)Tahap analisa, 5.)Tahap pengambilan kesimpulan, dan 6.)Tahap akhir. Masing-masing tahapan memiliki proses tersendiri.

Pada tahap pertama, dilakukan pemilihan studi kasus permasalahan, Selanjutnya dilakukan identifikasi permasalahan dan formulasi permasalahan. Kemudian dilanjutkan dengan studi literatur dari sejumlah paper referensi untuk memperoleh gap penelitian. Kemudian dilakukan pengajuan usulan solusi terkait permasalahan yang diangkat, disertai dengan pertanyaan penelitian. Pada tahap implementasi, dilakukan implementasi terhadap usulan solusi yang diajukan, yaitu dengan melakukan instalasi dan konfigurasi python dan Harvester.

2.4. Metodologi Experimental

Metodologi yang digunakan di dalam penelitian ini adalah Metodologi Eksperimental. Metodologi eksperimental merupakan metodologi penelitian yang terdiri dari sembilan langkah, meliputi: 1.)Tinjauan pustaka, 2.)Perancangan solusi, 3.)Skenario pengujian, 4.)Implementasi, 5.)Pengujian, 6.)Analisis, 7.)Diskusi, 8.)Dokumentasi, dan 9.)Publikasi[20].

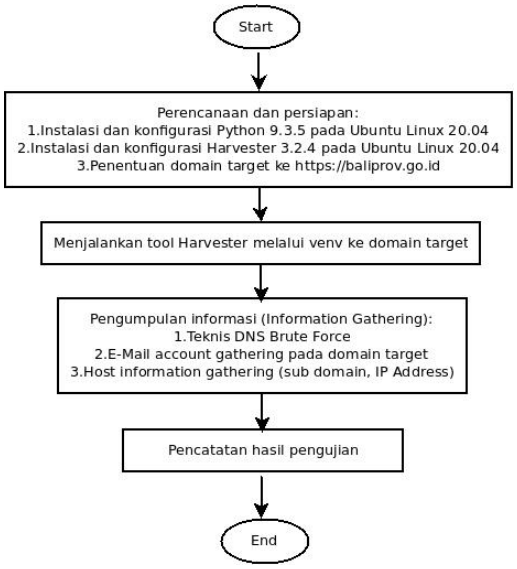
Pada tinjauan pustaka, digunakan sejumlah literatur dari paper pada jurnal ilmiah lima tahun ke belakang (2018-2023), buku referensi sepuluh tahun ke belakang (2013-2023), serta referensi dari website (resmi). Untuk perancangan solusi, dibuatkan workflow diagram dari penelitian serta flowchart penelitian. Untuk skenario pengujian digunakan pengujian di sisi peneliti menggunakan Black Box Testing melalui pengujian information gathering ke domain target menggunakan The Harvester. Untuk implementasi dan pengujian menggunakan Linux Ubuntu, The Harvester, pada jaringan internet ke domain target, kemudian hasilnya dicatat dan dianalisis. Pada diskusi dan dokumentasi, dilakukan pada penulisan paper penelitian ini. Terakhir dilakukan publikasi paper penelitian ini pada jurnal ilmiah.

2.5. Workflow Diagram

Workflow diagram menggambarkan alur kerja dan urutan langkah yang dilakukan di dalam penelitian. Pada penelitian ini, fokus utama adalah pada tahapan pengumpulan informasi (information gathering) terhadap domain target Bali Smart Island. Gambar 2. menunjukkan workflow diagram. Berdasarkan Gambar 2., pada tahapan perencanaan dan persiapan, dilakukan proses instalasi dan konfigurasi python pada sistem operasi Linux Ubuntu. Python diperlukan untuk menjalankan tool OSINT Harvester melalui venv python. Pada penelitian ini, digunakan python versi 3.9.5 pada sistem operasi Linux Ubuntu versi 20.04. Setelah python terkonfigurasi dengan baik, kemudian dilanjutkan dengan melakukan instalasi dan

DOI: https://doi.org/10.38204/tematik.v10i2.1559

konfigurasi tool OSINT Harvester pada sistem operasi Linux Ubuntu 20.04. Pada penelitian ini, digunakan Harvester versi 3.2.4.



Gambar 2. Workflow Diagram

Selanjutnya dilakukan penentuan target domain untuk proses information gathering. Pada penelitian ini, domain yang menjadi target adalah website Pemerintah Provinsi Bali pada URL https://baliprov.go.id. Information gathering dilakukan dengan tiga tahapan terurut.

