LAPORAN

PRAKTIK KERJA LAPANGAN

ANALISIS TEKNIK PENERJEMAHAN ARTIKEL KEAMANAN SIBER DAN AKTA NOTARIS

ANNISA FITRIA
1908411008

PROGRAM STUDI BAHASA INGGRIS UNTUK KOMUNIKASI BISNIS DAN PROFESIONAL

JURUSAN ADMINISTRASI NIAGA

DEPOK

2023

HALAMAN PENGESAHAN
LAPORAN PRAKTIK KERJA LAPANGAN

a.	Judul Naskah	: Analisis Teknik Penerjemahan Artikel Keamanan Siber dan Akta Notaris
b.	Penyusun	
	1) Nama	: Annisa Fitria
	2) NIM	: 1908411008
c.	Jurusan	: Administrasi Niaga
d.	Program Studi	: Bahasa Inggris Untuk Komunikasi Bisnis dan Profesional
e.	Waktu Pelaksanaan	: 1 Agustus 2022 – 2 September 2022
f.	Tempat Pelaksanaan	: Dewan Ketahanan Nasional (JI. Medan Merdeka Barat No.15, RT.2/RW.3, Gambir, Kecamatan Gambir, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10110)

Depok, 20 Januari 2023

Pembimbing PNJ,

Dra. Lenny Brida, Dipl. TESOL, M.Psi., M.Hum.
NIP. 195808121986032001

Pembimbing Perusahaan

Abdul Cholik, S.H., M.H.
Kolonel Ach/ NRP. 11050

Mengesahkan,

KPS BISPRO,

Dr. Dra. Ina Sukaesih, Dipl. TESOL, M.M., M.Hum

NIP. 196104121987032004

HALAMAN PENGESAHAN
LAPORAN PRAKTIK KERJA LAPANGAN

a.	Judul Naskah	: Analisis Teknik Penerjemahan Artikel Keamanan Siber dan Akta Notaris
b.	Penyusun	
	1) Nama	: Annisa Fitria
	2) NIM	: 1908411008
c.	Jurusan	: Administrasi Niaga
d.	Program Studi	: Bahasa Inggris Untuk Komunikasi Bisnis dan Profesional
e.	Waktu Pelaksanaan	: 7 September 2022 – 30 November 2022
f.	Tempat Pelaksanaan	: PT Jakarta International Translation Service, Jl. Raya Lenteng Agung No.22, Jagakarsa, Jakarta Selatan

Depok, 20 Januari 2023

Pembimbing PNJ,

Dra. Lenny Brida, Dipl. TESOL, M.Psi., M.Hum.
NIP. 195808121986032001

Pembimbing Perusahaan,

M. Ali Mahfudz

Mengesahkan,
KPS BISPRO,

Dr. Dra. Ina Sukaesih, Dipl. TESOL, M.M., M.Hum
NIP. 196104121987032004

KATA PENGANTAR

Puji syukur Penulis panjatkan kepada Allah SWT, karena atas berkat dan rahmat-Nya, Penulis dapat menyelesaikan laporan Praktik Kerja Lapangan yang dilaksanakan di PT Jakarta Internasional Translation Service. Laporan Praktik Kerja Lapangan ini dilakukan sebagai salah satu rangka memenuhi syarat untuk mencapai gelar Sarjana Terapan. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, penyusunan laporan Praktik Kerja Lapangan akan sangat sulit bagi Penulis untuk diselesaikan. Oleh karena itu, Penulis mengucapkan terima kasih kepada:

a. Dr. Dra. Ina Sukaesih, Dipl. Tesol, M. M., M. Hum, selaku kepala Program Studi Bahasa Inggris untuk Komunikasi Bisnis dan Profesional
b. Dra. Lenny Brida, Dipl. TESOL, M.Psi., M.Hum. selaku dosen pembimbing yang telah meluangkan waktu, tenaga dan pikiran untuk membimbing Penulis dalam menulis laporan Praktik Kerja Lapangan ini.
c. Kolonel Arh Abdul Cholik, S.H., M.H. selaku penyelia di Dewan Ketahanan Nasional yang telah memberikan kesempatan dan membimbing Penulis untuk melaksanakan Praktik Kerja Lapangan di Dewan Ketahanan Nasional
d. Bapak Ali Mahfudz selaku penyelia di PT Jakarta Internasional Translation Service yang telah memberikan kesempatan dan membimbing Penulis untuk melaksanakan Praktik Kerja Lapangan di PT Jakarta Internasional Translation Service
e. Orang tua, keluarga serta teman-teman yang telah memberikan Doa dan dukungannya kepada Penulis.

