BINUS UNIVERSITY

People
Innovation
Excellence

43 YEARS OF BINUS
Empowering Society, Building The Nation

PENGUKUHAN GURU BESAR TETAP

Prof. Dr. Drs. Nilo Legowo, M.Kom.

Orasi Ilmiah:

"Tantangan Keamanan Informasi untuk Keberlanjutan Bisnis dengan Manajemen Risiko Sistem Informasi dan Pendekatan Fuzzy"

26 Februari 2025

Orasi Ilmiah Pengukuhan Guru Besar Tetap Binus University dalam bidang- Manajemen Risiko Sistem Informasi

Tantangan Keamanan Informasi untuk keberlanjutan bisnis dengan Manajemen Risiko Sistem Informasi dan pendekatan Fuzzy

(Prof.Dr.Drs.Nilo Legowo, M.Kom)

Bismillaahirrahmaanirrahiim,

Assalaamu'alaikum Warahmatullahi wabarakaatuh, Selamat pagi dan salam sejahtera bagi kita semua, semoga Allah SWT selalu melimpahkan rahmat dan hidayah-Nya kepada kita semua, Shalawat dan salam kita panjatkan kepada Nabi Besar Muhammad SAW. Amin ya robal alamin.

Yang Saya Hormati,

- Menteri Pendidikan Tinggi, Sains, dan Teknologi, Republik Indonesia Prof. Brian Yuliarto, S.T, M.Eng., Ph.D.
- Lembaga Layanan Pendidikan Tinggi Wilayah III Bapak Prof. Dr. Toni Taharudin, S.Si, M.Sc beserta segenap jajaranya.
- Chief Executive Officer Yayasan Bina Nusantara Bapak Ir. Bernard Gunawan
- Chief Strategic Officer Yayasan Bina Nusantara Bapak Ir. Carmelus Susilo
- President of BINUS Higher Education Bapak Stephen Wahyudi Santoso, BSE, MSIST, CBDMP dan segenap jajaranya.
- Ketua Dewan Guru Besar Universitas Bina Nusantara Bapak Prof. Dr. Ir. Harjanto Prabowo, M.M.
- Rektor dan Ketua Senat Universitas Bina Nusantara Ibu Dr. Nelly, S.Kom., M.M., CSCA
- Guru Besar Tamu Kehormatan:
    - Prof. Dr. Ir. Kudang Boro Seminar, M. Sc. Guru besar dalam bidang ilmu smart & precision agriculture dari Institut Pertanian Bogor
    - Prof. Dr. Ir. R. Eko Indrajit, M.Sc., MBA., Mphil., MA. Guru besar dalam bidang ilmu Komputer dari Universitas Pradita Banten
    - Prof. Dr.Ir. Edi Abduchman MS., M.Sc. Guru Besar dalam Bidang Ilmu Statistika, dari Universitas Trisakti.
- Para Guru Besar Tamu yang hadir secara onsite ataupun online
- Para Guru Besar Universitas Bina Nusantara dan Dewan Pelantik Guru Besar
- Para Wakil Rektor, Dekan, Direktur, HoD, HoP Universitas Bina Nusantara

- Seluruh teman dosen, mahasiswa dan alumni yang saya banggakan
- Seluruh tamu undangan yang hadir secara onsite ataupun online
- Seluruh teman-teman, keluarga dan kerabat yang saya cintai.

Pada kesempatan yang baik ini, Perkenankan saya menyampaikan pidato pengukuhan saya sebagai Guru Besar Tetap Universitas Bina Nusantara di bidang Manajemen Risiko Sistem Informasi.

Judul orasi ilmiah saya adalah: **Tantangan Keamanan Informasi untuk keberlanjutan bisnis dengan Manajemen Risiko Sistem Informasi dan pendekatan Fuzzy**

A. Pendahuluan:

Pertumbuhan perusahaan yang semakin cepat seiring dengan penggunaan sistem informasi dan teknologi informasi bagaikan satu kesatuan yang tidak dapat di pisahkan untuk kelangsungan bisnis perusahaan.

Saat ini perusahaan yang banyak melakukan upaya transformasi digital dalam mendukung proses bisnis dan opersional perusahaan dalam rangka meningkatkan produktifitas dan efisiensi dalam memberikan layanan.

Dalam era digital yang sangat tergantung dengan penggunaan teknolgi informasi yang semakin maju, perusahaan dihadapkan pada tantangan signifikan terkait ancaman siber yang sering muncul dalam operasional keseharian ini, yang dapat menimbulkan kerentanan dan risiko keamanan informasi yang dapat mengganggu kelangsungan bisnis perusahaan.

Perkembangan teknologi digital yang pesat telah membawa perubahan signifikan dalam cara individu, organisasi, dan pemerintah mengelola informasi. Namun, di balik manfaatnya, ancaman terhadap keamanan data pribadi semakin meningkat, terutama dengan adanya serangan siber Situasi ini memunculkan kebutuhan mendesak akan kerangka hukum yang kuat untuk melindungi data pribadi.

Jenis serangan sangat beragam mulai dari serangan siber seperti pencurian data, ransomware, malware, phishing, dan peretasan data, pelanggaran privasi dan lainnya yang tidak hanya mengancam operasional harian, tetapi juga integritas dan kepercayaan pelanggan terhadap performa perusahaan.

Menurut Lanier (2014), “Data is the new oil,” yang menegaskan bahwa data memiliki nilai yang sangat tinggi dalam era digital ini, sehingga pengelolaannya harus dilakukan dengan hati-hati.

1. Definisi manajemen risiko dalam konteks bisnis modern

Manajemen risiko dalam sistem informasi perusahaan menjadi semakin krusial di era digital saat ini. Integrasi teknologi informasi dalam operasional bisnis membawa manfaat signifikan, namun juga menimbulkan berbagai risiko yang perlu dikelola dengan baik.

- Seperti semua terminologi yang digunakan dalam manajemen risiko, definisi untuk "risiko" juga sangat luas. Satu definisi untuk risiko yang diterapkan pada keamanan informasi secara khusus adalah:

“The expected loss of confidentiality, integrity, availability, or accountability (CIAA).”

- Dilanjutkan dengan definisi risiko yang lebih umum dari Jack Jones pencipta Factor Analysis of Information Risk (FAIR) framework:
  "The probable frequency and probable magnitude of future loss"

Pentingnya manajemen risiko siber tercermin dari dampak yang ditimbulkan oleh serangan siber, seperti kehilangan pendapatan, kesempatan bisnis, dan pelanggan. Data menunjukkan bahwa serangan siber dapat menyebabkan penurunan pendapatan dan hilangnya kepercayaan pelanggan, yang berdampak negatif pada pertumbuhan perusahaan dalam jangka panjang.