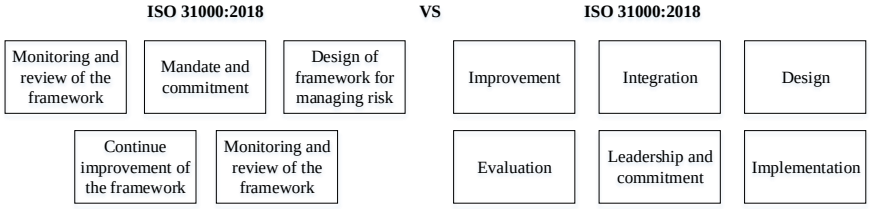
Pada tahapan pertama, dilakukan DNS Brute Force atau Recon DNS. Tahapan ini bertujuan untuk memastikan bahwa tidak terdapat pengecekan pada trafik DNS di domain target, sehingga dapat diperoleh sejumlah informasi penting mengenai enumerasi domain target, yang meliputi: a.)Reverse lookup domain, b.)NS record, c.)Zone transfer, d.)Enumerasi DNS Record (MX, SOA, NS, A, AAAA, SPF,TXT), e.)Top Level Domain (TLD), f.)Brute Force sub domain (domain dan wordlist), dan f.)IP Range (CIDR).

Pada tahapan kedua, dilakukan pengumpulan akun E-Mail yang menggunakan domain target. Pada tahapan ketiga, dilakukan pengumpulan informasi host target (sub domain dan IP Address). Data-data ini dikumpulkan untuk digunakan pada tahapan pengukuran dan penilaian tingkat risiko dengan menggunakan ISO 31000:2018, untuk kemudian dilakukan penyusunan dan pemberian rekomendasi.

2.6. Manajemen Risiko ISO 31000 (2009 dan 2018)

Manajemen risiko menggunakan standarisasi ISO 31000. Saat ini terdapat dua versi yang digunakan, yaitu tahun 2009 dan tahun 2018. Terdapat perbedaan signifikan antara ISO 31000:2018 (versi tahun 2018) dengan ISO 31000:2009 (versi tahun 2009), yaitu berupa enam prinsip berbeda pada kedua versi tersebut[21]. Gambar 3. menunjukkan bagan perbandingan kedua versi ISO 31000. Berdasarkan Gambar 3., pada ISO 31000:2009, terdapat lima prinsip manajemen risiko, yang meliputi: 1.)Monitoring and review of the framework, 2.)Mandate and commitment, 3.)Design of framework for managing risk, 4.)Continue improvement of the framework, 5.)Monitoring and review of the framework.

Sedangkan pada ISO 31000:2018, terdapat enam prinsip manajemen risiko, yang meliputi: 1.)Improvement, 2.Integration, 3.)Design, 4.)Evaluation, 5.)Leadership and commitment, 6.)Implementation. Pada penelitian ini, menggunakan standarisasi ISO 31000 tahun 2018 (ISO 31000:2018) dengan pertimbangan penilaian risiko yang lebih baik dan lebih detail.



Gambar 3. Bagan Perbandingan ISO 31000 2009 dan 2018

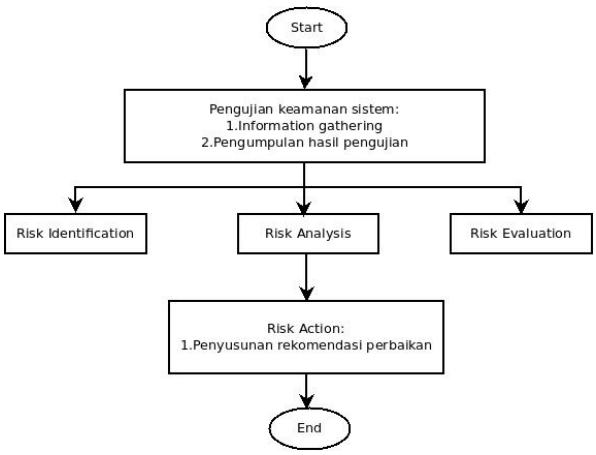
2.7. Flowchart Manajemen Risiko ISO 31000:2018

Urutan proses manajemen risiko pada penelitian ini, meliputi lima langkah, yaitu: 1.)Pengujian keamanan sistem (information gathering) dan pengumpulan hasil-hasil pengujian, 2.)Risk identification, 3.)Risk Analysis, 4.)Risk Evaluation, 5.)Risk Action berupa penyusunan rekomendasi perbaikan. Gambar 4. menunjukkan flowchart diagram dari manajemen risiko ISO 31000:2018.

Berdasarkan Gambar 4., pada tahap awal dilakukan pengujian keamanan (information gathering) pada domain target. Dari data-data hasil pengujian, kemudian dilakukan risk identification untuk melakukan identifikasi risiko, disertai dengan deskripsi risiko dan dampaknya.

Dari hasil risk identification kemudian dilanjutkan dengan risk analysis, untuk menganalisis dampak-dampak yang ditimbulkan oleh risiko-risiko yang telah teridentifikasi, disertai dengan tingkat kemungkinan risiko (likelihood level) dan tingkat dampak yang ditimbulkan oleh risiko (impact level).

