KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS DIPONEGORO
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT

Gedung ICT Lantai 4
Jalan Prof. Sudarto, S.H.
Tembalang Semarang Kode Pos 50275
Tel. (024) 7460032, Faks. (024) 7460039
lppm.undip.ac.id | email: lppm[at]live.undip.ac.id

SURAT PENUGASAN PELAKSANAAN KEGIATAN BATCH II
RISET PUBLIKASI INTERNASIONAL (RPI)
DIBIAYAI SELAIN ANGGARAN PENDAPATAN DAN BELANJA NEGARA (SELAIN APBN)
UNIVERSITAS DIPONEGORO TAHUN ANGGARAN 2022

Nomor : 569-174/UN7.D2/PP/VII/2022

Pada hari ini SELASA tanggal DUA PULUH ENAM bulan JULI tahun DUA RIBU DUA PULUH DUA kami yang bertanda tangan di bawah ini:

1. Prof. Dr. Jamari, S.T., M.T. : Ketua Lembaga Penelitian dan Pengabdian kepada Masyarakat Universitas Diponegoro berkedudukan di Kota Semarang, berdasarkan SK Rektor Universitas Diponegoro Nomor: 561/UN7.P/KP/2019 tanggal 2 Agustus 2019 tentang pengangkatan Ketua Lembaga Penelitian dan Pengabdian kepada Masyarakat Universitas Diponegoro periode masa jabatan 2019-2022, untuk selanjutnya disebut PIHAK PERTAMA.

2. Dr. Ir. R. Rizal Isnanto, S.T., M.M., M.T., IPM : Dosen Fakultas Teknik Universitas Diponegoro, dalam hal ini bertindak sebagai Ketua Pelaksana Riset Publikasi Internasional (RPI) Tahun Anggaran 2022 yang selanjutnya disebut PIHAK KEDUA.

Berdasarkan Surat Keputusan Rektor Universitas Diponegoro nomor: 215/UN7.A/HK/VII/2022 tanggal 25 Juli 2022, tentang Penetapan Pendanaan Kegiatan Riset dan Pengabdian kepada Masyarakat Universitas Diponegoro Batch II Tahun 2022 yang di biayai Selain Anggaran Pendapatan dan Belanja Negara (APBN) Tahun Anggaran 2022, PIHAK PERTAMA dan PIHAK KEDUA, secara bersama-sama sepakat mengikatkan diri dalam suatu Penugasan Pelaksanaan Kegiatan Riset dengan ketentuan dan syarat-syarat sebagaimana diatur dalam pasal-pasal sebagai berikut:

Pasal 1
Pelaksanaan Penugasan

(1) PIHAK PERTAMA menugaskan kepada PIHAK KEDUA untuk melaksanakan Riset tahun ke 1 dari rencana 2 tahun dengan Tim Riset dan Judul Riset sebagai berikut:

- Tim Riset : 1. Dr. Ir. R. Rizal Isnanto, S.T., M.M., M.T., IPM
  2. Jatmiko Endro Suseno, S.Si., M.Si., Ph.D.
- Judul Riset : Security Governance Model at the Top Management of Startup on the Implementation of Secure Software Development Lifecycle (SSDL) by Using a Quantitative Approach

(2) PIHAK PERTAMA menyerahkan dana riset sebagaimana dimaksud pada ayat (1) sebesar Rp. 58.700.000,00 (*Lima puluh delapan juta tujuh ratus ribu rupiah*) yang berasal dari Selain Anggaran Pendapatan dan Belanja Negara (Selain APBN) Universitas Diponegoro Tahun Anggaran 2022;

(3) PIHAK KEDUA bertanggung jawab penuh atas pelaksanaan riset, pengadministrasian, pembelanjaan, dan pelaporan keuangan sebagaimana dimaksud pada ayat (1) sesuai dengan ketentuan yang berlaku;

(4) PIHAK KEDUA berkewajiban mengembalikan sisa dana riset yang tidak dibelanjakan ke Bendahara Penerimaan Universitas Diponegoro melalui PIHAK PERTAMA;

(5) Apabila PIHAK KEDUA tidak dapat melaksanakan riset sebagaimana dimaksud pada ayat (1) maka PIHAK KEDUA wajib mengembalikan dana sebagaimana disebutkan pada ayat (2) ke Bendahara Universitas Diponegoro melalui PIHAK PERTAMA.

Pasal 2
Cara Pembayaran dan Mekanisme Pencairan Dana Riset

(1) Dana riset sebagaimana dimaksud dalam pasal 1 ayat (2) dibayarkan melalui rekening atas nama PIHAK KEDUA pada bank yang ditunjuk oleh PIHAK PERTAMA;

(2) PIHAK PERTAMA akan membayarkan dana riset kepada PIHAK KEDUA secara bertahap dengan ketentuan sebagai berikut:

a. Pembayaran tahap pertama sebesar 70% dari total dana riset yaitu 70% x Rp. 58.700.000,00 = Rp. 41.090.000,00 (*Empat puluh satu juta sembilan puluh ribu rupiah*) setelah PIHAK KEDUA menandatangani dan mengunggah Surat Pelaksanaan Penugasan (SPK) maupun mengunggah proposal pelaksanaan di laman SIP3MU;

b. Pembayaran tahap kedua sebesar 30% dari total dana riset yaitu 30% x Rp. 58.700.000,00 = Rp. 17.610.000,00 (*Tujuh belas juta enam ratus sepuluh ribu rupiah*) setelah PIHAK KEDUA mengunggah seluruh laporan sesuai dengan ketentuan yang berlaku ke laman SIP3MU.

Pasal 3
Pemblokiran Dana Riset

(1) PIHAK KEDUA memberikan kuasa penuh kepada PIHAK PERTAMA untuk melakukan blokir saldo sejumlah dana yang telah dibayarkan oleh PIHAK PERTAMA kepada PIHAK KEDUA apabila PIHAK KEDUA belum memenuhi segala kewajiban dan persyaratan pancairan;

(2) PIHAK PERTAMA tidak melakukan pemblokiran dana riset tahap pertama (70%) yang telah ditransfer kepada PIHAK KEDUA;

(3) PIHAK PERTAMA melakukan pemblokiran dana riset tahap kedua (30%) yang telah ditransfer kepada PIHAK KEDUA;

(4) Pembukaan blokir sebagaimana disebut pada ayat (3) dilakukan setelah PIHAK KEDUA menyelesaikan seluruh kewajibannya.

Pasal 4
Jangka Waktu Pelaksanaan Riset

Surat Penugasan Pelaksanaan Kegiatan Riset ini berlaku dari tanggal 11 Juli 2022 sampai dengan 15 Desember 2022.

Pasal 5
Monitoring dan Evaluasi Riset

(1) PIHAK PERTAMA berhak melakukan monitoring dan evaluasi terhadap pelaksanaan riset yang dilakukan oleh PIHAK KEDUA.

(2) PIHAK KEDUA wajib mengikuti monitoring dan evaluasi riset yang dilakukan oleh PIHAK PERTAMA dengan persyaratan mengunggah Laporan Kemajuan dan Buku Catatan Hasil Riset pada laman SIP3MU LPPM Universitas Diponegoro serta menyerahkan Laporan Penggunaan Dana Riset tahap pertama sebesar 70% minimal dalam bentuk draft selambat-lambatnya 1 (satu) minggu sebelum pelaksanaan monitoring dan evaluasi.

Pasal 6
Luaran Riset

(1) PIHAK KEDUA berkewajiban memenuhi luaran yang telah ditetapkan dalam proposal riset, sesuai dengan Buku Panduan Pelaksanaan Penelitian dan Pengabdian kepada Masyarakat Universitas Diponegoro yang berlaku;

(2) Batas waktu pencapaian luaran sebagaimana dimaksud pada ayat (1) dapat dicapai selama 6 (enam) bulan setelah kontrak selesai. Dan apabila belum tercapai dapat diberi tambahan waktu selama 6 (enam) bulan lagi atau lebih berdasarkan hasil evaluasi oleh *reviewer*;

(3) Hak kepemilikan luaran riset sebagaimana dimaksud pada ayat (1) adalah milik Universitas Diponegoro dan dikelola sesuai dengan kententuan yang berlaku.

Pasal 7
Pelaporan Riset

(1) PIHAK KEDUA berkewajiban mengunggah ke laman SIP3MU LPPM Universitas Diponegoro antara lain: Surat pelaksanaan Penugasan Kegiatan (SPK), Proposal Pelaksanaan, Buku Catatan Hasil Riset, Laporan Kemajuan Riset, Laporan Akhir Riset, Luaran Riset, Poster (bagi riset tahun terakhir) dan menyerahkan Laporan Penggunaan Dana Riset tahap pertama sebesar 70% maupun tahap kedua sebesar 30% dijilid menjadi 1 (satu) dan dibuat rangkap 2 (dua), asli diserahkan kepada PIHAK PERTAMA serta *copy* sebagai arsip PIHAK KEDUA;

(2) Batas waktu kewajiban penyerahan Laporan Penggunaan Dana Riset maupun unggah laporan-laporan riset ke laman SIP3MU Undip seperti termaktub pada ayat (1), paling lambat tanggal 15 Desember 2022;

(3) Bilamana diperlukan PIHAK PERTAMA dapat meminta kepada PIHAK KEDUA untuk menyerahkan dokumen hasil unggahan sebagaimana tersebut pada ayat (1) dalam bentuk *hardcopy* dengan persyaratan sebagai berikut:

a. Laporan diketik dengan huruf times new roman ukuran 12, spasi 1,5;
b. Ukuran kertas kwarto A4;
c. Warna cover dijilid sesuai dengan skema riset yang ada di buku panduan yang berlaku;
d. *Hardcopy* laporan dijilid dalam bentuk *soft cover laminating*;
e. Di bagian bawah cover ditulis:

Dibiayai Selain Anggaran Pendapatan dan Belanja Negara (Selain APBN) Universitas Diponegoro Tahun Anggaran 2022 Keputusan Rektor Universitas Diponegoro Nomor : 215/UN7.A/HK/VII/2022 No SPK : 569-174/UN7.D2/PP/VII/2022

Pasal 8
Perubahan Susunan Tim Pelaksana Riset

Perubahan terhadap susunan tim pelaksana riset dapat dibenarkan apabila telah mendapat persetujuan tertulis dari Ketua Lembaga Penelitian dan Pengabdian kepada Masyarakat Universitas Diponegoro.