2. Permasalahan Keamanan Informasi dalam Manajemen Risiko Tantangan Serangan Ransomeware di Industri

Gambar 1. Respons insiden ransomware kesadaran situasional yang diusulkan pada Gambar

Gambar 2. Distribusi Serangan Ransomware berdasarkan Industri

1. Desain kerangka kerja adalah artefak tiga fase; setiap fase sesuai dengan satu modul dalam pendekatan kesadaran situasional.

Serangan Ransomware menyerang industry Manufacturing mengapa. Peretas menyerang barang produksi yang di hasilkan oleh manufacture di jual ke mana., siapa Vendor nya, siapa customernya, Siapa pembeli produk itu (yang dikenal dengan Pivot Attact), di pantulkan ke Perusahaan lain yang tidak cukup aware karyawan Perusahaan itu.

Serangan siber adalah salah satu dari masalah besar sistem informasi, menurut Cybersecurity Ventures (2021). Pada tahun 2021, kerugian akibat serangan siber diperkirakan mencapai $6 trilliun dan angka ini diperkirakan akan terus meningkat. Aktivitas kejahatan dunia maya adalah salah satu tantangan terbesar yang akan dihadapi umat manusia dalam dua dekade mendatang.

Serangan ini biasanya menargetkan platform e-commerce, perbankan yang memungkinkan pencurian data pribadi dan finansial pelanggan.

Dampak finansial: target pilihan berisiko dampak finansial yang lebih besar dari target peluang.

Menurut Katadata, 23% ***perusahaan*** yang menjadi korban ***serangan siber*** kehilangan kesempatan untuk mendapatkan kontrak ***bisnis*** baru.

Menurut data dari Kominfo terdapat 1.730 penipuan online di Indonesia mulai dari Agustus 2018 hingga 16 Februari 2023 (katadata.co.id, 2023). Salah satu penipuan online yang sering terjadi di Indonesia yaitu penipuan belanja di e-commerce sebanyak 21% (suara.com, 2021).

Selain itu dari survei APAC yang dilakukan secara menyeluruh banyak konsumen yang menjadi korban penipuan di e-commerce 32% nya penipuan terkait gadget dan sisanya 27% terkait dengan pakaian (suara.com, 2021).

3. Tren Biaya Pelanggaran Data 2024

Menurut Laporan Biaya Pelanggaran Data tahunan IBM, dampak finansial yang mengejutkan dari pelanggaran data mencapai rata-rata global sebesar $4,88 juta Menurut pakar keamanan siber Jeff Crume.

Sulit untuk mengevaluasi risiko siber dengan penuh kepastian. Perusahaan jarang memiliki visibilitas penuh terhadap taktik penjahat siber, kerentanan jaringan mereka sendiri, atau risiko yang lebih tidak terduga seperti cuaca buruk dan kelalaian karyawan. Serangan siber yang sama dapat memiliki konsekuensi yang berbeda diantara Perusahaan

Munculnya ancaman siber yang semakin kompleks dan terorganisir menuntut perusahaan untuk membuat strategi dan mitigasi risiko dengan menerapkan manajemen risiko sistem informasi yang dengan menerapkan standar yang efektif. Proses ini mencakup identifikasi risiko, analisa risiko, penilaian, dan pengendalian ancaman terhadap informasi digital dan sistem teknologi informasi perusahaan.

Pentingnya Manajemen Risiko di Era Digital

Pentingnya manajemen risiko siber tercermin dari dampak yang ditimbulkan oleh serangan siber, seperti kehilangan pendapatan, kesempatan bisnis, dan pelanggan. Data menunjukkan bahwa serangan siber dapat menyebabkan penurunan pendapatan dan hilangnya kepercayaan pelanggan, yang berdampak negatif pada pertumbuhan perusahaan dalam jangka panjang.

- Perlindungan Data Sensitif = Perusahaan harus melindungi sejumlah besar data sensitif dari pencurian atau kerusakan, termasuk informasi pelanggan dan rahasia dagang.
- Jaminan Kelangsungan Bisnis= Manajemen risiko yang efektif memastikan operasi tetap berjalan lancar bahkan selama insiden siber.
- Kepatuhan Regulasi=Memenuhi peraturan industri membutuhkan langkah-langkah perlindungan data dan keamanan informasi yang kuat.
- Reputasi dan Manajemen Kepercayaan= Keamanan informasi yang kuat membangun kepercayaan pelanggan dan melindungi reputasi perusahaan.
- Keamanan Keuangan= Manajemen risiko membantu mencegah kerugian keuangan akibat serangan siber, perbaikan sistem, dan gangguan bisnis.

1. Perlindungan Data Sensitif

Perusahaan harus melindungi sejumlah besar data sensitif dari pencurian atau kerusakan, termasuk informasi pelanggan dan rahasia dagang di berbagai Industri Manufaktur dan Perbankan dan lainnya.

Dengan meningkatnya digitalisasi, perusahaan menghadapi volume data yang sangat besar, dengan berbagai jejenis data sensitif yang harus dilindungi yang sering kali sulit dikelola dengan metode konvensional. Hal ini menimbulkan risiko kebocoran data, akses tidak sah, dan serangan

siber yang semakin canggih. Menurut laporan oleh "Journal of Cybersecurity" (2022), 43% perusahaan global melaporkan peningkatan serangan ransomware dalam dua tahun terakhir.

2. Ancaman Insider dan Kurangnya Kesadaran Karyawan

Ancaman dari orang dalam (ancaman insider), baik disengaja maupun tidak, masih menjadi salah satu kelemahan utama dalam sistem keamanan informasi perusahaan. Sebuah studi oleh "Information Systems Management" (2021) menunjukkan bahwa lebih dari 60% insiden keamanan informasi terkait dengan kesalahan manusia atau praktik kerja yang tidak aman.

3. Kepatuhan terhadap Regulasi

Perusahaan juga menghadapi tantangan untuk mematuhi berbagai standar dan regulasi, seperti GDPR, HIPAA, dan ISO/IEC 27001. Ketidakpatuhan dapat mengakibatkan denda besar, kehilangan reputasi, dan konsekuensi hukum lainnya. Misalnya, pada tahun 2021, denda GDPR mencapai lebih dari €1,2 miliar (Sumber: "International Data Privacy Journal", 2021).

Kasus penggunaan IT Assest Management (ITAM): Meninjau inventaris aset TI, lisensi perangkat lunak, kepatuhan perangkat keras dan perangkat lunak, manajemen vendor dan kepatuhan pihak ketiga, serta privasi data dan kepatuhan GDPR. General Data Protection Regulation (GDPR)

Kepatuhan organisasi ke peraturan pemerintah menjadi hal yang sangat penting yang harus di taati dan di laksankan dalam kegiatan Operasionalnya. Organisasi yang tidak mematuhi aturan regulasi yang ada akan mendapatkan sangsi dan risiko yang sesuai dengan peraturan yang ada.