DOI: https://doi.org/10.38204/tematik.v10i2.1559



Gambar 4. Flowchart Manajemen Risiko ISO 31000:2018

2.8. Likelihood Level

Likelihood level pada manajemen risiko ISO 31000:2018, memiliki lima skala penilaian beserta poin penilaian masing-masing[22]. Tabel 2. menunjukkan kelima skala penilaian likelihood level beserta dengan skor penilaian masing-masing:

Tabel 2. Kelima Skala Penilaian Likelihood Level

No	Skala Penilaian	Skor Penilaian
1	Rare (jarang terjadi)	1
2	Unlikely (hampir tidak pernah terjadi)	2
3	Possible (agak sering terjadi)	3
4	Likely (cukup sering terjadi)	4
5	Almost (hampir selalu terjadi)	5

Berdasarkan Tabel 2., kelima skala penilaian likelihood level memiliki poin atau skor penilaian masing-masing, yaitu dari skala penilaian jarang terjadi (rare) dengan skor penilaian 1 hingga skala penilaian hampir selalu terjadi (almost) dengan skor penilaian 5.

2.9. Impact Level

Penilaian likelihood level diikuti dengan penilaian impact level. Impact level memiliki lima skala penilaian beserta poin penilaian masing-masing[23]. Tabel 3. menunjukkan kelima skala penilaian Impact Level beserta poin penilaian masing-masing:

Tabel 3. Kelima Skala Penilaian Impact Level

No	Skala Penilaian	Skor Penilaian
1	Insignificant (tidak berdampak sama sekali)	1
2	Minor (berdampak kecil)	2
3	Moderate (berdampak menengah)	3
4	Major (berdampak cukup tinggi)	4
5	Catastrophic (berdampak sangat tinggi)	5

Berdasarkan Tabel 3., kelima skala penilaian impact level memiliki poin atau skor penilaian masing-masing, yaitu dari skala penilaian tidak berdampak sama sekali (insignificant) dengan skor penilaian 1 hingga skala penilaian berdampak sangat tinggi (catastrophic) dengan skor penilaian 5.

2.10. Risk Evaluation

Dari hasil risk analysis, kemudian dilanjutkan ke risk evaluation. Risk evaluation bertujuan untuk menilai atau mengevaluasi hasil analisa risiko yang telah dilakukan, terkait dengan tingkat kemungkinan risiko (likelihood level), tingkat dampak yang ditimbulkan (impact level), dan tingkat risiko (risk level).

Risk evaluation dilakukan menggunakan matriks evaluasi, yang melibatkan skala penilaian dan skor penilaian dari likelihood level dan impact level untuk memperoleh nilai dari risk level[24]. Tabel 4. menunjukkan matriks evaluasi untuk risk evaluation, di mana sumbu X menyatakan skor penilaian dari impact level dan sumbu Y menyatakan skor penilaian dari likelihood level:

Tabel 4.Matriks Evaluasi untuk Risk Evaluation

Skor Penilaian Likelihood Level					
5	M	M	H	H	H
4	L	M	M	H	H
3	L	M	M	M	H
2	L	L	M	M	M
1	L	L	L	M	M
Skor Penilaian Impact Factor	1	2	3	4	5

Keterangan:L=Low, M= Medium, H= High

Berdasarkan kepada Tabel 4., apabila sebuah risiko memiliki skala penilaian likelihood level likely (bernilai 4) dan skala penilaian impact level major (bernilai 4), maka berdasarkan kepada matriks evaluasi, risk level yang diperoleh adalah High (H).

Pasca risk evaluation, kemudian dilakukan penyusunan rekomendasi perbaikan. Rekomendasi perbaikan diharapkan dapat membantu Pemerintah Provinsi Bali untuk melakukan perbaikan keamanan sistem, sehingga dapat meningkatkan kualitas layanan publik, kenyamanan, dan tingkat kepercayaan masyarakat kepada pemerintah di dalam pelayanan publik, dalam rangka mewujudkan program Bali Smart Island.

3. Hasil dan Pembahasan

3.1. Implementasi OSINT

Implementasi dan pengujian dilakukan dengan cara melakukan instalasi tool OSINT Harvester, python3, dan python3-pip pada komputer penulis. Instalasi Tool Harvester menggunakan perintah-perintah berikut pada Terminal Linux:

```
git clone https://github.com/laramies/theHarvester

cd ~/theHarvester

python3.7 -m pip install -r requirements/dev.txt

python3.7 -m pip install -r requirements/base.txt
```

3.2. Pengujian Information Gathering

Setelah tool OSINT Harvester terinstall, kemudian dilanjutkan dengan melakukan pengujian information

DOI: https://doi.org/10.38204/tematik.v10i2.1559

gathering berupa reconnaissance (footprinting). Reconnaissance dilakukan untuk mengumpulkan sebanyak mungkin informasi mengenai domain target secara spesifik. Reconaissance pada proses information gathering, dilakukan dalam bentuk DNS Brute Force, dengan cara mengumpulkan informasi DNS dari domain target (baliprov.go.id) menggunakan tool OSINT Harvester, menggunakan perintah:

python3 theharvester.py -d baliprov.go.id -l 100 -c.