Pasal 9
Pajak dan Meterai

(1) PIHAK KEDUA berkewajiban membayar pajak sesuai dengan ketentuan yang berlaku;

(2) Tata cara pembayaran pajak diatur oleh PIHAK PERTAMA dalam Panduan Pertanggungjawaban Keuangan Penelitian dan Pengabdian Kepada Masyarakat;

(3) Biaya Materai dalam surat penugasan ini dibebankan kepada PIHAK KEDUA.

Pasal 10
Kepemilikan Hasil Riset

(1) Hak Kekayaan Intelektual (HKI)/Paten yang dihasilkan dari pelaksanaan riset menjadi milik Universitas Diponegoro, diatur dan dikelola sesuai dengan peraturan yang berlaku;

(2) Setiap publikasi, makalah, dan/atau ekspos dalam bentuk apapun yang berkaitan dengan hasil riset ini wajib mencantumkan nama Universitas Diponegoro sebagai pemberi dana pelaksanaan riset.

(3) Bilamana pelaksanaan riset ini menghasilkan aset tetap maka PIHAK KEDUA berkewajiban menyerahkan kepada PIHAK PERTAMA yang dilampiri berita acara serah terima dengan ketentuan sebagai berikut:

   a. Aset tetap tersebut telah terdaftar dalam registrasi pengelolaan barang milik Negara;

   b. Aset tetap tersebut dilampiri dengan Standar Operasional Prosedur (SOP).

(4) Hasil riset yang berupa aset tetap dari kegiatan ini dicatat secara tertib dan akuntabel dalam inventaris fakultas homebase ketua riset dan menjadi aset Universitas Diponegoro.

Pasal 11
Pelanggaran Kode Etik Ilmiah

(1) Pengusulan dan Pelaksanaan Riset harus berdasarkan kode etik ilmiah;

(2) Apabila dikemudian hari ternyata judul riset sebagaimana dimaksud pada pasal 1 ditemukan adanya pelanggaran kode etik ilmiah, maka kegiatan riset tersebut dinyatakan batal dan PIHAK KEDUA wajib mengembalikan dana riset yang telah diterima ke bendahara penerima Universitas Diponegoro melalui PIHAK PERTAMA.

Pasal 12
Sanksi/Denda

(1) Apabila sampai dengan batas waktu yang telah ditentukan, PIHAK KEDUA belum memenuhi kewajibannya maka dapat dikenakan sanksi oleh PIHAK PERTAMA;

(2) Apabila PIHAK KEDUA belum dapat menyelesaikan pekerjaan berdasarkan jangka waktu yang telah ditetapkan dalam surat penugasan ini, maka dapat dikenakan denda oleh PIHAK PERTAMA;

(3) Dalam memberikan/tidak memberikan sanksi/denda PIHAK PERTAMA memperhatikan hasil evaluasi *reviewer*.

Pasal 13
Penyelesaian Perselisihan

Apabila terjadi perselisihan antara PIHAK PERTAMA dan PIHAK KEDUA dalam Surat Penugasan Pelaksanaan Kegiatan Riset ini, akan dilakukan penyelesaian secara musyawarah dan mufakat, sekiranya tidak tercapai penyelesaian secara musyawarah dan mufakat maka penyelesaian dilakukan melalui proses hukum dengan memilih tempat di Pengadilan Negeri Semarang, sebagai upaya hukum tingkat pertama dan terakhir.

Pasal 14
Keadaan Memaksa (*force majeure*)

(1) PARA PIHAK dibebaskan dari tanggung jawab atas keterlambatan atau kegagalan dalam memenuhi kewajiban yang dimaksud dalam Penugasan Pelaksanaan Riset yang disebabkan atau diakibatkan oleh peristiwa diluar kekuasaan PARA PIHAK yang dapat digolongkan sebagai keadaan memaksa (*force majeure*);

(2) Peristiwa atau kejadian yang dapat digolongkan keadaan memaksa (*force majeure*) dalam Penugasan Pelaksanaan Riset ini antara lain: bencana alam, wabah penyakit, kebakaran, perang, blokade, peledakan, sabotase, revolusi, pemberontakan, huru-hara, serta adanya tindakan pemerintah dalam bidang ekonomi dan moneter yang secara nyata berpengaruh terhadap Penugasan Pelaksanaan Riset ini;

(3) Apabila terjadi keadaan memaksa (*force majeure*) maka pihak yang mengalami wajib memberitahukan kepada pihak lainnya secara tertulis, selambat-lambatnya dalam waktu 7(tujuh) hari kerja sejak terjadinya keadaan memaksa (*force majeure*) disertai bukti-bukti yang sah dari pihak yang berwajib, dan PARA PIHAK dengan itikad baik akan segera membicarakan penyelesaiannya.

Pasal 15
Adendum dan Penutup

(1) Hal-hal yang belum diatur dalam Surat Penugasan Pelaksanaan Kegiatan Riset ini diatur kemudian antara PIHAK PERTAMA dan PIHAK KEDUA yang akan dituangkan dalam bentuk adendum dan merupakan bagian tak terpisahkan dari Surat Penugasan ini;
(2) Surat Penugasan Pelaksanaan Kegiatan Riset ini dibuat rangkap 2 (dua) dan bermaterai cukup sesuai dengan ketentuan yang berlaku.

PIHAK KEDUA	PIHAK PERTAMA
Dr. Ir. R. Rizal Isnanto, S.T., M.M., M.T., IPM	Prof. Dr. Jamari, S.T., M.T.
NIDN 0027077008	NIP 197403042000121001

RESEARCH REPORT FOR
INTERNATIONAL SCIENTIFIC PUBLICATION (RPI)

RESEARCH TITLE

Security Governance Model at the Top Management of startup on the Implementation of Secure Software Development Lifecycle (SSDL) by Using Quantitative Approach

The 1st year of the 2 year plan

INVESTIGATORS :

1.	Dr. Ir. R. Rizal Isnanto, S.T., M.M., M.T., IPM.	0027077008
2.	Jatmiko Endro Suseno, S.Si., M.Si., Ph.D.	0021117203
3.	Doddy Ferdiansyah	30000320520039

UNIVERSITAS DIPONEGORO
AND
PARTNER

December, 2022

LAPORAN PENELITIAN / PENGABDIAN KEPADA MASYARAKAT

UNIVERSITAS DIPONEGORO

Petunjuk:Pengusul hanya diperkenankan mengisi di tempat yang telah disediakan sesuai dengan petunjuk pengisian.

Skema Hibah

Riset Publikasi Internasional (RPI)

Judul (*Title*)

Model Tata Kelola Keamanan Pada Top Management Startup Tentang Penerapan Secure Software Development Lifecycle (SSDL) Dengan Menggunakan Pendekatan Kuantitatif

Keterkaitan penelitian/pengabdian kepada masyarakat lain (*Linkages*)
(Maksimum 50 kata)

Click or tap here to enter text.

ABSTRAK(*Abstract*)

Perkembangan software startup sangat masif karena banyak layanan yang berubah menjadi digital. Berbagai aplikasi bermunculan yang sesuai fungsinya dengan memanfaatkan momentum transformasi digital. Misalnya, aplikasi untuk sektor Pendidikan, sektor industri, dan sektor ekonomi. Dengan prioritas utama mereka adalah membuat aplikasi, faktor keamanan menjadi kurang diperhatikan. Hal ini dibuktikan dengan banyaknya pembobolan data yang merugikan perusahaan dan lembaga publik yang serius. Di sinilah peran manajemen tingkat atas muncul dalam merestrukturisasi strategi perusahaan, khususnya startup perangkat lunak, untuk mendukung pembuatan aplikasi yang lebih aman. Dalam penelitian ini matriks RACI digunakan untuk menentukan siapa yang cocok untuk menerapkan strategi keamanan dalam tata kelola keamanan informasi dalam struktur organisasi perangkat lunak startup. Dimana studi ini dimulai dari identifikasi pemangku kepentingan, peran manajemen tingkat atas dalam startup perangkat lunak, dan aktivitas dalam siklus hidup pengembangan perangkat lunak yang aman. Dan hasil dari penelitian ini adalah indikator strategi yang cocok untuk software startup.