Contoh :

Peraturan Bank Indonesia Nomor 2 Tahun 2024 Tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran,

Menurut Peraturan Menteri Keuangan Republik Indonesia nomor 12/PMK.09/2016 pasal 1 no 3 di jelaskan bahwa proses manajemen risiko adalah penerapan kebijakan, prosedur, dan praktik manajemen yang bersifat sistematis atas aktivitas komunikasi dan konsultasi, penetapan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, mitigasi risiko, serta pemantauan dan review.

Rekapitulasi dan manajemen kepercayaan pada keamanan informasi yang kuat membangun kepercayaan pelanggan , sebagai contoh perlindungan data customer yang perlu di jaga dari Serangan siber dengan keluarnya UU PDP No 27 Tahun 2022 tentang pelindungan data pribadi di Indonesia hadir sebagai respons terhadap tantangan serangan siber ini. UU PDP bertujuan memberikan pelindungan hukum bagi individu atas data pribadi. Data pribadi ini perlu di jaga demi melindungi reputasi perusahaan.

B. Keamanan Informasi dalam Keberlanjutan Bisnis.

Menurut Adel A.N at all [2018] mempertimbangkan masalah penilaian pengembangan keamanan informasi perusahaan dalam ketidakpastian menggunakan metode Fuzzy Analytical Hierarchy Process (AHP). Penilaian terhadap pengembangan keamanan informasi merupakan langkah awal dalam membangun sistem manajemen keamanan informasi di setiap organisasi.

Salah satu cara yang mungkin untuk memecahkan masalah pengembangan keamanan informasi adalah dengan menggunakan metodologi pengambilan keputusan multikriteria. Proses hierarki analitis melibatkan subjektivitas manusia, yang menghadirkan jenis ketidakpastian dan memerlukan penggunaan metode pengambilan keputusan di bawah ketidakpastian ini.

1. Resiko dan ketidakpastian

Setiap perusahaan selalu menghadapi ketidakpastian secara teratur, apakah mereka mau atau tidak.

Menurut Rørvik (2013) adanya manajemen risiko untuk membantu mengatasi tantangan yang ditimbulkan oleh ketidakpastian, itu harus benar-benar terfokus dan efektif diterapkan di seluruh organisasi.

Menurut Hillson (2017) mencoba untuk memperjelas hubungan antara risiko dan ketidakpastian melalui pendekatan pragmatis, di mana ia membagi ketidakpastian menjadi dua kelompok: yang penting bagi organisasi, dan yang tidak penting.

Kematangan keamanan informasi ini didasarkan pada model analisis kerentanan keamanan informasi multilevel hierarkis untuk standar keamanan ISO 27001:2013. Konsep himpunan fuzzy menerapkan Proses Hirarki Analitis untuk mengukur pengembangan keamanan informasi organisasi dalam lingkungan yang tidak pasti. Penggunaan pendekatan ini membantu menentukan pentingnya faktor dan indikator secara lebih efektif.

Pentingnya keberlanjutan bisnis dalam menghadapi risiko operasional

Menurut Alovsat Garaja Aliyev (2022) menjelaskan bahwa teknologi untuk memastikan keberlanjutan keamanan informasi dalam pembentukan ekonomi digital dan prospeknya. Telah ditunjukkan bahwa transformasi digital ekonomi dan masyarakat merupakan prioritas bagi negara-negara maju di dunia. Dinyatakan bahwa pembentukan masyarakat intelektual dan ekonomi yang aman dan berkelanjutan berdasarkan informasi, pengetahuan, dan teknologi baru merupakan salah satu tujuan utama. Fitur-fitur transisi dari ekonomi industri ke ekonomi informasi berbasis TIK baru dianalisis, di transformasi digital sektor ekonomi riil.

Telah dicatat bahwa memastikan pengembangan ekonomi modern berdasarkan teknologi digital, pengembangan sektor teknologi tinggi merupakan salah satu tujuan utama. Area potensial untuk digitalisasi ekonomi telah diidentifikasi. Fitur ekonomi dari teknologi utama yang membentuk ekonomi digital telah dipelajari.

Penerapan teknologi modern untuk memastikan keberlanjutan keamanan informasi dalam ekonomi digital dan pengembangan area pengembangannya yang menjanjikan telah menjadi isu topikal di zaman ini. Pembentukan masyarakat intelektual dan ekonomi yang aman dan berkelanjutan berdasarkan informasi, pengetahuan, dan teknologi digital merupakan salah satu tujuan utama.

Perlu dicatat bahwa dalam konteks transformasi digital sektor-sektor utama ekonomi negara, keberlanjutan keamanan informasi mereka hanya dapat dicapai berdasarkan pendekatan yang sistematis.

Harus ada penggunaan mekanisme administratif yang komprehensif dalam hal perundang-undangan, serta langkah-langkah organisasi yang efektif, serta perangkat keras modern dan teknologi dasar yang relevan

Analisis keadaan pertumbuhan di bidang serangan siber dalam beberapa tahun dan tahap utama evolusi keamanan siber dijelaskan. Rekomendasi telah dikembangkan sesuai dengan pengalaman negara-negara maju tentang teknologi keamanan siber cerdas Alovsat Garaja Aliyev (2022).

D. Pendekatan manajemen risiko SI pakai Framework ISO

Karena alasan ini, pihak berwenang seperti National Institute of Standards and Technology (NIST) menyarankan pendekatan manajemen risiko siber sebagai proses berulang yang berkelanjutan, bukan hanya sekali kejadian.

Tim manajemen risiko siber dapat terdiri dari direktur, pemimpin eksekutif seperti CEO dan chief information security officer (CISO), anggota tim TI dan keamanan, hukum dan SDM, serta perwakilan dari unit bisnis lainnya.

Perusahaan dapat menggunakan banyak metodologi manajemen risiko siber, termasuk Kerangka Kerja Keamanan Siber NIST (NIST CSF) dan Kerangka Kerja Manajemen Risiko NIST (NIST RMF). Meskipun metode ini sedikit berbeda, namun semuanya mengikuti serangkaian langkah inti yang serupa.

Untuk menghadapi ancaman ini, perusahaan perlu mengembangkan strategi manajemen risiko siber yang komprehensif. Langkah-langkah yang dapat diambil meliputi pengembangan strategi untuk mengurangi atau menghilangkan dampak ancaman, seperti penerapan kontrol keamanan, pelatihan bagi karyawan, menanamkan kesadaran keamanan informaasi serta rencana merespons insiden.

Dengan menerapkan manajemen risiko siber yang efektif, perusahaan dapat melindungi data, jaringan komputer, dan perangkat mereka dari akses yang tidak sah, kerusakan, atau serangan yang dapat membahayakan operasional bisnis. Kondisi manajemen risiko yang efektif dapat meningkatkan keamanan informasi dan hal ini untuk memastikan kelangsungan bisnis di tengah gelombang transformasi digital yang terus berkembang dan penuh tantangan.

General Data Protection Regulation (GDPR)

- Peraturan Perlindungan Data Umum UE bukan hanya tentang melindungi data informasi sensitif dari peretas dan kebocoran.
- GDPR juga menjelaskan kerahasiaan data mengenai privasi data.