Proses pengumpulan informasi (information gathering) pada domain target https://baliprov.go.id menggunakan tool OSINT Harvester, dilakukan ke dalam dua tahap. Tahap pertama adalah melakukan DNS Brute Force, sedangkan tahap kedua adalah mengumpulan informasi host dan akun E-Mail pada domain target. Dengan menggunakan algoritma Brute Force, proses enumerasi menggunakan 566 kata. Setelah proses enumerasi, diperoleh informasi mengenai tujuh host beserta sub domain dan IP Address dari domain target.

Proses pengumpulan informasi host, data E-Mail, sub-domain, IP Address, dan URL dari sumber data publik, menggunakan mesin pencari Bing. Pemilihan mesin pencari Bing bertujuan untuk mendukung pencarian data dari media sosial dan Google. Pada proses ini, ditemukan 93 host beserta dengan sub domain dan IP Address. Proses pengumpulan informasi host, data E-Mail, sub domain, IP Address, dan URL dari sumber data publik, juga dilakukan menggunakan mesin pencari Google, sebagai mesin pencari terbesar di dunia dan banyak digunakan oleh pengguna internet. Proses ini menemukan 22 host beserta sub domain, IP Address, dan E-Mail.

3.3. Hasil Pengujian Information Gathering

Hasil-hasil dari pengujian information gathering, dimasukkan ke dalam tabel, disertai dengan nomor modul pengujian. Penomoran modul dan langkah-langkah pengujian, disesuaikan dengan pedoman dari OTGV4.2. Tabel 5. menunjukkan hasil pengujian information gathering:

Tabel 5. Hasil Pengujian Information Gathering

No Modul	Kode Modul	Tujuan Pengujian	Hasil
4.2.1	OTG-INFO-001	Search engine discovery dan reconnaissance pada domain target dengan menggunakan mesin pencari Bing	Sukses
4.2.2	OTG-INFO-001	Search engine discovery dan reconnaissance pada domain target dengan menggunakan mesin pencari Google	Sukses
4.2.3	OTG-INFO-001	Information gathering untuk semua E-Mail pada domain target di *.@baliprov.go.id	Sukses
4.2.4	OTG-INFO-004	Enumerasi jumlah sub domain yang aktif pada domain target *.baliprov.go.id menggunakan algoritma brute force	Sukses

Berdasarkan Tabel 5., terdapat empat nomor modul pengujian dengan dua kode modul pengujian information gathering sesuai pedoman OTGv4.2. Kedua kode modul pengujian tersebut yaitu OTG-INFO-001 dan OTG-INFO-004. Pengujian-pengujian yang dilakukan meliputi: 1.)Search engine discovery dan reconnaissance menggunakan mesin pencari Bing, 2.)Search engine discovery dan reconnaissance menggunakan mesin pencari Google, 3.)Information gathering untuk semua E-Mail pada domain target di *.@baliprov.go.id, 4.)Enumerasi jumlah sub domain yang aktif pada domain target (*.baliprov.go.id) menggunakan brute force. Keempat pengujian menunjukkan hasil sukses.

3.3. Hasil Risk Identification

Hasil-hasil pengujian information gathering digunakan untuk melakukan proses identifikasi risiko (risk identification), analisis risiko (risk analysis), dan evaluasi risiko (risk evaluation). Risk identification dimulai dengan mengelompokkan setiap risiko dengan kode risiko (risk code) masing-masing. Kemudian dilakukan deskripsi penjelasan dari setiap risiko (risk description) dan dampak yang dapat ditimbulkan oleh risiko-risiko tersebut (risk impact) terhadap sistem dan organisasi pemilik sistem dan domain baliprov.go.id. Tabel 6. menunjukkan hasil dari risk identification:

Tabel 6. Hasil dari Risk Identification

Risk Code	Risk Identification	Risk Description	Risk Impact
R1	Host, subdomain, IP Address discovery dan reconnaissance menggunakan mesin pencari Bing	Proses pengumpulan informasi (information gathering) dari domain target yang meliputi host, sub domain, dan IP Address menggunakan mesin pencari Bing	Attacker dapat memperoleh semua informasi penting mengenai domain target (host, sub domain, IP Address) yang dapat digunakan sebagai petunjuk untuk melakukan penyerangan
R2	Host, subdomain, IP Address discovery dan reconnaissance menggunakan mesin pencari Google	Proses pengumpulan informasi (information gathering) dari domain target yang meliputi host, sub domain, dan IP Address menggunakan mesin pencari Google	Attacker dapat memperoleh semua informasi penting mengenai domain target (host, sub domain, IP Address) yang dapat digunakan sebagai petunjuk untuk melakukan penyerangan