Kata Kunci (*Keywords*)

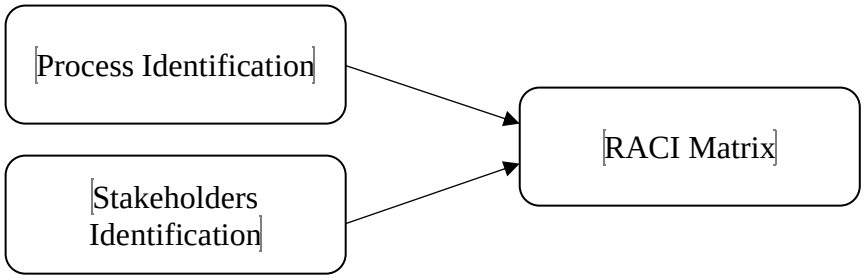
information security governance, RACI matrix, startup software, strategy, top-level management

HASIL PELAKSANAAN PENELITIAN (*Result*)

Dari hasil wawancara yang dilakukan pada CEO sebuah software startup yang berdomisili di Bandung Jawa Barat, secara struktur organisasi mereka memiliki beberapa peran sebagai berikut :

No	Peran
1	CEO
2	CTO
3	Web Development Director
4	Mobile Development Director
5	Backend Developer
6	Frontend Developer
7	Mobile Developer
8	Dev Ops Engineer
9	UI/UX Designer
10	Costumer Service

Perkembangan software development yang digunakan oleh beberapa software startup mulai meninggalkan cara lama secara perlahan. Mereka beralih ke metode pengembangan perangkat lunak yang gesit, kolaboratif [1], dan aman [20]. Sebagai contoh kita dapat melihat metode software development yang digunakan oleh software startup diatas yaitu menggunakan DevOps. Kemudian, dalam menentukan peran-peran (roles) dalam tingkat strategi pada software startup menggunakan metode RACI Matrix sedangkan untuk acuan strategi dalam SSDL menggunakan BSIMM [16]. Matriks RACI adalah alat untuk menggambarkan tanggung jawab pekerjaan [14] dan peran pemangku kepentingan serta menggunakan kepentingan dan pengaruh untuk mengklasifikasikan pemangku kepentingan dalam bentuk matriks [5]. Untuk tahapan pembuatan RACI Matrix dibuat menjadi tiga tahapan yaitu identifikasi proses, identifikasi stakeholder dan pemetaan RACI Matrix [6][7][15].



Hasil identifikasi peran di tingkat strategi menghasilkan 2 peran yaitu CEO dan CTO. Alasan mengapa hanya CEO dan CTO yang mengambil peran di tingkat strategi adalah

menurut Shenghui, struktur peran manajemen puncak sangat penting dalam kerjasama antar anggota manajemen puncak dalam mengarahkan organisasi dan membentuk strategi [10]. Dalam organisasi formal, struktur tim manajemen puncak terdiri dari berbagai jenis peran, seperti Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Financial Officer (CFO), Chief Strategy Officer (CSO), Chief Marketing Officer (CMO), Chief Digital Officer (CDO), Chief CSR Officer [10], Chief Technology Officer (CTO) [11][12], dan Chief Information Security Officer (CISO) [13]. Untuk melakukan mapping dari struktur top level management pada software startup dengan struktur formal organisasi berdasarkan [10], maka dibuat dalam dalam berikut.

No	TLM software Startup	TLM formal Organisasi	Status
1	CEO	CEO	Suitable
2	CTO	CTO	suitable
3	Web Development Director	COO	Not-suitable
4	Mobile Development Director	CFO	Not-suitable
5	Backend Developer	CSO	Not-suitable
6	Frontend Developer	CMO	Not-suitable
7	Mobile Developer	CDO	Not-suitable
8	Dev Ops	Chief CSR Officer	Not-suitable
9	UI/UX Designer	CISO	Not-suitable
10	Costumer Service	-	Not-suitable

Kemudian, Dalam BSIMM terdapat satu clause yang disebut strategy & metrics. Beberapa aktifitas dalam klausa ini adalah sebagai berikut :

Kode	Aktifitas
SM1.1:98	Publish process and evolve as necessary
SM1.3:82	Educate executives on software security
SM1.4:117	Implement security checkpoints and associated governance.
SM2.1:73	Publish data about software security internally and use it to drive change
SM2.2:63	Enforce security checkpoints and track exceptions
SM2.3:69	Create or grow a satellite (security champions)

SM2.6:71	Require security sign-off prior to software release.
SM2.7:64	Create evangelism role and perform internal marketing
SM3.1:27	Use a software asset tracking application with portfolio view.
SM3.2:18	Make SSI efforts part of external marketing.
SM3.3:26	Identify metrics and use them to drive resourcing.
SM3.4:5	Integrate software-defined lifecycle governance.
SM3.5:0	Integrate software supply chain risk management.

Klausa ini yang akan menjadi indikator aktifitas tingkat strategi untuk dimapping dengan peran yang sudah diidentifikasi sebelumnya. Dari proses pemetaan role yang sesuai dengan top level management formal organisasi, maka untuk kasus software startup terdiri dari dua role yaitu CEO dan CTO. Dari kedua role ini akan dibuat pemetaan terhadap aktifitas-aktifitas dalam siklus pengembangan perangkat lunak yang aman (SSDL) dalam BISMM sebagai berikut.

No	**Activity**	**Stakeholder**	
		CEO	**CTO**
A1	Publish process and evolve as necessary.	A, I	R
A2	Educate executives on software security.	R	C
A3	Implement security checkpoints and associated governance.	A, I	R
A4	Publish data about software security internally and use it to drive change.	R	C
A5	Enforce security checkpoints and track exceptions.	R	C
A6	Create or grow a satellite (security champions).	R	C
A7	Require security sign-off prior to software release.	A	R
A8	Create evangelism role and perform internal marketing.	R	C

A9	Use a software asset-tracking application with a portfolio view.	I	R
A10	Make SSI efforts part of external marketing.	R	C
A11	Identify metrics and use them to drive resourcing.	I	R
A12	Integrate software-defined lifecycle governance.	I	R
A13	Integrate software supply chain risk management.	R	C

Dari tabel diatas, jumlah peran yang harus dijalankan oleh CEO dan CTO sangat banyak. Hal ini dapat dianalisis dengan menggunakan dua cara, yaitu analisis vertikal dan analisis horizontal. pertama, hasil perhitungan R, A, C, I dari arah vertikal adalah sebagai berikut.

CEO	**Total**	**CTO**	**total**
R	7	R	6
A	3	A	0
C	0	C	7
I	5	I	0

Dengan total 7 Respnsible, CEO memiliki peran paling banyak dalam menjalankan pekerjaannya disusul CTO yang memiliki 6 Responsible. Pada baris kedua terdapat 3 CEO yang Accountable, sedangkan CTO tidak memiliki peran Accountable. kemudian pada baris ketiga, CEO tidak memiliki peran sebagai Consulted sedangkan CTO memiliki peran sebagai Consulted sebesar 7. Terakhir, CEO memiliki peran sebagai Informed sebesar 5 dan CTO tidak memiliki peran sebagai sebagai Informed. sekarang dilihat dari hasil analisis horizontal. Kemudian dari arah horizontal adalah sebagai berikut.

Activities	**Total**			
	R	**A**	**C**	**I**
A1	1	1		1
A2	1		1	
A3	1	1		1
A4	1		1	
A5	1		1	
A6	1		1	
A7	1	1		
A8	1		1	
A9	1			1

A10	1	1	
A11	1		1
A12	1		1
A13	1		1

Hasil penelitian menunjukkan bahwa dengan banyaknya peran yang dilakukan oleh CEO dan CTO dalam mengembangkan perangkat lunak yang aman, perangkat lunak startup akan mengalami fase ketidakstabilan kinerja. Menurut Shenghui Ma, jika suatu organisasi menerapkan peran informal dalam struktur organisasi, maka akan berdampak pada kinerja organisasi [10]. Selain itu, menurut Jose Santisteban dan David Mauricio, kinerja produk dan/atau layanan yang tinggi memuaskan kebutuhan pelanggan [17]. Jika dianalisis dari vertikal, CEO dan CTO memiliki peran yang paling bertanggung jawab. Dan ini dapat diartikan bahwa kedua peran tersebut merupakan peran kritis yang jika salah satu gagal menjalankan perannya maka proses pengembangan perangkat lunak yang aman tidak akan tercapai. Kemudian, banyaknya beban tanggung jawab yang dimiliki kedua peran tersebut sangat tidak efektif dalam sebuah organisasi. Namun di sisi lain, jika dianalisis secara horizontal, software startup memiliki tanggung jawab yang jelas. siapa yang melakukan pekerjaan, siapa yang membuat keputusan dan siapa yang mendapatkan informasi dari pekerjaan tersebut.

Dengan menerapkan metode pengembangan perangkat lunak yang sesuai untuk startup perangkat lunak dan telah memenuhi kebutuhan stakeholder, maka tingkat keberhasilan produk perangkat lunak yang dihasilkan akan semakin baik [2]. Beberapa metode pengembangan perangkat lunak yang aman yang digunakan sebagai praktik terbaik di dunia saat ini adalah Microsoft Security Development Lifecycle, Building Security in Maturity Model (BSIMM), dan OWASP Software Assurance Maturity Model (OWASP SAMM), dan lainnya [18].