2. Manajemen Risiko degan ISO 31000

- Menurut Badan Standarisasi Nasional (2016) secara garis besar arsitektur ini mencakup tiga elemen mendasar, yaitu: prinsip pengelolaan risiko, kerangka kerja, dan proses manajemen risiko.
- Dalam ISO 31000 dalam implementasinya memperhatikan tiga aspek penting yaitu prinsip manajemen risiko, kerangka kerja dan proses. Untuk melihat tiga aspek ini saling berkaitan dapat dilihat pada gambar berikut:

proses penilaian dan penanganan risiko dalam ISO 27001 selaras dengan prinsip dan pedoman umum yang disediakan dalam ISO 31000.
https://ictinstitute.nl/iso-31000-explained/

Risk Management Framework ISO 31000 & ISO2700

Proses ISO - Identifikasi dan Evaluasi Risiko

ISO 31000 adalah standar internasional yang menyediakan panduan untuk manajemen risiko secara komprehensif dalam organisasi. Proses manajemen risiko menurut ISO 31000 terdiri dari beberapa langkah yang saling berkesinambungan. Berikut adalah penjelasan langkah-langkah tersebut:

1. **Komunikasi dan Konsultasi**: Langkah pertama ini menekankan pentingnya komunikasi dan konsultasi dengan pemangku kepentingan internal dan eksternal sepanjang proses manajemen risiko.
2. **Penetapan Lingkup, Konteks, dan Kriteria**: Pada tahap ini, organisasi menetapkan ruang lingkup manajemen risiko, memahami konteks internal dan eksternal yang dapat mempengaruhi pencapaian tujuan, serta menentukan kriteria risiko yang akan digunakan untuk evaluasi.
3. **Penilaian Risiko (Risk Assessment)**: Proses ini terdiri dari tiga sub-langkah:
    - **Identifikasi Risiko**: Mengidentifikasi potensi risiko yang dapat mempengaruhi tujuan organisasi.
    - **Analisis Risiko**: Menganalisis sifat dan karakteristik risiko, termasuk penyebab dan dampaknya.
    - **Evaluasi Risiko**: Mengevaluasi risiko untuk menentukan prioritas penanganan berdasarkan tingkat keparahan dan kemungkinan terjadinya.
4. **Perlakuan Risiko (Risk Treatment)**: Setelah evaluasi, organisasi mengembangkan dan mengimplementasikan rencana untuk menangani risiko.
5. **Pemantauan dan Tinjauan (Monitoring and Review)**: Langkah ini memastikan bahwa proses manajemen risiko berjalan efektif dan sesuai dengan rencana.
6. **Penerimaan risiko** (risk acceptance) adalah keputusan untuk menerima risiko tertentu tanpa melakukan tindakan lebih lanjut untuk mengendalikannya. Keputusan ini diambil setelah melalui proses penilaian risiko yang komprehensif, di mana risiko tersebut dianggap berada dalam batas toleransi yang dapat diterima oleh organisasi.

- Menrut Cassidy (2016) manajemen risiko akan lebih efektif jika perusahaan menerapkan 11 prinsip manajemen risiko. Hal itu menjelaskan bagaimana ISO 31000 berpengaruh kepada perusuhaan karena sebelas prinsip ini akan berpengaruh pada dasar pertimbangan dalam penerapan manajemen risiko :
- Menurut Hopkin (2017) suksesnya manajemen risiko akan tergantung pada efektifitas kerangka kerja manajemen yang menyediakan dasar dan pengaturan yang akan melekat pada keseluruhan organisasi pada semua tingkatan yang di dasari oleh Plan,

Do, Check, Action. Kerangka kerja tersebut membantu dalam pengelolaan risiko secara efektif melalui pengaplikasian dari proses manajemen risiko.

Adopsi Teknologi dan Keberlanjutan Bisnis

Perkembangan teknologi 5.0 telah membawa transformasi besar dalam lanskap bisnis global. Era ini ditandai dengan integrasi teknologi pintar, kecerdasan buatan, dan interkonektivitas yang semakin mendalam antara manusia dan mesin. Serangan siber yang semakin berkembang maka perlu upaya untuk meningkatkan proses mitigasi dengan standar teknologi yang lebih update untuk kelangsungan bisnis.

Adopsi teknologi baru seperti AI, IoT, Machine Learning, dan cloud computing memerlukan strategi keamanan yang komprehensif, Membangun infrastruktur TI yang tangguh yang terintegrasi dengan proses bisnis untuk menjamin keberlanjutan operasional bisnis. Implementasi strategi manajemen risiko yang proaktif untuk mengantisipasi ancaman masa depan

Untuk menjamin kelangsungan bisnis di era digital, organisasi perlu mengadopsi pendekatan holistik yang menggabungkan teknologi terkini, prosedur keamanan yang kuat, dan pelatihan berkelanjutan bagi seluruh karyawan. Investasi dalam keamanan siber bukan lagi pilihan, melainkan kebutuhan fundamental untuk memastikan keberlanjutan operasional jangka panjang.

Pentingnya keberlanjutan bisnis dalam menghadapi risiko operasional, Menurut Alovsat Garaja Aliyev (2022) menjelaskan bahwa teknologi untuk memastikan keberlanjutan keamanan informasi dalam pembentukan ekonomi digital dan prospeknya. Telah ditunjukkan bahwa transformasi digital ekonomi dan masyarakat merupakan prioritas bagi negara-negara maju di dunia.

Dinyatakan bahwa pembentukan masyarakat intelektual dan ekonomi yang aman dan berkelanjutan berdasarkan informasi, pengetahuan, dan teknologi baru merupakan salah satu tujuan utama. Fitur-fitur transisi dari ekonomi industri ke ekonomi informasi berbasis TIK baru dianalisis, di transformasi digital sektor ekonomi riil.

Sebagai contoh, serangan ransomware yang terjadi di colonial pipeline yang terjadi pada tahun 2021menyebabkan pengoperasian pipa minyak terbesar di AS selama lima hari, dengan dampak berhentinya pasokan energi nasional.

Dimana akibat dari serangan tersebut perusahaan yang beroperasi di Texas America menutup penjualannya selama 2 hari setelah jaringan meter billing dari perusahaan tersebut terjangkit ransomware, sehingga pencatatan penjualan minyak tidak terekam, serangan ini dikenal sebagai serangan ransomware terbesar pada sector oil & gas.

Mengadopsi Teknologi AI dalam Risiko Keamanan Informasi

Peran GenAI dalam Mitigasi Risiko Keamanan Informasi

GenAI dapat digunakan untuk mendeteksi pola aktivitas yang tidak biasa dalam sistem informasi perusahaan, membantu mengidentifikasi potensi ancaman sebelum menjadi insiden besar. Dengan kemampuan analisis real-time, GenAI dapat memberikan rekomendasi langkah mitigasi atau secara otomatis menjalankan tindakan tertentu untuk mengurangi dampak risiko.