DOI: https://doi.org/10.38204/tematik.v10i2.1559

Risk Code	Risk Identification	Risk Description	Risk Impact
R3	Information gathering terhadap semua E-Mail dari domain target	Proses pengumpulan informasi (information gathering) mengenai akun-akun E-Mail pada domain target di *.@baliprov.go.id	Attacker dapat menyalahgunakan data-data E-mail tersebut untuk melakukan peretasan sistem, khususnya dengan teknik Social Engineering
R4	Sub domain enumeration (brute force) pada domain target	Proses enumerasi pada domain target *.baliprov.go.id menggunakan metode Brute Force	Attacker dapat mengetahui semua informasi penting dari domain target untuk melakukan penyerangan ke sistem (subdomain dan IP Address dari *.baliprov.go.id), spam, dan bentuk serangan lainnya sesuai dengan Common Weakness Enumeration (CWE) dan Common Vulnerabilities and Exposures (CVE)

Berdasarkan Tabel 6., hasil dari risk identification berhasil mengidentifikasikan empat risiko beserta dengan deskripsi dan dampak yang ditimbulkan. Risiko pertama (R1) berhasil mengidentifikasi adanya kemungkinan host, subdomain, IP Address discovery dan reconnaissance terhadap domain target oleh attacker dengan menggunakan mesin pencari Bing. Dampak yang ditimbulkan oleh risiko ini (risk impact) adalah attacker dapat memperoleh semua informasi penting mengenai domain target (host, sub domain, IP Address) yang dapat digunakan sebagai petunjuk untuk melakukan penyerangan ke domain target.

Risiko kedua (R2) berhasil mengidentifikasi adanya kemungkinan host, subdomain, IP Address discovery dan reconnaissance terhadap domain target oleh attacker dengan menggunakan mesin pencari Google. Seperti halnya R1, dampak yang ditimbulkan oleh risiko ini (risk impact) adalah attacker dapat memperoleh semua informasi penting mengenai domain target (host, sub domain, IP Address) yang dapat digunakan sebagai petunjuk untuk melakukan penyerangan ke domain target.

Risiko ketiga (R3) berhasil mengidentifikasi adanya kemungkinan pengumpulan informasi sejumlah akun E-Mail pada domain target di *.@baliprov.go.id oleh attacker, di mana data akun-akun E-Mail tersebut dapat disalahgunakan oleh attacker untuk melakukan penyerangan dengan teknik Social Engineering.

Risiko keempat (R4) berhasil mengidentifikasi adanya kemungkinan enumerasi pada domain target *.baliprov.go.id oleh attacker dengan menggunakan metode Brute Force, di mana attacker dapat memperoleh semua informasi penting dari domain target (subdomain, IP Address) *.baliprov.go.id, yang memungkinkan attacker untuk melakukan penyerangan ke sistem, melakukan spam, dan bentuk serangan lainnya sesuai dengan Common Weakness Enumeration (CWE) dan Common Vulnerabilities and Exposures (CVE).

3.5. Hasil Risk Analysis

Setelah dilakukan risk identification, kemudian dilakukan risk analysis. Risk analysis dimulai dengan melakukan analisis perhitungan risiko dari hasil Risk identification. Proses risk analysis dimulai dari penentuan tingkat kemungkinan risiko (likelihood level) dan tingkat dampak risiko (impact level). Setiap risiko yang telah teridentifikasi pada risk identification, diberikan skor penilaian likelihood level dan impact level sesuai ketentuan pada ISO 31000:2018. Tabel 7. menunjukkan hasil dari risk analysis:

Tabel 7.Hasil Risk Analysis

Risk Code	Risk Description	Likelihood Level	Impact Level
R1	Proses pengumpulan informasi (information gathering) dari domain target yang meliputi host, sub domain, dan IP Address menggunakan mesin pencari Bing	Possible (3)	Moderate (3)
R2	Proses pengumpulan informasi (information gathering) dari domain target yang meliputi host, sub domain, dan IP Address menggunakan mesin pencari Google	Possible (3)	Moderate (3)
R3	Proses pengumpulan informasi (information gathering) mengenai akun-akun E-Mail pada domain target di *.@baliprov.go.id	Possible (3)	Moderate (3)
R4	Proses enumerasi pada domain target *.baliprov.go.id menggunakan metode Brute Force	Possible (3)	Moderate (3)

Berdasarkan Tabel 7., keempat risiko yang ditandai dengan kode risiko (risk code) R1, R2, R3, dan R4, masing-masing memiliki skor penilaian likelihood

DOI: https://doi.org/10.38204/tematik.v10i2.1559

level dan impact level yang sama. Untuk skor penilaian likelihood level adalah possible. Hal ini berarti bahwa risiko agak sering terjadi. Poin penilaian untuk level ini adalah 3.