Software startup menghadapi tantangan antara lain kurangnya pengalaman, sumber daya yang terbatas, pengaruh dari beberapa entitas [3], dan pasar dan teknologi yang dinamis untuk memasuki pasar target dengan potensi tinggi [4]. Dan salah satu karakteristik yang menyebabkan kegagalan software startup adalah mereka lebih memilih keputusan berisiko pada produk yang dihasilkan daripada yang aman [19]. Maka dari penjelasan di atas dapat disimpulkan bahwa peran manajemen tingkat atas sangat diperlukan dalam mendukung

pembuatan strategi yang tepat dalam mengimplementasikan secure software development lifecycle (SSDL) dalam memproduksi produk perangkat lunaknya.

LUARAN PENELITIAN (***Target***).

Luaran untuk tahun pertama ini adalah jurnal internasional dengan reputasi scopus Q3. Untuk tempat jurnal yg sudah disubmit yaitu di Computer Science and Information Systems (Comsis) dengan URL : http://www.comsis.org

KENDALA PELAKSANAAN PENELITIAN (*Constraint*).

Daftar Pustaka (*References*)

1. Masood, Z., Hoda, R., Blincoe, K., Damian, D., "Like, Dislike, or Just Do It? How developers approach software development tasks", in Information and Software Technology 150 (2022). DOI: https://doi.org/10.1016/j.infsof.2022.106963
2. Parthasarathy, S., "A Decision Framework for Software Startups to Succeed in COVID-19 Environment", in Decision Analytic Journal 3 (2022). DOI: https://doi.org/10.1016/j.dajour.2022.100037
3. Suominen, A., Hyrynsalmi, S., Still, K., "Software Start-up Failure an Exploratory Study on the Impact of Investment", in IWSECO (2017).
4. Paternoster, N., Giardino, C., Unterkalmsteiner, M., Gorschek, T., Abrahamsson, P.," Software Development in Startup Companies: A Systematic Mapping Study", in Information and Software Technology 56 (2014). DOI: http://dx.doi.org/10.1016/j.infsof.2014.04.014
5. Hirmer, S.A., George-Williams, H., Rhys, J., McNicholl, D., McCulloch, M., "Stakeholder Decision-making: Understanding Sierra Leone's Energy sector", in Renewable and Sustainable Energy Reviews 145 (2021). DOI: https://doi.org/10.1016/j.rser.2021.111093
6. Tom Hilman., "Make Governance Easy With A RACI Matrix", June 4, (2021). Access at: https://immutableinc.io/make-governance-easy-with-a-raci-matrix/
7. Templatelab., "How to Make a RACI Matrix?", Access on September 21, (2022) at: https://templatelab.com/raci-chart/#How_to_Make_a_RACI_Matrix
8. Dan Strutzel., "30 DAYS TO A MORE POWERFUL BUSINESS VOCABULARY: The 500 Words You Need to Transform Your Career and Your Life", Published by Gildan Media LLC, (2020). eISBN: 978-1-7225-2428-9
9. Alan Williamson., "Think Like a CTO", Published by Manning Publications, (2022)
10. Shenghui Ma., Yasemin Y. Kor., David Seidl., "Top Mangement Team Roles Structure: A Vintage Point for Advincing Upper Echelons Research", Article in Strategic Management Journal, August (2022). DOI: 10.1002/smj.3368

11. Nathan J. Hiller., Marie-Michele Beauchesne., “Executive Leadership: CEOs, Top Management Teams, and Organizational-Level Outcomes”, in ResearchGate, May (2014). DOI: 10.1093/oxfordhb/9780199755615.013.028
12. Frank Tietze., Cornelius Herstatt., “The Role of the Chied Technology Officer – Responsibilities, Skills & Qualifications and Organizational Integration”, in ResearchGate, January (2007)
13. Pedro Monzelo., Sergio Nunes., “The Role of the Chied Information Security Officer (CISO) in Organizations”, in Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI), June (2019). ISSN 2183-489X
14. Rahmad Dwi Putra Suhanda, Devi Pratami., “RACI Matrix Design for Managing Stakeholders in Project Case Study of PT.XYZ”, in International Journal of Innovation in Enterprise System (IJIES), (2021). e-ISSN: 2580-3050
15. Woo-yeon Lee, Seung-hoon Lee, Chengquan Jin, and Chang-taek Hyun., “Development of the RACI Model for Processes of the Closure Phase in Construction Programs”, in Sustainability, (2021). doi.org/10.3390/su13041806
16. Migues, S., Steven, J., Ware, M., “Building Security In Maturity Model (BSIMM) Version 13”, Creative Commons Attribution-Share Alike 3.0, California (2022).
17. Jose Santisteban, David Mauricio, Orestes Cachay., “Critical Success Factors for technology-based startups”, in International Journal of Entrepreneurship and Small Business, January (2020). DOI:10.1504/IJESB.2020.10035620
18. Monica, I., Daniela, S.C., Espen, A.J., ”A Framework for a Sustainable Software Security Program”, in Evolving Software Processes : Trends and Future Directions, (2022). ISBN 978-1-119-82126-7
19. Rahmat, N., Mohammad, I.A., Djoko, S.G., “Characteristics of startup company and its strategy: Analysis of Indonesia fashion startup companies”, in International Journal of Engineering & Technology, (2018)
20. Alenezi, M., Basit, H.A., Beg, M.A., Shaukat, M.S., “Synthesizing secure software development activities for linear and agile lifecycle models”, in Journal of Software : Practice and Experience, January (2022). DOI : doi.org/10.1002/spe.3072

Lampiran (appendicies)

Lampiran 1. BUKTI LUARAN PENELITIAN

Strategy indicators for SSDL in software startups based on ISG

R. Rizal Isnanto[1], Jatmiko E. Suseno[2], and Doddy Ferdiansyah[3,4]

[1] Departement of Computer Engineering, Diponegoro University,
Semarang, Indonesia
rizal@lecturer.undip.ac.id
[2] Departement of Physics, Diponegoro University,
Semarang, Indonesia
jatmikoendro@lecturer.undip.ac.id
[3] Program of Information System Doctoral, Diponegoro University,
Semarang, Indonesia
[4] Departement of Informatics Engineering, Pasundan University,
Bandung, Indonesia
doddyferdiansyah@students.undip.ac.id

Abstract. The development of startup software is massive because many services have turned digital. Various applications have emerged that match their functions by taking advantage of the momentum of digital transformation. For example, applications for the Education sector, industrial sector, and economic sector. With their top priority being generating applications, the security factor becomes less of a concern. This is evidenced by the many data breaches that have caused losses to serious companies and public institutions. This is where the role of top-level management emerges in restructuring the company's strategy, especially software startups, to support producing more secure applications. In this study, the RACI matrix is used to determine who is suitable for implementing a security strategy in information security governance within the organizational structure of the software startup. Where this study starts from stakeholder identification, top-level management roles in software startup, and activities in the secure software development lifecycle. And the results of this study are strategy indicators that are suitable for software startup

Keywords: information security governance, RACI matrix, startup software, strategy, top-level management.

1. Introduction

The development of software development used by some software startups began to leave the old methods slowly. They switched to agile and collaborative software development methods [1]. Likewise with software produced by startups, the security aspect of the product from startup software must be improved. Because software security is a very important concern and security activities need to support the software development cycle process [20] So, for a software startup, besides assets in the form of software products such as software as a service, another asset that must be maintained is the software development method they apply [2,3]. By applying a software development method that is suitable for software startups and has met the needs of stakeholders, the success rate of the resulting software product will be even better [2]. One is increasing the security factor in the software development process or the secure software development lifecycle. For example, some of the safe software development methods that are used as best practices in the world today are the Microsoft security development lifecycle, the Building Security in Maturity Model (BSIMM), and the OWASP Software Assurance Maturity Model (OWASP SAMM), and others [18].

However, not all software startups successfully implement good software development methods. This can happen because of the challenges of the startups themselves. As mentioned by Suominen, software startups face challenges including the lack of experience, limited resources, influence from several entities [3], and dynamic markets and technologies to enter the target market with high potential [4]. Not only that, when it comes to software startups, the characteristics of the organizations within them are very different from those of larger companies. And one of the characteristics that causes the failure of startup software is that they prefer risky decisions on the resulting product rather than a secure one [19]. So from the explanation above it can be concluded that the role of top-level management is needed in supporting making the right strategy in implementing secure software development lifecycle (SSDL) in producing their software products.

Top-level management roles in software startup determine the success of the SSDL implementation strategy. The main objective in this study, to determine the appropriate roles in software startup, we use the RACI Model with three main steps, namely identifying stakeholders related to startup software, then identifying what top-level roles are currently being carried out by startup software, and finally identify what activities are in SSDL. In this case, one of the SSDL methods is used, namely the Building Security in Maturity Model (BSIMM), which focuses only on the strategy section [16].

2. Methodology

In conducting this study, several steps were taken to solve the problems raised in this study. The steps taken are to determine the research framework, identify stakeholders, identify roles that will be determined as top-level management, and identify what activities are involved in the secure software development lifecycle (SSDL) process. One of the SSDL methods used in this study is BSIMM, where the domains in BSIMM consist of 4 domains namely governance, intelligence, SSDL touchpoints, and deployment. In this study, the domain that is our focus is Governance. For activities in the governance domain, it consists of 3 namely strategy & metrics (SM), Compliance & Policy (CP), and Training (T) [16]. Specifically for this study, we only take strategy & matrix (SM) activities which will be mapped with identification results from stakeholders and the role of top-level management in startup software. After carrying out all these steps, the results require discussion regarding the results produced.