Sesuai hasil penelitian yang kami lakukan untuk melakukan control dan peringatan dini terhadap serangan , ancaman baik dari dalam atau dari luar melalui jaringan computer VPN perusahaan melalui Outler Detection (N.Legowo,W.M Bad 2024).

GenAI dapat mensimulasikan berbagai skenario serangan dan mengevaluasi efektivitas kontrol keamanan yang ada, memungkinkan perusahaan untuk mengoptimalkan strategi mereka. GenAI dapat digunakan untuk menciptakan simulasi pelatihan keamanan bagi karyawan, meningkatkan kesadaran dan kompetensi mereka dalam menghadapi ancaman siber. Sebagai contoh Bank mengadopsi sistem GenAI untuk memitigasi risiko keamanan informasi. Dengan menggunakan algoritma deteksi berbasis AI, Hasilnya mencatat pengurangan 30% dalam insiden keamanan selama satu tahun.

Mengadopsi Teknologi AI dalam Risiko keamanan informasi Biaya global rata-rata pelanggaran data pada tahun 2024, mengalami peningkatan 10% dari tahun lalu dan total tertinggi yang pernah tercatat US**$ 4,88 juta**.

Rata-rata penghematan biaya yang dicapai organisasi dengan penggunaan AI dan otomasi keamanan yang ekstensif dalam pencegahan $ 2,22 juta.

Pendekatan Sistem Fuzzy dalam Manajemen Risiko

E. Solusi untuk Masa Depan dengan Fuzzy dan AI

Salah satu cara yang mungkin untuk memecahkan masalah pengembangan keamanan informasi adalah dengan menggunakan metodologi pengambilan keputusan multikriteria. Proses hierarki analitis melibatkan subjektivitas manusia, yang menghadirkan jenis ketidakpastian dan memerlukan penggunaan metode pengambilan keputusan di bawah ketidakpastian ini.

Kematangan keamanan informasi ini didasarkan pada model analisis kerentanan keamanan informasi multilevel hierarkis untuk standar keamanan ISO 27001:2013. Konsep himpunan fuzzy menerapkan Proses Hirarki Analitis untuk mengukur pengembangan keamanan informasi organisasi dalam lingkungan yang tidak pasti. Penggunaan pendekatan ini membantu menentukan pentingnya faktor dan indikator secara lebih efektif

Mitigasi Ancaman Cyber Keamanan Informasi dengan sistema Fuzzy untuk Menentukan Level Risiko

Sistem fuzzy adalah metode yang efektif untuk mengelola risiko keamanan informasi dalam manajemen risiko sistem informasi. Pendekatan ini berguna untuk menangani ketidakpastian dan subjektivitas dalam penilaian risiko. Berikut adalah penjelasan rinci tentang penerapan sistem fuzzy dalam mitigasi ancaman cyber keamanan informasi:

Sistem fuzzy menggunakan logika linguistik dan fungsi keanggotaan untuk merepresentasikan data yang tidak pasti atau ambigu. Dalam konteks keamanan informasi, sistem ini membantu menentukan level risiko berdasarkan variabel seperti probabilitas ancaman dan dampaknya.

Pendekatan ini menggunakan algoritma berbasis logika fuzzy untuk menentukan level risiko dengan input berupa variabel linguistik seperti **rendah**, **sedang**, dan **tinggi**. Sistem ini cocok untuk menangani ketidakpastian dalam data.

Mitigasi Ancaman Cyber dengan Sistem Fuzzy

Komponen Utama Sistem Fuzzy

1. Fuzzification: Konversi input numerik menjadi nilai linguistik (misalnya, *rendah*, *sedang*, *tinggi*).
2. Inference System: Penerapan aturan fuzzy (fuzzy rules) untuk mengevaluasi hubungan antara input dan output.
3. Defuzzification: Konversi hasil linguistik menjadi nilai numerik untuk interpretasi akhir.

Dalam konteks keamanan informasi, sistem ini membantu menentukan level risiko berdasarkan variabel seperti probabilitas ancaman dan dampaknya. Pendekatan ini menggunakan algoritma berbasis logika fuzzy dengan input berupa variabel linguistik, yang sangat cocok untuk menangani ketidakpastian dalam data.

Langkah-langkah Menggunakan Sistem Fuzzy dalam Menentukan Level Risiko

a. Identifikasi Variabel Input

- Probabilitas Ancaman (P): Seberapa sering ancaman seperti serangan phishing, malware, atau DDoS dapat terjadi.
- Dampak (I): Seberapa besar kerugian yang diakibatkan oleh ancaman tersebut terhadap sistem informasi.

Hasil Penelitian

Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001 (N.Legowo, Y.Juhartoyo, 2022)

Penjelasan Hasil Penelitian

1. Tingkat kematangan saat ini telah mencapai 75%, berdasarkan informasi yang dihimpun dengan menggunakan checklist berdasarkan Lampiran A standar ISO 27001:2005.
2. Manajemen kelangsungan bisnis yang telah mencapai tingkat kematangan 55%, saat ini memerlukan revisi atau perbaikan prosedur manajemen kelangsungan bisnis. Sementara domain dengan tingkat kematangan tinggi telah mencapai 93 persen kepatuhan.

3. Berdasarkan hasil penilaian risiko (risk assessment), terdapat tiga (3) risiko dasar nilai aset teknologi informasi yang sangat tinggi (extremely high) dan tujuh (7) risiko dasar nilai aset yang tinggi (High), dan disarankan untuk melakukan perbaikan prosedur , untuk menjaga ketersediaan SAN Storage dan Komunikasi Data serta meningkatkan kapasitas sumber daya manusia, khususnya programmer aplikasi dengan pelatihan, untuk meningkatkan keterampilan programmer, guna menurunkan tingkat risiko sistem keamanan informasi perusahaan.
4. Untuk mengelola sistem manajemen risiko keamanan teknologi informasi, organisasi perlu memilih implementasi atau kerangka kerja sistem keamanan informasi, seperti ISO 27001.

Berdasarkan hasil penelitian menggunakan standar ISO 27001 di peroleh Divisi Sistem dan Operasi Teknologi Informasi bertanggung jawab untuk melengkapi kuesioner ini melalui wawancara langsung dengan unit kerja terkait.

Setelah semua tanggapan responden diperoleh melalui wawancara dan kuesioner, tanggapan tersebut dikategorikan menurut pengendalian domain dan ISO 27001:2005. Kemudian, tanggapan tersebut diberi bobot/nilai yang proporsional terhadap data. Untuk menghitung bobot/nilai per-domain, nilai per kontrol akan dirata-ratakan dan kemudian digunakan untuk menghitung bobot/nilai. Skala kesesuaian/kematangan berkisar antara 0 hingga 100 persen, dengan 0 menunjukkan bahwa tidak ada prosedur atau kontrol yang saat ini beroperasi dan 100 menunjukkan bahwa semua prosedur dan kontrol yang ada sesuai dengan keadaan operasi saat ini. Hasil perhitungan berbasis domain ditampilkan dalam Tabel 2.