Untuk skor penilaian impact level adalah moderate. Hal ini berarti bahwa risiko berdampak menengah (tidak terlalu tinggi dan tidak terlalu rendah). Poin penilaian untuk level ini adalah 3.

3.6. Hasil Risk Evaluation

Dari hasil risk analysis, kemudian dilanjutkan ke risk evaluation. Risk evaluation dilakukan dengan menggunakan matriks likelihood level dan impact level dari setiap risiko, untuk memperoleh tingkatan risiko (risk level). Tabel 8. menunjukkan risk evaluation dari setiap risiko:

Tabel 8. Hasil Risk Evalution

Risk Code	Risk Description	Likelihood Level	Impact Level	Risk Level
R1	Proses pengumpulan informasi (information gathering) dari domain target yang meliputi host, sub domain, dan IP Address menggunakan mesin pencari Bing	Possible (3)	Moderate (3)	Medium
R2	Proses pengumpulan informasi (information gathering) dari domain target yang meliputi host, sub domain, dan IP Address menggunakan mesin pencari Google	Possible (3)	Moderate (3)	Medium
R3	Proses pengumpulan informasi (information gathering) mengenai akun-akun E-Mail pada domain target di *.@baliprov.go.id	Possible (3)	Moderate (3)	Medium
R4	Proses enumerasi pada domain target *.baliprov.go.id menggunakan metode Brute Force	Possible (3)	Moderate (3)	Medium

Berdasarkan Tabel 8., keempat risiko yang ditandai dengan risk code R1, R2, R3, dan R4, masing-masing memiliki likelihood level possible (dengan poin 3) dan impact level moderate (dengan poin 3). Mengacu dari matriks risk evalution pada Tabel 4., maka risk level bernilai medium. Hal ini berarti bahwa risiko bernilai tidak terlalu tinggi dan tidak terlalu rendah, namun perlu untuk segera dilakukan pencegahan, penanggulangan, atau tindakan perbaikan oleh organisasi bersangkutan, untuk mencegah terjadinya hal-hal yang tidak diinginkan.

3.7. Hasil Risk Action (Rekomendasi Perbaikan)

Berdasarkan hasil risk evaluation dengan risk level medium, maka langkah terakhir pada penelitian ini adalah melakukan risk action dengan cara melakukan penyusunan rekomendasi. Penyusunan rekomendasi melibatkan hasil-hasil dari risk identification, risk analysis, dan risk evaluation, untuk disusun ke dalam sebuah tabel rekomendasi perbaikan. Tabel 9. menunjukkan penyusunan rekomendasi berdasarkan hasil dari risk evaluation:

Tabel 9.Rekomendasi Perbaikan

Risk Code	Risk Identification	Risk Description	Risk Recommendation
R1	Host, subdomain, IP Address discovery dan reconnaissance menggunakan mesin pencari Bing	Proses pengumpulan informasi (information gathering) dari domain target yang meliputi host, sub domain, dan IP Address menggunakan mesin pencari Bing	1.Konfigurasikan name server untuk menonaktifkan zone-transfer DNS terhadap host-host yang tidak terpercaya atau tidak dikenali 2.Konfigurasikan web server untuk mencegah pengindeksan direktori tanpa file indeks
R2	Host, subdomain, IP Address discovery dan reconnaissance menggunakan mesin pencari Google	Proses pengumpulan informasi (information gathering) dari domain target yang meliputi host, sub domain, dan IP Address menggunakan mesin pencari Google	1.Konfigurasikan name server untuk menonaktifkan zone-transfer DNS terhadap host-host yang tidak terpercaya atau tidak dikenali 2.Konfigurasikan web server untuk mencegah pengindeksan direktori tanpa file indeks
R3	Information gathering terhadap semua E-Mail dari domain target	Proses pengumpulan informasi (information gathering) mengenai akun-akun E-Mail pada domain target di *.@baliprov.go.id	1.Menggunakan anti virus dan anti spam pada sistem dan pengguna untuk mencegah spam akibat E-Mail information gathering oleh attacker. 2.Pada pengguna diberikan edukasi mitigasi pada penggunaan layanan E-Mail: penggunaan fitur Blind

DOI: https://doi.org/10.38204/tematik.v10i2.1559

Risk Code	Risk Identification	Risk Description	Risk Recommendation
			Carbon Copy (BCC) pada pengiriman E-Mail ke lebih dari satu pengguna, mengganti sisipan (attachment) E-Mail ke URL Google Drive/layanan cloud drive, menghapus E-Mail lama yang tidak diperlukan.
R4	Sub domain enumeration (brute force) pada domain target di *.baliprov.go.id	Proses enumerasi pada domain target *.baliprov.go.id menggunakan metode Brute Force	1.Konfigurasikan server SMTP. 2.Pergunakan NT Local Area Network Management (NTLM) atau bentuk otentikasi dasar untuk membatasi akses pengguna (hanya untuk pengguna yang berhak). 3.Menggunakan detail kontak administrasi jaringan terpusat pada database Network Information Center (NIC). 4.Konfigurasikan name server untuk menonaktifkan zone-transfer DNS untuk host-host yang tidak terpercaya atau tidak dikenali. 5.Mengkonfigurasikan web server untuk mencegah pengindeksan direktori tanpa file indeks.