2.1. Research Framework

This study uses the RACI matrix method to determine the roles and responsibilities at the top-level management for all SSDL activities. The RACI matrix is a tool for describing job responsibilities [14] and the roles of stakeholders and using interests and influence to classify stakeholders in the form of a matrix [5]. Usually, the RACI matrix describes the relationship between jobs and determines the roles, responsibilities, and levels of authority for each activity. Another term that is more often seen by others is called the RACI matrix RACI stands for

• Responsible: Who is going to be completing the task?
• Accountable: Who is ultimately responsible for a task and can also delegate to those who are Responsible?
• Consulted: Who will need consulting about the activity, and where will there be two-way communication on the matter?
• Informed: Who must be kept informed, although there is just one-way communication?

To create a RACI matrix, several steps must be met. The first step is to define or identify all tasks. The second step is to list all stakeholders with interest in the project. The third step is to fill the sections determining who is responsible and accountable. It would help if those who will be consulted and informed before doing every task are also mentioned. The fourth step is to ensure that everyone has at least one stakeholder, and they will be responsible for each task [6][7]. The RACI matrix is made into three stages, namely, process identification, stakeholder identification, and RACI matrix mapping [15].

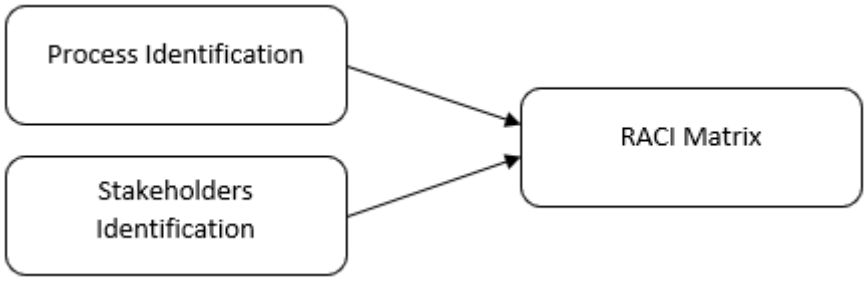


Fig 1. Three stages of the RACI matrix.

2.2. Identification of Stakeholders in Software Startup

In this first study, we interviewed the Chief Executive Officer (CEO) of a software startup in Bandung, Indonesia. The results of interviews regarding what roles are in the startup software are as follows:

Table 1. List of stakeholders and description.

No	Role	Description
1	CEO	The Chief Executive Officer (CEO) is the highest position in a company. His responsibilities as the Board of Trustees for the company's success or failure [8].
2	CTO	The Chief Technology Officer (CTO) is responsible for the technology vision and execution of a company [9].
3	Web Development Director	The Director of Web Development will manage team members and contribute to team web development and growth.
4	Mobile Development Director	The Director of Mobile Development will manage team members and contribute to team mobile development and growth.
5	Backend Developer	Backend Developers are the experts who build and maintain the mechanisms that process data and perform actions on websites.
6	Frontend Developer	A Frontend Developer is a person who will use any of the frameworks or the packages such as Jquery, Angular JS, Angular JS 2, NodeJS, ReactJs, backboneJS, and Bootstrap.
7	Mobile Developer	A mobile developer creates software for mobile devices and technology.
8	DevOps Engineer	A DevOps Engineer introduces processes, tools, and methodologies to balance the needs throughout the software development life cycle, from coding and deployment to maintenance and updates.
9	UI/UX Designer	A UX/UI Designer carries out user research first and then implements the findings in the visual design in mockups, wireframes, and prototypes.
10	Customer Service	Customer Service is the direct one-on-one interaction between a consumer making a purchase and a representative of the company selling it.

2.3. Identify Top-Level Roles in Software Startup

According to Shenghui et al., the role structure of top management is very important in cooperating among members of top management in directing the organization and forming strategy [10]. In a formal organization, the structure of the top management team consists of various types of roles, such as the Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Financial Officer (CFO), Chief Strategy Officer (CSO), Chief Marketing Officer (CMO), Chief Digital Officer (CDO), Chief CSR officer [10], Chief Technology Officer (CTO) [11][12], and Chief Information Security Officer (CISO) [13]. Each position in top management is very important in carrying out organizational activities according to their roles and responsibilities [10]. Table 2 shows the mapping of the top-level management structure on startup software with the formal organizational structure based on [10].

Table 2. Mapping top-level management structure to formal organization structure in software startups.

No	TLM software startup	TLM formal organization	Status
1	CEO	CEO	Suitable
2	CTO	CTO	Suitable

3	Web Development Director	COO	Not suitable
4	Mobile Development Director	CFO	Not suitable
5	Backend Developer	CSO	Not suitable
6	Frontend Developer	CMO	Not suitable
7	Mobile Developer	CDO	Not suitable
8	Dev Ops	Chief CSR Officer	Not suitable
9	UI/UX Designer	CISO	Not suitable
10	Customer Service	–	Not suitable

Table 2 shows that there are only two roles in top-level management in software startups that follow the organization's formal top-level management standards, CEO and CTO.

2.4. Activity Identification on SSDL

In the SSDL, many methods can be applied by a software startup. One of the SSDL methods applied in this study is the Building Security in Maturity Model (BSIMM). The BSIMM studies current software security initiatives or programs. It quantifies the application security (appsec) practices of different organizations across industries, sizes, and geographies while identifying the variations that make each organization unique [16]. In the BSIMM, there is one clause called strategy and metrics. Table 3 shows some of the activities in this clause.

Table 3. Activity strategy and metrics in the building security in maturity model (BSIMM).

Code	Activity
SM1.1:98	Publish process and evolve as necessary
SM1.3:82	Educate executives on software security
SM1.4:117	Implement security checkpoints and associated governance.
SM2.1:73	Publish data about software security internally and use it to drive change
SM2.2:63	Enforce security checkpoints and track exceptions
SM2.3:69	Create or grow a satellite (security champions)
SM2.6:71	Require security sign-off prior to software release.
SM2.7:64	Create evangelism role and perform internal marketing
SM3.1:27	Use a software asset-tracking application with a portfolio view.
SM3.2:18	Make SSI efforts part of external marketing.
SM3.3:26	Identify metrics and use them to drive resourcing.
SM3.4:5	Integrate software-defined lifecycle governance.
SM3.5:0	Integrate software supply chain risk management.

3. Results

From the role mapping process under the organization's formal top-level management, the software startup case consists of two roles: CEO and CTO. From these two roles, a mapping of the activities in the SSDL in the BISMM is created, as shown in Table 4.

Table 4. Results from the RACI matrix for each activity in the secure software development lifecycle (SSDL).

No	Activity	Stakeholder	
		CEO	CTO
A1	Publish process and evolve as necessary.	A, I	R

A2	Educate executives on software security.	R	C
A3	Implement security checkpoints and associated governance.	A, I	R
A4	Publish data about software security internally and use it to drive change.	R	C
A5	Enforce security checkpoints and track exceptions.	R	C
A6	Create or grow a satellite (security champions).	R	C
A7	Require security sign-off prior to software release.	A	R
A8	Create evangelism role and perform internal marketing.	R	C
A9	Use a software asset-tracking application with a portfolio view.	I	R
A10	Make SSI efforts part of external marketing.	R	C
A11	Identify metrics and use them to drive resourcing.	I	R
A12	Integrate software-defined lifecycle governance.	I	R
A13	Integrate software supply chain risk management.	R	C

Table 4 concludes that a software startup implementing an informal role structure in top-level management will result in interpersonal conflicts within the top management team. Additionally, the workload of the CEO and CTO will be even greater. From table 4 above, the number of roles that must be carried out by the CEO and CTO is very large. This can be analyzed using two ways, namely vertical analysis and horizontal analysis. first, the results of calculating R, A, C, I from the vertical direction are as follows.

Table 5. Total RACI of Vertical

CEO	**Total**	**CTO**	**total**
R	7	R	6
A	3	A	0
C	0	C	7
I	5	I	0

With a total of 7 responsible, the CEO has the most roles in carrying out his work followed by the CTO who has 6 responsible. In the second row, there are 3 accountable CEOs, while the CTO does not have an accountable role. then in the third row, the CEO does not have a consulted role while the CTO has a consulted role of 7. Finally, the CEO has an informed role of 5 and the CTO does not have an informed role. now seen from the results of the horizontal analysis.

Tabel 6. Total RACI of Horizontal

Activities	**Total**			
	R	**A**	**C**	**I**

A1	1	1		1
A2	1		1	
A3	1	1		1
A4	1		1	
A5	1		1	
A6	1		1	
A7	1	1		
A8	1		1	
A9	1			1
A10	1		1	
A11	1			1
A12	1			1
A13	1			1

4. Discussion

The results of the study show that with the many roles performed by CEOs and CTOs in developing secure software, startup software will experience a phase of performance instability. According to Shenghui Ma, if an organization applies for an informal role in the organizational structure, it will impact organizational performance [10]. Moreover, according to Jose Santisteban and David Mauricio, a product and/or service's high performance satisfies customers' needs [17]. When analyzed from the vertical, the CEO and CTO have the most responsible roles. And this can be interpreted that both roles are critical roles which if one fails to carry out its role then the secure software development process will not be achieved. Then, the many responsible burdens that are owned by the two roles are very ineffective in an organization. But on the other hand, if analyzed horizontally, startup software has clear responsibilities. who does the work, who makes the decisions and who gets the information from the work.