Table 2: Current maturity level

Clause	Domain / Control	Current Condition (%)
A5	Security Policy	75
A6	Organization of Information Security	83
A7	**Asset Management**	**60**
A8	Human Resources Security	78
A9	**Physical and Environmental Security**	**69**
A10	Communications and Operations Management	84
A11	Access Control	74
A12	Information System Acquisition, Development and Maintaining	77
A13	Information Security Incident Management	75
A14	**Business Continuity Management**	**55**
A15	**Compliance**	**93**

Hasil Penelitian

Fuzzy Risk Model for Research and Development Department in Clinical Laboratory (N.Legowo, W. Sardjono 2023)

Hasil penelitain menjelaskan Risiko keamanan informasi merupakan hal yang sangat penting dan menjadi perhatian krusial, khususnya dalam laboratorium klinis yang bertanggung jawab untuk mengelola informasi kesehatan publik yang sensitif.

Berbagai upaya telah dilakukan oleh berbagai lembaga untuk mengatasi tantangan mendesak ini secara efektif. Penelitian ini berupaya mengembangkan model keputusan berbasis komputer untuk menilai risiko keamanan informasi.

Model ini dibangun secara ilmiah menggunakan metode logika fuzzy sebagai pendekatan intinya dan dirancang melalui pendekatan berorientasi objek.

Membangun sebuah model keputusan untuk menilai risiko, dengan berfokus secara khusus pada perusahaan sektor publik. Karena studi ini hanya membahas dua kategori risiko, kinerja model dinilai berdasarkan konsep pengukuran akurasi. yang dibandingkan dengan pengukuran manual.

Tabel 1 menyajikan pernyataan risiko yang terkait dengan Departemen R&D laboratorium klinis. Di antara 31 pernyataan yang dinilai secara manual untuk probability (P) dan Impact(I), empat contoh disorot. Risiko-risiko ini terdiri dari 26% risiko sedang dan 74% risiko rendah; ketika mempertimbangkan aspek keamanan informasi, 7% risiko adalah confidentiality (kerahasiaan), 45% adalah integrity (integritas), dan 48% adalah availability (ketersediaan). Semua pernyataan risiko diidentifikasi dengan cermat, dengan kategori memainkan peran penting dalam menentukan faktor probability (P) and impact (I).

Dengan demikian, parameter yang dipertimbangkan dalam model yang diusulkan adalah P, I, dan R. Semua parameter dikonversi menjadi fuzzy membership function (FMF). FMF untuk setiap P, I, dan R dikonfigurasikan masing-masing pada Gambar 5 hingga 7; di mana parameter P dan I sebagai parameter anteseden dan kemudian parameter R sebagai parameter konsekuen. Berdasarkan analisis lapangan, P dan I diidentifikasi dengan enam variabel linguistik.

Variabel linguistik untuk P adalah “sangat jarang” (VS), “jarang” (SE), “kadang-kadang” (O), “cukup sering” (QO), “sering” (OF), “sangat sering” (VO).

Dan kemudian, variabel linguistik untuk I adalah “kecil” (SM), “kecil” (MI), “menengah” (IN), “gangguan” (B), “utama” (MA), dan “kritis” (C).

Khusus untuk parameter R ditentukan melalui empat variabel verbal: “rendah” (L), “menengah” (M), “moderat” (MO), dan “tinggi” (H).

Hasil dari uji model yang di lakukan di dapat yang mengesankan bahwa model ini berhasil mensimulasikan 31 skenario risiko dengan tingkat akurasi 93,55%.

Fig. 2. Risk Analysis Matrix.

Aturan fuzzy yang digunakan dalam model disajikan dalam Tabel 3, sebagai empat contoh aturan fuzzy dari 36 aturan (berasal dari lima jenis masing-masing P dan I) dalam menentukan empat R.

FMF untuk setiap P, I, dan R dikonfigurasikan masing-masing pada Gambar 5 hingga 7; di mana parameter P dan I sebagai parameter anteseden dan kemudian parameter R sebagai parameter konsekuen.

Fig. 5. The Probability FMF.

Fig. 6. The Impact FMF.

Fig. 7. The Risk FMF.

Fig. 8. Risk Value for 31 Risk Statements as the Constructed Model Simulation Result.

Lebih jauh, risiko sederhana bergantung pada nilai probabilitas dan dampak yang diperoleh dari tahap analisis.

Penelitian selanjutnya dapat menggali lebih dalam konsep risiko, dengan fokus khusus pada probabilitas dan dampak risiko. Akan menarik untuk mengeksplorasi data kategori risiko lain untuk lebih memperkaya model keputusan yang ada.

Rencana Pengembangan Manajemen Risiko SI

Serangan ciber sudah semakain canggih maka untuk strategi manajemen risiko juga harus mengikuti perkembangan teknologi yang di terapkan dalam manajemen risiko yang terjadi di perusahaan, dalam upaya untuk mengantisipasi ancaman ini.

Seperti dalam penelitian saya yang berjudul .." ISO Fuzzy……

- strategi manajemen risiko juga harus mengikuti perkembangan teknologi seperti halnya strategi pengambilan keputusan untuk menentukan risiko yang terjadi di perusahaan perlu di lakukan lebih cepat.
- Membahas cara untuk melakukan mitigasi dari kemungkinan munculnya risiko di perusahaan dengan menggunakan beberapa framework keamanan informasi, serta mengikuti langkah-langkah yang ada dalam framework tersebut, (seperti ISO 27001, 31001 dan lainya).
- Selain itu dalam upaya melakukan mitigasi terhadap munculnya risiko perlu di lakukan control dan monitoring dari setiap proses dan aktivitas bisnis yang menggunakan sistem informasi , software aplikasi dan jaringan komputer.
- membuat pemetan level risiko dengan menggunakan pendekatan ISO Fuzzy logic. Dalam pengambilan keputusan dengan cepat, Seperti judul yang akan di publikasi „ ISO 27001 fuzzy-based Medical Information Security Risk Model

Tools AI dan GenAI untuk Penilaian Risiko menggunakan Machine Learning membantu dalam memprediksi pola serangan siber berdasarkan data historis.

Tools AI dan Generative AI (GenAI) dapat digunakan untuk:

Mengidentifikasi kerentanan baru melalui simulasi, Menyediakan strategi mitigasi berdasarkan skenario ancaman.

Strategi tools dalam mitigasi risiko untuk Solusi pengambilan keputusan terbaik dari berbagai alternatif yang tersedia untuk mengelola risiko. Dalam rangka untuk meminimalkan dampak risiko terhadap operasional, keuangan, atau reputasi perusahaan.

Srategi mitigasi semakin memainkan peran penting dalam mendukung proses ini dengan:

- Analisis data yang cepat dan mendalam.
- Prediksi potensi risiko di masa depan.
- Pemberian rekomendasi berbasis data historis dan real-time.