Berdasarkan Tabel 9., masing-masing risiko yang ditandai dengan risk code R1, R2, R3, dan R4, diberikan satu atau lebih rekomendasi perbaikan (risk recommendation), sesuai dengan risk identification, risk analysis, dan risk evaluation. Rekomendasi-rekomendasi perbaikan, diharapkan dapat membantu pihak Pemerintah Provinsi Bali di dalam meningkatkan keamanan sistem, untuk mewujudkan layanan publik yang aman, nyaman, terpercaya, dan lebih baik, sesuai dengan program Bali Smart Island.

4. Kesimpulan

Pada bagian ini, penulis menyimpulkan hasil-hasil dari penelitian smart security risk management pada Bali Smart Island menggunakan OSINT, OTGv4.2, dan ISO 31000:2018. Berdasarkan kepada pengujian yang telah dilakukan dan hasil-hasil pengujian, diperoleh kesimpulan bahwa pengujian keamanan sistem pada domain target melalui information gathering dapat dilakukan dengan baik berbasis metode OSINT dan OTGv4.2, menggunakan tool OSINT Harvester. Penilaian risiko melalui tahapan risk identification, risk analysis, dan risk evaluation, telah sesuai dengan pedoman framework ISO 31000:2018. Penyusunan rekomendasi dapat dilakukan dengan baik, memanfaatkan hasil-hasil dari penilaian risiko, beserta pemberian saran perbaikan.

5. Saran

Ke depannya, penelitian ini dapat dilanjutkan dengan menggunakan framework dan metode pengujian keamanan lainnya beserta dengan tool-tool pendukung. Framework dan metode pengujian yang dapat penulis usulkan di antaranya ISAF, OSSTM, dan NIST. Sedangkan untuk tool pengujian keamanan sistem dapat menggunakan paket security pada distribusi Linux yang mengkhusus ke security (misal: Kali Linux) atau melalui Linux Ubuntu desktop dengan menambahkan paket Katoolin melalui repositori online.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada pihak-pihak yang telah memberikan dukungan dan bantuan dalam pelaksanaan penelitian ini: Pemerintah Provinsi Bali untuk bantuan informasi dan akses domain pengujian pada studi kasus penelitian ini, rekan-rekan sejawat di Universitas Udayana untuk dukungan selama penelitian, Christian Martorella dan tim sebagai pengembang tool OSINT Harvester yang digunakan sebagai alat pengujian pada penelitian ini, tim Edge Security untu dokumentasi OTGv4.2 sebagai pedoman pada penelitian ini, Komunitas Linux Indonesia atas dukungan dan saran teknis selama penelitian menggunakan Linux Ubuntu, komunitas Open Web Application Security Project (OWASP) yang telah menyediakan sumber daya dan informasi mengenai keamanan web dan aplikasi, komunitas OWASP Indonesia atas semua masukan dan kritik konstruktif bagi penulis dalam menyusun artikel penelitian ini, serta terima kasih kepada pihak-pihak lain yang tidak dapat disebutkan satu per satu,

DOI: https://doi.org/10.38204/tematik.v10i2.1559

yang turut berperan dalam penelitian ini. Semoga penelitian ini dapat bermanfaat bagi pemerintah (khususnya Pemerintah Provinsi Bali), masyarakat, akademisi, di bidang security risk management pada Smart City. Penulis menyadari bahwa penelitian ini masih memiliki banyak kekurangan dan keterbatasan, sehingga penulis mengharapkan kritik dan saran yang membangun dari pembaca.

Daftar Pustaka

[1] Pratama, I.P.A.E., "Smart City Beserta Cloud Computing dan Teknologi-Teknologi Pendukung Lainnya," Penerbit Informatika. Bandung. 2014. ISBN: 978-602-1514-40-5.

[2] Rizkinaswara, L., "Gerakan Menuju 100 Smart City," Website Kementerian Komunikasi dan Informatika Republik Indonesia (online). 2022. Available: https://aptika.kominfo.go.id/2022/07/gerakan-menuju-100-smart-city-2/ [accessed: 17 November 2023].

[3] Pemerintah Provinsi Bali. "Nangun Sat Kerthi Loka Bali, Melalui Pola Pembangunan Semesta Berencana Menuju Bali Era Baru", Website Pemerintah Provinsi Bali (online). 2021. Available: https://baliprov.go.id/ [accessed: 1 June 2021].