When an organization's performance is disrupted, the resulting software product does not match the user's needs. What is very worrying is that when a startup shows symptoms like that, the startup software will be at risk of failure because perceived performance influences a startup's success. Therefore, in the next study, we will identify what positions should be in the software startup and what roles are more suitable for each.

5. Conclusions

Seperti yang dikatakan oleh Alenezi et al, sebuah perangkat lunak yang kurang aman itu dikarenakan pengembang tidak memiliki pengetahuan keamanan itu sendiri [20]. Pengetahuan keamanan ini juga tidak hanya berlaku bagi programmer atau operator, tetapi juga harus dimiliki oleh para top-level management. Sehingga apa yang di inginkan oleh software startup dengan tujuan dari SSDL dapat berjalan dengan bersama-sama.

In the case of this study, the roles of the CEO and CTO in software startups are numerous and have high intensity. The worry is that they will get stressed more quickly and result in ineffective decision-making by them as top level management. Even though the roles and responsibilities are good. Suggestions for startup software that has the RACI matrix results above are that the CEO and CTO must be able to shift some of the responsibilities they carry to the middle level management and lower level management. So that the load will be more evenly distributed and balanced, and the management will be better in determining the strategy in software startup.

Ketika mereka sudah berada dijalan yang sama, maka produk software yang dihasilkan akan lebih aman, walaupun menurut Al-Dhahri et al, dalam menangani keamanan dalam sebuah sistem, tidak ada yang dapat menjamin 100% keamanan dari sistem tersebut [21]

6. References

1. Masood, Z., Hoda, R., Blincoe, K., Damian, D., "Like, Dislike, or Just Do It? How developers approach software development tasks", in Information and Software Technology 150 (2022). DOI: https://doi.org/10.1016/j.infsof.2022.106963
2. Parthasarathy, S., "A Decision Framework for Software Startups to Succeed in COVID-19 Environment", in Decision Analytic Journal 3 (2022). DOI: https://doi.org/10.1016/j.dajour.2022.100037
3. Suominen, A., Hyrynsalmi, S., Still, K., "Software Start-up Failure an Exploratory Study on the Impact of Investment", in IWSECO (2017).
4. Paternoster, N., Giardino, C., Unterkalmsteiner, M., Gorschek, T., Abrahamsson, P.," Software Development in Startup Companies: A Systematic Mapping Study", in Information and Software Technology 56 (2014). DOI: http://dx.doi.org/10.1016/j.infsof.2014.04.014
5. Hirmer, S.A., George-Williams, H., Rhys, J., McNicholl, D., McCulloch, M., "Stakeholder Decision-making: Understanding Sierra Leone's Energy sector", in Renewable and Sustainable Energy Reviews 145 (2021). DOI: https://doi.org/10.1016/j.rser.2021.111093
6. Tom Hilman., "Make Governance Easy With A RACI Matrix", June 4, (2021). Access at: https://immutableinc.io/make-governance-easy-with-a-raci-matrix/
7. Templatelab., "How to Make a RACI Matrix?", Access on September 21, (2022) at: https://templatelab.com/raci-chart/#How_to_Make_a_RACI_Matrix
8. Dan Strutzel., "30 DAYS TO A MORE POWERFUL BUSINESS VOCABULARY: The 500 Words You Need to Transform Your Career and Your Life", Published by Gildan Media LLC, (2020). eISBN: 978-1-7225-2428-9
9. Alan Williamson., "Think Like a CTO", Published by Manning Publications, (2022)
10. Shenghui Ma., Yasemin Y. Kor., David Seidl., "Top Mangement Team Roles Structure: A Vintage Point for Advincing Upper Echelons Research", Article in Strategic Management Journal, August (2022). DOI: 10.1002/smj.3368
11. Nathan J. Hiller., Marie-Michele Beauchesne., "Executive Leadership: CEOs, Top Management Teams, and Organizational-Level Outcomes", in ResearchGate, May (2014). DOI: 10.1093/oxfordhb/9780199755615.013.028
12. Frank Tietze., Cornelius Herstatt., "The Role of the Chied Technology Officer – Responsibilities, Skills & Qualifications and Organizational Integration", in ResearchGate, January (2007)
13. Pedro Monzelo., Sergio Nunes., "The Role of the Chied Information Security Officer (CISO) in Organizations", in Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI), June (2019). ISSN 2183-489X
14. Rahmad Dwi Putra Suhanda, Devi Pratami., "RACI Matrix Design for Managing Stakeholders in Project Case Study of PT.XYZ", in International Journal of Innovation in Enterprise System (IJIES), (2021). e-ISSN: 2580-3050
15. Woo-yeon Lee, Seung-hoon Lee, Chengquan Jin, and Chang-taek Hyun., "Development of the RACI Model for Processes of the Closure Phase in Construction Programs", in Sustainability, (2021). doi.org/10.3390/su13041806
16. Migues, S., Steven, J., Ware, M., "Building Security In Maturity Model (BSIMM) Version 13", Creative Commons Attribution-Share Alike 3.0, California (2022).
17. Jose Santisteban, David Mauricio, Orestes Cachay., "Critical Success Factors for technology-based startups", in International Journal of Entrepreneurship and Small Business, January (2020). DOI:10.1504/IJESB.2020.10035620
18. Monica, I., Daniela, S.C., Espen, A.J., "A Framework for a Sustainable Software Security Program", in Evolving Software Processes : Trends and Future Directions, (2022). ISBN 978-1-119-82126-7
19. Rahmat, N., Mohammad, I.A., Djoko, S.G., "Characteristics of startup company and its strategy: Analysis of Indonesia fashion startup companies", in International Journal of Engineering & Technology, (2018)
20. Alenezi, M., Basit, H.A., Beg, M.A., Shaukat, M.S., "Synthesizing secure software development activities for linear and agile lifecycle models", in Journal of Software : Practice and Experience, January (2022). DOI : doi.org/10.1002/spe.3072
21. Al-Dhahri, S., Al-Sarti, M., Abdaziz, A., " Information Security Management System", in International Journal of Computer Applications, January (2017)

Sertifikat Proof Reading

enago
Author First, Quality First
www.enago.com

ulatus
localize to globalize
www.ulatus.com

voxtab
we are all ears
www.voxtab.com

CERTIFICATE OF EDITING

This is to certify that the paper titled **Strategy indicators for SSDL in software startups based on ISG** commissioned to us by **Doddy Ferdiansyah** has been edited for English language, grammar, punctuation, and spelling by Enago, the editing brand of Crimson Interactive Inc. under Top Impact Editing B2C.

- ISO 17100:2015 Translation Service Providers
- ISO 27001:2013 Information Security Management System
- ISO 9001:2015 Quality Management System

Issued by:
Enago, Crimson Interactive Inc.
160, Greentree Dr, Ste 101 street,
Dover City, Kent, Delaware, 19904
Phone: +1-302-498-8358

Disclaimer : The intent of the author's message has been preserved during the editing process. The author is free to accept or reject our changes in the document after reviewing our edits. This certificate has been awarded at the time of sharing the final edited version (full file or sections of the file) with the author. Enago does not bear any responsibility for any alterations done by the author to the edited document post **16 Nov 2022**.

Japan	www.enago.jp, www.ulatus.jp, www.voxtab.jp	**Russia**	www.enago.ru	**About Crimson:**	
Taiwan	www.enago.tw, www.ulatus.tw	**Arabic**	www.enago.ae	Crimson Interactive INC is one of the world's leading academic research support services. Since 2005, we've supported over 2 million researchers in 125 countries with their publication goals.	
China	www.enago.cn, www.ulatus.cn	**Turkey**	www.enago.com.tr		
Brazil	www.enago.com.br, www.ulatus.com.br	**S. Korea**	www.enago.co.kr		
Germany	www.enago.de	**Global**	www.enago.com, www.ulatus.com, www.voxtab.com		

Bukti submit Jurnal

From: Mirjana Ivanović
Sent: Tuesday, November 29, 2022 7:10 PM
To: Doddy Ferdiansyah
Subject: [ComSIS] Submission Acknowledgement - #15395

Dear Dr. Doddy Ferdiansyah,

let me thank you for submitting the manuscript #15395, "Strategy indicators for SSDL in software startups based on ISG" to journal Computer Science and Information Systems. You will be able to track its progress through the reviewing procedure by logging in to the journal web site:

Manuscript URL:
https://ojs.pmf.uns.ac.rs/index.php/comsis/author/submission/15395
Username: doy2kali1

If you have any questions, please do not hesitate to contact me.

Best regards,
Mirjana Ivanović
Computer Science and Information Systems
--
ComSIS - Computer Science and Information Systems journal
http://www.comsis.org/

Active Submissions

ACTIVE ARCHIVE

ID	MM-DD SUBMIT	SEC	AUTHORS	TITLE
15395	11-29	ART	Isnanto, Suseno, Ferdiansyah	STRATEGY INDICATORS FOR SSDL IN SOFTWARE STARTUPS BASED...