Framework CRISP-DM (Cross-Industry Standard Process for Data Mining)

Proses pemodelan ini, ada 4 tahap utama dalam model yang diusulkan penulis: preprocessing, clustering, outlier detection and post-processing. Secara umum, dapat dijelaskan pada Gambar 6.

Kontribusi Binus University dalam Manajemen Risiko SI

Kontribusi Universitas Bina Nusantara dalam keberlanjutan pengembangan manajemen risiko keamanan informasi.

Universitas Bina Nusantara telah banyak berkontribusi dalam pengembangan keamanan informasi untuk kelangsungan bisnis dengan menggunakan Manajemen Risiko sistem informasi melalui beberapa kegiatan, baik dalam Penelitian di Industri Kesehatan , pengembangan teknologi, maupun pelatihan sumber daya manusia di Industri Perbankan yang siap menghadapi tantangan bisnis di era Digital.

Melalui berbagai kontribusi ini, Binus berperan aktif dalam usulan model pengambilan keputusan untuk menentukan level risiko dalam manajemen risiko sistema informasi dengan menggunakan Fuzzy logic dan penggunaan AI di berbagai industri untuk kelangsungan bisnis di Indonesia.

Membuat pemetan level risiko dengan pendekatan ISO Fuzzy logic. seperti ISO 27001 FUZZY-BASED Medical Information Security Risk Model .

- Pengembangan topik penelitan yang sudah ada
- Mengembangkan Metode dan Framework
- Penggunaan Tools baru seiring perkembangan Teknolgi AI
- Melakukan Catur Darma
- Keterlibatan dan Kolaborasi Multidisiplin

Penelitian yang di biayai

Daftar Penelitian yang di biayai

No	Tahun	Judul Penelitian	Sumber Dana	Penulis
1	2014	Pemodelan *adaptive neuro fuzzy inference system* (anfis) untuk diagnosa awal penyakit *dengue hemorrhagic fever*	Ristek DIKTI	N Legowo, A G. Salman. B. Kanigoro
2	2014	Sistem Informasi Peringatan Dini Pengendalian Hama dan Penyakit (SIPERDITAN) Tanaman Padi Berbasiskan Geografic Information System (GIS)	Hibah KKP3 Badan Litbang Kementerian Pertanian	Harisno, N. Legowo
3	2016	Pemodelan Services Berbasis Sinergi SOA & BPM Untuk Meningkatkan Fleksibilitas Sistem Informasi (Studi Kasus:BinusMaya)	Hibah Dosen UBinus	A.N.Fajar, N.Legowo
4	2017	The Application of Nash Equilibrium for Harnessing Disruptive Innovations	Ristek Dikti	A. Trisetyarso, F. Faisal, N.Legowo

5	2018	Identifikasi Dan Prediksi Tingkat Kesulitan Instans Penjadwalan Kuliah Menggunakan Pembelajaran Mesin	Terapan, Internal PT Binus	M.Tuga , N.Legowo
6	2019	Mengukur Tingkat Kesulitan Komputerisasi Penjadwalan Kuliah Menggunakan Teknik Pembelajaran Mesin	Ristek Dikti	M.Tuga, N.Legowo
7	2020	Mengukur Tingkat Kesulitan Komputerisasi Penjadwalan Kuliah Menggunakan Teknik Pembelajaran Mesin Lanjutan	Ristek Dikti	M.Tuga, N.Legowo
8	2023	Model Risiko Keamanan Informasi Medis Berbasis Fuzzy ISO 27001	Ristek Dikti	N.Legowo, W.Sardjono, E.Sutanto
9	2024	Model Risiko Keamanan Informasi Medis Berbasis Fuzzy ISO 27001	Ristek Dikti	N.Legowo, W.Sardjono, T.Prasandy,
10	2024	Pengembangan Alat Pengukur Tingkat Kematangan Proses Manajemen Proyek Teknologi Dan Sistem Informasi Berbasis Pmbok Versi 6	Ristek Dikti	N.Legowo, N.Suryanto

References

- Application and Data Integration Based on Services Oriented Architecture in Enterprise (N.Legowo, A. Sumedi, 2023).
- Outlier Detection in VPN Authentication Logs for Corporate Computer Networks Access using CRISP-DM, (N.Legowo, W.M. Bad, 2024).
- Fuzzy Risk Model for Research and Development Department in Clinical Laboratory (N. Legowo, at al 2023).
- Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001 (N.Legowo, Y.Juhartoyo, 2022)
- Assessment of Security Awareness Perception on Indonesian Media Industry, (T.P. Putra, N.Legowo, 2024).
- Audit information system risk management using ISO 27001 framework at private bank (E.Kaban, N Legowo, 2018)
- Risk Management of Credit Card Payment Gateway using Octave Allegro Methodology At Electronic Payment Provider Institution (N.Legowo, K.A. Saputra, 2019)
- Implementation of incident management for data services using ITIL V3 in telecommunication operator company (A.D. Nugraha, N.Legowo 2017)

- Evaluating Hotel Technology Service Management via ITIL Practice for Incident Response Enhancements, (D.Jonathan, N.Legowo, 2024)
- ISO 27001 Fuzzy-Based Medical Information Security Risk Model, Submitted (N.Legowo, W.Sardjono at.al 2025).in Process
- A Hospital Enterprise Architecture for Medical Information Security, submitted (N.Legowo, W. Sardjono, at al, 2025). in Process
- Adel A.N., Abdualmajed A. Al-Khulaidi, Mijahed N. Aljober. Measuring the ınformation security maturity of enterprises under uncertainty using Fuzzy AHP. I.J. Information Technology and Computer Science, 2018, 4, pp.10-25.
- Tegar Pratama Putra , Nilo Legowo (2024) Enhancing Information Security Awareness in the Indonesia Media Industry Using AHP Approach.
- Alovsat Garaja Aliyev (2022) Technologies Ensuring the Sustainability of Information Security of the Formation of the Digital Economy and their Perspective Development Directions.
- Zhengbing Hu, Sergiy Gnatyuk, Oksana Koval, Viktor Gnatyuk and Serhii Bondarovets. Anomaly detection system in secure cloud computing environment. I. J. Computer Network and Information Security, 2017, 4, pp.10-21.
- https://cybersecurityventures.com/annual-cybercrime-report-2017/

Ucapan Terima Kasih

Bapak/ibu yang saya hormati,

Sebelum saya mengakhiri pidato pengukuhan ini, sekali lagi saya dan keluarga memanjatkan puji syukur kehadirat Allah SWT atas segala nikmat yang telah dianugrahkanNya kepada kami sekeluarga khususnya atas pengangkatan saya sebagai Guru Besar Tetap di Universitas Bina Nusantara.