[4] Crane, L., Gantz, G. and Isaacs, S.I. "Introduction to Risk Management," Journal of Business Strategy, Vol.3, 2013. pp.41-43.

[5] Outreville, J.F. "The Relationship between Insurance and Economic Development: 85 Empirical Papers for a Review of the Literature," Risk Management and Insurance Review, Vol.16, 2013. pp.71-122. https://doi.org/10.1111/j.1540-6296.2012.01219.

[6] OWASP. "OWASP Testing Guide version 4.2 (OTGv4.2)", OWASP homepage (online). Available: https://owasp.org/www-project-web-security-testing-guide/v42/ [accessed: 28 May 2021].

[7] C. Martorella. "The Harvester: the Open Source OSINT Tool for Information Gathering", Laramies/The Harvester GitHub (online). Available: https://github.com/laramies/theHarvester [accessed: 28 May 2021].

[8] Saluky, "Tinjauan Artificial Intelligence untuk Smart Government," Information Technology Engineering Journals (ITEJ), Vol.03, No.01, 2018.

[9] J. More, "Job Reconnaissance Using Hacking Skills to Win the Job Hunt Game", Elsevier Inc. 2014.

[10] Kalinin, M.; Krundyshev,V.; Zegzhda, P. "Cybersecurity Risk Assessment in Smart City Infrastructures", Machines Vol.9, No. 78, 2021. https://doi.org/10.3390/machines9040078

[11] A.N. Kazak; N. Shamayeva. "Separate Aspects of Smart Cities Security," 2018 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2018, pp.216-218, doi: 10.1109/ITMQIS.2018.8524909

[12] P.T. Pradeep; K.L. Shashikala, "Smart City Services Challenges and Approach," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 553-558, doi: 10.1109/COMITCon.2019.8862243.

[13] P. Hui, "Construction of Information Security Risk Assessment Model in Smart City," 2020 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), 2020, pp. 393-396, doi: 10.1109/TOCS50858.2020.9339614.

[14] M. Pouryazdan and B. Kantarci, "The Smart Citizen Factor in Trustworthy Smart City Crowdsensing," in IT Professional, vol. 18, no. 4, pp. 26-33, July-Aug. 2016, doi: 10.1109/MITP.2016.72.

[15] K. Waedt, A. Ciriello, M. Parekh and E. Bajramovic, "Automatic assets identification for smart cities: Prerequisites for cybersecurity risk assessments," 2016 IEEE International Smart Cities Conference (ISC2), 2016, pp. 1-6, doi: 10.1109/ISC2.2016.7580812.

[16] S. K. Lala, A. Kumar and S. T., "Secure Web Development using OWASP Guidelines," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 323-332, doi: 10.1109/ICICCS51141.2021.9432179.

[17] I.P.A.E. Pratama, A.A.B.A. Wiradarma, "Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company)", International Journal of Computer Network and Information Security (IJCNIS), Vol.11, No.7, 2019.

[18] M. A. Juniawan, P. Sandhyaduhita, B. Purwandari, S. B. Yudhoatmojo and M. A. A. Dewi, "Smart government assessment using Scottish Smart City Maturity Model: A case study of Depok city," 2017 International Conference on Advanced Computer Science and Information Systems (ICACSIS), 2017, pp. 99-104, doi: 10.1109/ICACSIS.2017.8355018.

[19] S. Manggalou, et al., "Risk management analysis of public street lighting (SMART PJU) as Quick win smart environment of Semarang City," International Journal of Science, Technology & Management (IJSTM), Vol.4, No.5, 2023.

[20] P. Cash, et al., "Experimental Design Research: Approaches, Perspectives, Applications" Springer Link. 2016.

[21] I.P.A.E Pratama, M.T.S. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," Jurnal Telematika, Vol.15, No.2, 2020.

[22] B. Dharma, D.C. Pratiwi, "Developing Financial Risk Strategy Decisions for Construction Projects From Perspective of the Project Owner," Journal of Management and Business Innovation (JOMBI), Vol.2, No.1, 2020.

[23] Periyadi, "Analisis Resiko Teknologi Informasi Sistem Terintegrasi iGracias Berbasis Risk Assesment Menggunakan SNI ISO-IEC 27001-2009," Jurnal Teknologi Informasi Vol.2, No.3, 2015.

[24] M. Azizah, W. Yustanti, "Pemilihan Metode Risk Assessment Pada UPT-TIK di Perguruan Tinggi Menggunakan Metode AHP (Analytical Hierarchy Process) (Studi kasus: UPT-TIK Wilayah Kota Surabaya)," Jurnal Manajemen Informatika. Vol.10, No.01, 2019.

DOI: https://doi.org/10.38204/tematik.v10i2.1559