Computer Science and Information Systems 00(0):0000–0000 https://doi.org/10.2298/CSIS123456789X

Strategy indicators for SSDL in software startups based on ISG

R. Rizal Isnanto[1], Jatmiko E. Suseno[2], and Doddy Ferdiansyah[3,4]

[1] Departement of Computer Engineering, Diponegoro University, Semarang, Indonesia
rizal@lecturer.undip.ac.id
[2] Departement of Physics, Diponegoro University, Semarang, Indonesia
jatmikoendro@lecturer.undip.ac.id
[3] Program of Information System Doctoral, Diponegoro University, Semarang, Indonesia
[4] Departement of Informatics Engineering, Pasundan University, Bandung, Indonesia
doddyferdiansyah@students.undip.ac.id

Abstract. The development of startup software is massive because many services have turned digital. Various applications have emerged that match their functions by taking advantage of the momentum of digital transformation. For example, applications for the Education sector, industrial sector, and economic sector. With their top priority being generating applications, the security factor becomes less of a concern. This is evidenced by the many data breaches that have caused losses to serious companies and public institutions. This is where the role of top-level management emerges in restructuring the company's strategy, especially software startups, to support producing more secure applications. In this study, the RACI matrix is used to determine who is suitable for implementing a security strategy in information security governance within the organizational structure of the software startup. Where this study starts from stakeholder identification, top-level management roles in software startup, and activities in the secure software development lifecycle. And the results of this study are strategy indicators that are suitable for software startup

Keywords: information security governance, RACI matrix, startup software, strategy, top-level management.

1. Introduction

The development of software development used by some software startups began to leave the old methods slowly. They switched to agile and collaborative software development methods [1]. Likewise with software produced by startups, the security aspect of the product from startup software must be improved. Because software security is a very important concern and security activities need to support the software

development cycle process [20] So, for a software startup, besides assets in the form of software products such as software as a service, another asset that must be maintained is the software development method they apply [2,3]. By applying a software development method that is suitable for software startups and has met the needs of stakeholders, the success rate of the resulting software product will be even better [2]. One is increasing the security factor in the software development process or the secure software development lifecycle. For example, some of the safe software development methods that are used as best practices in the world today are the Microsoft security development lifecycle, the Building Security in Maturity Model (BSIMM), and the OWASP Software Assurance Maturity Model (OWASP SAMM), and others [18].

However, not all software startups successfully implement good software development methods. This can happen because of the challenges of the startups themselves. As mentioned by Suominen, software startups face challenges including the lack of experience, limited resources, influence from several entities [3], and dynamic markets and technologies to enter the target market with high potential [4]. Not only that, when it comes to software startups, the characteristics of the organizations within them are very different from those of larger companies. And one of the characteristics that causes the failure of startup software is that they prefer risky decisions on the resulting product rather than a secure one [19]. So from the explanation above it can be concluded that the role of top-level management is needed in supporting making the right strategy in implementing secure software development lifecycle (SSDL) in producing their software products.

Top-level management roles in software startup determine the success of the SSDL implementation strategy. The main objective in this study, to determine the appropriate roles in software startup, we use the RACI Model with three main steps, namely identifying stakeholders related to startup software, then identifying what top-level roles are currently being carried out by startup software, and finally identify what activities are in SSDL. In this case, one of the SSDL methods is used, namely the Building Security in Maturity Model (BSIMM), which focuses only on the strategy section [16].

2. Methodology

In conducting this study, several steps were taken to solve the problems raised in this study. The steps taken are to determine the research framework, identify stakeholders, identify roles that will be determined as top-level management, and identify what activities are involved in the secure software development lifecycle (SSDL) process. One of the SSDL methods used in this study is BSIMM, where the domains in BSIMM consist of 4 domains namely governance, intelligence, SSDL touchpoints, and deployment. In this study, the domain that is our focus is Governance. For activities in the governance domain, it consists of 3 namely strategy & metrics (SM), Compliance & Policy (CP), and Training (T) [16]. Specifically for this study, we only take strategy & matrix (SM) activities which will be mapped with identification results from stakeholders and the role of top-level management in startup software. After carrying out all these steps, the results require discussion regarding the results produced.

2.1. Research Framework

This study uses the RACI matrix method to determine the roles and responsibilities at the top-level management for all SSDL activities. The RACI matrix is a tool for describing job responsibilities [14] and the roles of stakeholders and using interests and influence to classify stakeholders in the form of a matrix [5]. Usually, the RACI matrix describes the relationship between jobs and determines the roles, responsibilities, and levels of authority for each activity. Another term that is more often seen by others is called the RACI matrix RACI stands for

• Responsible: Who is going to be completing the task?
• Accountable: Who is ultimately responsible for a task and can also delegate to those who are Responsible?
• Consulted: Who will need consulting about the activity, and where will there be two-way communication on the matter?
• Informed: Who must be kept informed, although there is just one-way communication?

To create a RACI matrix, several steps must be met. The first step is to define or identify all tasks. The second step is to list all stakeholders with interest in the project. The third step is to fill the sections determining who is responsible and accountable. It would help if those who will be consulted and informed before doing every task are also mentioned. The fourth step is to ensure that everyone has at least one stakeholder, and they will be responsible for each task [6][7]. The RACI matrix is made into three stages, namely, process identification, stakeholder identification, and RACI matrix mapping [15].

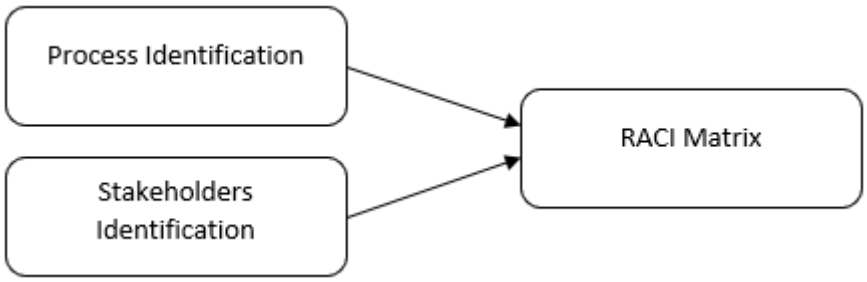


Fig 1. Three stages of the RACI matrix.

2.2. Identification of Stakeholders in Software Startup

In this first study, we interviewed the Chief Executive Officer (CEO) of a software startup in Bandung, Indonesia. The results of interviews regarding what roles are in the startup software are as follows:

Table 1. List of stakeholders and description.

No	Role	Description
1	CEO	The Chief Executive Officer (CEO) is the highest position in a company. His

No	Role	Description
		responsibilities as the Board of Trustees for the company's success or failure [8].
2	CTO	The Chief Technology Officer (CTO) is responsible for the technology vision and execution of a company [9].
3	Web Development Director	The Director of Web Development will manage team members and contribute to team web development and growth.
4	Mobile Development Director	The Director of Mobile Development will manage team members and contribute to team mobile development and growth.
5	Backend Developer	Backend Developers are the experts who build and maintain the mechanisms that process data and perform actions on websites.
6	Frontend Developer	A Frontend Developer is a person who will use any of the frameworks or the packages such as Jquery, Angular JS, Angular JS 2, NodeJS, ReactJs, backboneJS, and Bootstrap.
7	Mobile Developer	A mobile developer creates software for mobile devices and technology.
8	DevOps Engineer	A DevOps Engineer introduces processes, tools, and methodologies to balance the needs throughout the software development life cycle, from coding and deployment to maintenance and updates.
9	UI/UX Designer	A UX/UI Designer carries out user research first and then implements the findings in the visual design in mockups, wireframes, and prototypes.
10	Customer Service	Customer Service is the direct one-on-one interaction between a consumer making a purchase and a representative of the company selling it.

2.3. Identify Top-Level Roles in Software Startup

According to Shenghui et al., the role structure of top management is very important in cooperating among members of top management in directing the organization and forming strategy [10]. In a formal organization, the structure of the top management team consists of various types of roles, such as the Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Financial Officer (CFO), Chief Strategy Officer (CSO), Chief Marketing Officer (CMO), Chief Digital Officer (CDO), Chief CSR officer [10], Chief Technology Officer (CTO) [11][12], and Chief Information Security Officer (CISO) [13]. Each position in top management is very important in carrying out organizational activities according to their roles and responsibilities [10]. Table 2 shows

the mapping of the top-level management structure on startup software with the formal organizational structure based on [10].

Table 2. Mapping top-level management structure to formal organization structure in software startups.

No	TLM software startup	TLM formal organization	Status
1	CEO	CEO	Suitable
2	CTO	CTO	Suitable
3	Web Development Director	COO	Not suitable
4	Mobile Development Director	CFO	Not suitable
5	Backend Developer	CSO	Not suitable
6	Frontend Developer	CMO	Not suitable
7	Mobile Developer	CDO	Not suitable
8	Dev Ops	Chief CSR Officer	Not suitable
9	UI/UX Designer	CISO	Not suitable
10	Customer Service	–	Not suitable

Table 2 shows that there are only two roles in top-level management in software startups that follow the organization's formal top-level management standards, CEO and CTO.

2.4. Activity Identification on SSDL

In the SSDL, many methods can be applied by a software startup. One of the SSDL methods applied in this study is the Building Security in Maturity Model (BSIMM). The BSIMM studies current software security initiatives or programs. It quantifies the application security (appsec) practices of different organizations across industries, sizes, and geographies while identifying the variations that make each organization unique [16]. In the BSIMM, there is one clause called strategy and metrics. Table 3 shows some of the activities in this clause.

Table 3. Activity strategy and metrics in the building security in maturity model (BSIMM).