Selanjutnya, izinkanlah saya mengucapkan terima kasih pada berbagai pihak yang telah membantu dan mendukung saya mencapai jabatan fungsional akademik tertinggi di Universitas Bina Nusantara. Secara khusus, saya mengucapkan terima kasih pada:

- Pemerintah Republik Indonesia, melalui Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi, Bapak Prof. Satryo Sumantri Brojonegoro, Ph.D. beserta jajarannya yang telah menetapkan dan mengangkat saya sebagai Guru Besar Tetap di Binus Graduate Program, Universitas Bina Nusantara,
- Direktur Jenderal Pendidikan Tinggi, Riset, dan Teknologi, Bapak Prof. Dr. rer. nat. Abdul Haris, M.Sc. dan jajarannya, yang telah menerbitkan Sertifikat Uji Kompetensi Jenjang Jabatan akademik Dosen

sebagai Guru Besar tetap di Universitas Bina Nusantara pada bidang ilmu Industrial & System Engineering.

- Kepala Lembaga Layanan Pendidikan Tinggi Wilayah III Lembaga Layanan Pendidikan Tinggi Wilayah III Bapak Prof. Dr. Toni Taharudin, S.Si., M.Sc, beserta jajaranya, yang telah mendukung, memproses, dan menyetujui usulan Senat Perguruan Tinggi Universitas Bina Nusantara.
- Chief Executive Officer Yayasan Bina Nusantara Bapak Ir. Bernard Gunawan
- Chief Strategic Officer Yayasan Bina Nusantara Bapak Ir. Carmelus Susilo
- President of BINUS Higher Education Bapak Stephen Wahyudi Santoso, BSE, MSIST, CBDMP dan segenap jajaranya.
- Ketua Dewan Guru Besar Universitas Bina Nusantara Bapak Prof. Dr. Ir. Harjanto Prabowo,M.M.
- Rektor dan Ketua Senat Universitas Bina Nusantara Ibu Dr. Nelly, S.Kom., M.M., CSCA
- Para Guru Besar Dewan Pelantik dan wakil rektor Universitas Bina Nusantara
- Direktur Binus Graduate Program, Prof.Dr. Sani Muhamad Isa, S.Si., M.Kom., dan sebelumnya, alm Prof. Dr. Gerardus Polla M.App.Sc. yang telah memberikan keteladanan, menugaskan dan kesempatan saya untuk melanjutkan kuliah S3 DRM di Binus.
- Bapak Sablin Yusuf dan Dr. Fredy Purnomo yang telah merekrut saya sebagai FM STR di SOCS dan menugaskan saya di Deputy Head prodi MMSI, BGP.
- Ketua Jurusan Dr. Ir Tanty Oktavia, S.Kom,MM, dan sebelumnya DR. Viany Utami Tjin, S.Kom, dan sebelumnya alm Dr. Ir. Harisno MM dan Semua Dosen MMSI yang selalu membangun team work dalam berkarya di program studi.
- Prof..Dr.Ir. Edi Abdurachman MS., M.Sc. DR. Ir Iman Herwidiana Kartowisastro Msc dan Alm Prof Dr. Dyah Budiastuti, SE., MM selaku Promotor dan Ko Promotor saya saat menempuh studi S3 di Binus University yang telah membimbing dan melatih saya dalam melakukan penelitian, penerbitan journal internasional.
- Prof. Dr. Ir. Kudang Boro Seminar, M. Sc., Prof. Dr. Ir. R. Eko Indrajit, M.Sc., MBA., Mphil., MA., Prof. Dr. Ir. Edi Abdurachman, MS., M.Sc. yang telah berkenan hadir menjadi dewan pelantik eksternal yang berkenan hadir dan memberikan testimoni dalam acara pengukuhan guru besar ini.
- Bapak Dr. Ir. Bonifasius Wahyu Pudjianto, M.Eng (Kepala badan pengembangan sumber daya manusia Kemkomdigi), yang berkenan hadir dan memberikan testimodi pada acara pengukuhan di pagi hari ini.
- Prof. Dr. Idris Gautama SE, MM sebagai mentor pengajuan guru besar, yang telah membantu saya dalam percepatan pengajuan sebagai guru besar.

- Ibu Dr. Olifia Rombot, S.Sos., S.Pd., M.Pd., mba Sri Utari, Mas Syahrial dan seluruh staf di LRC yang telah membantu dalam pengurusan dan pengajuan guru besar tetap di Binus.
- Pak Joko Raditya, ibu Ika, ibu Yuni , ibu DR. Astari ,dan pak Dr.Gunawan serta seluruh anggota panitia pengukuhan guru besar ini.
- Seluruh personil GBP Band yang telah memberikan penghiburan dan suasana yang meriah di acara pengukuhan guru besar ini.
- Keluarga di kantor, teman-teman dosen BGP serta teman-teman BGP operation yang banyak membantu saya dalam berkarya di Binus.
- Keluarga besar terutama Bapak saya almarhum Rochmanoe dan ibu saya Rumiyati, Istri saya Nur Edi Peni, Anak Saya Ary Suryo Bimantoro,S.Kom,M.Kom, Annisa Sita Pratiwi, S.Kom. Kakak saya Handri Herawati, Adik saya Joni Agus Prasetyo, yang selalu berdoa dan memberikan, semangat dan momen penting dalam hidup saya.
- Seluruh keluarga besar Mertodiharjo, Om , Tante, kakak, Adik, ponakan, yang selalu memberikan dukungan dan spirit untuk berkarya.
- Seluruh kolega dosen yang telah hadir dalam acara Pengukuhan dari Binus, Perbanas Insitute, UIN Jakarta, Ubara, Univ. Pancasila, Usni, Univ. Bakri, Untar, Univ. Esa Unggul, Univ. Mercubuana, Bunda Mulia, UG, UnKris, Unas, ITB Swadarma, STMIK Jayakarta.
- Seluruh teman – teman saya di SMP N1, SMAN1 Magetan, Kuliah S1 Unesa, S2 Benarif, S3 DRM Binus yang telah hadir ,yang selalu memberikan dukungan dan inspirasi dalam karir saya.

Akhir kata, saya mengucapkan terima kasih yang tak terhingga kepada seluruh hadirin yang dengan penuh kesabaran mengikuti acara pengukuhan ini, baik secara onsite maupun secara online. Semoga Allah SWT senantiasa memberikan Rahmat dan HidayahNya serta membalas segala budi baik bapak ibu semua dengan kebaikan yang berlipat ganda, Amin.

Pantun : mhn kata cakep ya bapak dan ibu.

Pergi ke pantai melihat karang,
Ombak besar harus diwaspada.
Risiko sistem informasi harus diterawang,
Agar bisnis tak mudah merana.

Ada satu lagi bapa dan ibu:

Ke Kemanggisan naik sepeda,
Melihat kampus Binus megah berdiri.
Terima kasih untuk teman2 semua,
Orasi ilmiah sampai disini

Wabillahi Taufiq Wal Hidayah, Wassalamu’alaikum Warahmatullahi Wabarakaatuh.