Code	Activity
SM1.1:98	Publish process and evolve as necessary
SM1.3:82	Educate executives on software security
SM1.4:117	Implement security checkpoints and associated governance.
SM2.1:73	Publish data about software security internally and use it to drive change
SM2.2:63	Enforce security checkpoints and track exceptions
SM2.3:69	Create or grow a satellite (security champions)
SM2.6:71	Require security sign-off prior to software release.
SM2.7:64	Create evangelism role and perform internal marketing
SM3.1:27	Use a software asset-tracking application with a portfolio view.
SM3.2:18	Make SSI efforts part of external marketing.

SM3.3:26	Identify metrics and use them to drive resourcing.
SM3.4:5	Integrate software-defined lifecycle governance.
SM3.5:0	Integrate software supply chain risk management.

3. Results

From the role mapping process under the organization's formal top-level management, the software startup case consists of two roles: CEO and CTO. From these two roles, a mapping of the activities in the SSDL in the BISMM is created, as shown in Table 4.

Table 4. Results from the RACI matrix for each activity in the secure software development lifecycle (SSDL).

No	**Activity**	**Stakeholder**	
		CEO	**CTO**
A1	Publish process and evolve as necessary.	A, I	R
A2	Educate executives on software security.	R	C
A3	Implement security checkpoints and associated governance.	A, I	R
A4	Publish data about software security internally and use it to drive change.	R	C
A5	Enforce security checkpoints and track exceptions.	R	C
A6	Create or grow a satellite (security champions).	R	C
A7	Require security sign-off prior to software release.	A	R
A8	Create evangelism role and perform internal marketing.	R	C
A9	Use a software asset-tracking application with a portfolio view.	I	R
A10	Make SSI efforts part of external marketing.	R	C
A11	Identify metrics and use them to drive resourcing.	I	R
A12	Integrate software-defined lifecycle governance.	I	R

No	Activity	Stakeholder	
		CEO	CTO
A13	Integrate software supply chain risk management.	R	C

Table 4 concludes that a software startup implementing an informal role structure in top-level management will result in interpersonal conflicts within the top management team. Additionally, the workload of the CEO and CTO will be even greater. From table 4 above, the number of roles that must be carried out by the CEO and CTO is very large. This can be analyzed using two ways, namely vertical analysis and horizontal analysis. first, the results of calculating R, A, C, I from the vertical direction are as follows.

Table 5. Total RACI of Vertical

CEO	Total	CTO	total
R	7	R	6
A	3	A	0
C	0	C	7
I	5	I	0

With a total of 7 responsible, the CEO has the most roles in carrying out his work followed by the CTO who has 6 responsible. In the second row, there are 3 accountable CEOs, while the CTO does not have an accountable role. then in the third row, the CEO does not have a consulted role while the CTO has a consulted role of 7. Finally, the CEO has an informed role of 5 and the CTO does not have an informed role. Now seen from the results of the horizontal analysis.

Tabel 6. Total RACI of Horizontal

Activities	Total			
	R	A	C	I
A1	1	1		1
A2	1		1	
A3	1	1		1
A4	1		1	
A5	1		1	
A6	1		1	
A7	1	1		
A8	1		1	
A9	1			1
A10	1		1	
A11	1			1
A12	1			1
A13	1			1

4. Discussion

The results of the study show that with the many roles performed by CEOs and CTOs in developing secure software, startup software will experience a phase of performance instability. According to Shenghui Ma, if an organization applies for an informal role in the organizational structure, it will impact organizational performance [10]. Moreover, according to Jose Santisteban and David Mauricio, a product and/or service's high performance satisfies customers' needs [17]. When analyzed from the vertical, the CEO and CTO have the most responsible roles. And this can be interpreted that both roles are critical roles which if one fails to carry out its role then the secure software development process will not be achieved. Then, the many responsible burdens that are owned by the two roles are very ineffective in an organization. But on the other hand, if analyzed horizontally, startup software has clear responsibilities. who does the work, who makes the decisions and who gets the information from the work.

When an organization's performance is disrupted, the resulting software product does not match the user's needs. What is very worrying is that when a startup shows symptoms like that, the startup software will be at risk of failure because perceived performance influences a startup's success. Therefore, in the next study, we will identify what positions should be in the software startup and what roles are more suitable for each.

5. Conclusions

As said by Alenezi et al, a software that is less secure is because the developer does not have security knowledge itself [20]. This security knowledge does not only apply to programmers or operators, but also must be possessed by top-level management. So what the startup software wants with the goal of SSDL can run together. In the case of this study, the roles of the CEO and CTO in software startups are numerous and have high intensity. The worry is that they will get stressed more quickly and result in ineffective decision-making by them as top level management. Even though the roles and responsibilities are good. Suggestions for startup software that has the RACI matrix results above are that the CEO and CTO must be able to shift some of the responsibilities they carry to the middle level management and lower level management. So that the load will be more evenly distributed and balanced, and the management will be better in determining the strategy in software startup. When they are on the same path, the resulting software product will be safer, although according to Al-Dhahri et al, in dealing with security in a system, no one can guarantee 100% security of the system [21]

6. References

1. Masood, Z., Hoda, R., Blincoe, K., Damian, D., "Like, Dislike, or Just Do It? How developers approach software development tasks", in Information and Software Technology 150 (2022). DOI: https://doi.org/10.1016/j.infsof.2022.106963

2. Parthasarathy, S., "A Decision Framework for Software Startups to Succeed in COVID-19 Environment", in Decision Analytic Journal 3 (2022). DOI: https://doi.org/10.1016/j.dajour.2022.100037
3. Suominen, A., Hyrynsalmi, S., Still, K., "Software Start-up Failure an Exploratory Study on the Impact of Investment", in IWSECO (2017).
4. Paternoster, N., Giardino, C., Unterkalmsteiner, M., Gorschek, T., Abrahamsson, P.," Software Development in Startup Companies: A Systematic Mapping Study", in Information and Software Technology 56 (2014). DOI: http://dx.doi.org/10.1016/j.infsof.2014.04.014
5. Hirmer, S.A., George-Williams, H., Rhys, J., McNicholl, D., McCulloch, M., "Stakeholder Decision-making: Understanding Sierra Leone's Energy sector", in Renewable and Sustainable Energy Reviews 145 (2021). DOI: https://doi.org/10.1016/j.rser.2021.111093
6. Tom Hilman., "Make Governance Easy With A RACI Matrix", June 4, (2021). Access at: https://immutableinc.io/make-governance-easy-with-a-raci-matrix/
7. Templatelab., "How to Make a RACI Matrix?", Access on September 21, (2022) at: https://templatelab.com/raci-chart/#How_to_Make_a_RACI_Matrix
8. Dan Strutzel., "30 DAYS TO A MORE POWERFUL BUSINESS VOCABULARY: The 500 Words You Need to Transform Your Career and Your Life", Published by Gildan Media LLC, (2020). eISBN: 978-1-7225-2428-9
9. Alan Williamson., "Think Like a CTO", Published by Manning Publications, (2022)
10. Shenghui Ma., Yasemin Y. Kor., David Seidl., "Top Mangement Team Roles Structure: A Vintage Point for Advincing Upper Echelons Research", Article in Strategic Management Journal, August (2022). DOI: 10.1002/smj.3368
11. Nathan J. Hiller., Marie-Michele Beauchesne., "Executive Leadership: CEOs, Top Management Teams, and Organizational-Level Outcomes", in ResearchGate, May (2014). DOI: 10.1093/oxfordhb/9780199755615.013.028
12. Frank Tietze., Cornelius Herstatt., "The Role of the Chied Technology Officer – Responsibilities, Skills & Qualifications and Organizational Integration", in ResearchGate, January (2007)
13. Pedro Monzelo., Sergio Nunes., "The Role of the Chied Information Security Officer (CISO) in Organizations", in Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI), June (2019). ISSN 2183-489X
14. Rahmad Dwi Putra Suhanda, Devi Pratami., "RACI Matrix Design for Managing Stakeholders in Project Case Study of PT.XYZ", in International Journal of Innovation in Enterprise System (IJIES), (2021). e-ISSN: 2580-3050
15. Woo-yeon Lee, Seung-hoon Lee, Chengquan Jin, and Chang-taek Hyun., "Development of the RACI Model for Processes of the Closure Phase in Construction Programs", in Sustainability, (2021). doi.org/10.3390/su13041806
16. Migues, S., Steven, J., Ware, M., "Building Security In Maturity Model (BSIMM) Version 13", Creative Commons Attribution-Share Alike 3.0, California (2022).
17. Jose Santisteban, David Mauricio, Orestes Cachay., "Critical Success Factors for technology-based startups", in International Journal of Entrepreneurship and Small Business, January (2020). DOI:10.1504/IJESB.2020.10035620
18. Monica, I., Daniela, S.C., Espen, A.J., "A Framework for a Sustainable Software Security Program", in Evolving Software Processes : Trends and Future Directions, (2022). ISBN 978-1-119-82126-7
19. Rahmat, N., Mohammad, I.A., Djoko, S.G., "Characteristics of startup company and its strategy: Analysis of Indonesia fashion startup companies", in International Journal of Engineering & Technology, (2018)
20. Alenezi, M., Basit, H.A., Beg, M.A., Shaukat, M.S., "Synthesizing secure software development activities for linear and agile lifecycle models", in Journal of Software : Practice and Experience, January (2022). DOI : doi.org/10.1002/spe.3072
21. Al-Dhahri, S., Al-Sarti, M., Abdaziz, A., " Information Security Management System", in International Journal of Computer Applications, January (2017)