Akhir kata, Penulis berharap Allah SWT membalas segala kebaikan semua pihak yang telah memberikan bantuan serta dukungannya.

Depok, Januari 2023

Penulis

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1. Latar Belakang

Politeknik Negeri Jakarta merupakan perguruan tinggi negeri vokasi yang didirikan untuk memenuhi kebutuhan dalam dunia industri jasa maupun industri manufaktur. Tujuannya adalah untuk mempersiapkan sumber daya manusia yang siap kerja dan profesional dalam bidangnya sehingga dapat ikut serta berperan untuk memajukan bangsa. Politeknik juga menerapkan kurikulum teori (45%) dan praktik (55%). Oleh karena itu, mahasiswa Politeknik Negeri Jakarta harus mengikuti kegiatan PKL (Praktik kerja Lapangan).

Praktik Kerja Lapangan merupakan salah satu kegiatan wajib perkuliahan di Politeknik termasuk prodi Bahasa Inggris dan Komunikasi Bisnis dan Profesional. Melalui kegiatan PKL ini, mahasiswa diharapkan mengenali, memahami kondisi lingkungan kerja, jenis pekerjaan, bidang usaha, dan berbagai peluang yang ada dalam perusahaan, institusi, instansi, dan dunia industri. Setelah PKL selesai, mahasiswa melaporkan hasil kegiatan berupa Laporan Kerja Praktik Lapangan kepada pembimbing masing-masing.

Penulis melaksanakan kegiatan PKL di dua instansi atau perusahaan. Instansi pertama adalah Dewan Ketahanan Nasional atau Wantannas yang merupakan lembaga pemerintah. Penulis diberikan tugas untuk menulis artikel bahasa Inggris pada minggu pertama dan kedua. Selanjutnya, penulis diberikan tugas untuk menerjemahkan artikel tentang keamanan siber dari bahasa Indonesia ke bahasa Inggris. Tempat kedua adalah PT Jakarta International Translation Service (JITS). Penulis diberikan tugas untuk menerjemahkan berbagai macam dokumen, seperti dokumen kredensial, sertifikat/akta, ijazah, surat keterangan dokter, dan abstrak.

1.2. Ruang Lingkup Kegiatan

Pada Praktik Kerja Lapangan di Dewan Ketahanan Nasional, Penulis berfokus untuk menulis beberapa artikel dan menerjemahkan Artikel Keamanan Siber pada bagian pendahuluan. Selanjutnya, PT Jakarta International Translation Service

memberikan tugas untuk menerjemahkan dokumen-dokumen kredensial, akademik, dan hukum.

1.3. Waktu dan Tempat Pelaksanaan

Waktu dan tempat pelaksanaan Praktik Kerja Lapangan (PKL) yang dilaksanakan oleh Penulis adalah sebagai berikut:

Tempat 1

a. Waktu : 1 Agustus 2022 s.d 2 September 2022
b. Instansi : Dewan Ketahanan Nasional
c. Alamat : Jl. Medan Merdeka Barat No.15 Jakarta Pusat
d. Situs : https://www.wantannas.go.id/

Tempat 2

a. Waktu : 7 September 2022 s.d 30 November 2022
b. Instansi : PT Jakarta Internasional Translation Service
c. Alamat : Jl. Lenteng Agung Baru No.22, Jakarta Selatan
d. Situs : Jits.co.id

1.4. Tujuan dan Kegunaan

1.4.1. Tujuan

Tujuan dari Praktik Kerja Lapangan ini adalah sebagai berikut:

a. Memahami proses penerjemahan Artikel Keamanan Siber dan Akta Notaris
b. Memahami istilah-istilah yang digunakan dalam Artikel Keamanan Siber dan Akta Notaris
c. Menerapkan ilmu pengetahuan yang telah dipelajari dan yang diberikan oleh mentor tentang penerjemahan
d. Sebagai salah satu syarat akademik untuk memenuhi SKS.

1.4.2. Kegunaan

Kegunaan dari Praktik Kerja Lapangan ini adalah sebagai berikut:

1. Menambah pengetahuan terkait dengan penerjemahan Artikel Keamanan Siber dan Akta Notaris
2. Mengasah kemampuan dalam menerjemahkan Artikel Keamanan Siber dan Akta Notaris
3. Melatih kedisiplinan dan tanggung jawab

BAB IV

PENUTUP

4.1. Kesimpulan

Setelah pelaksanaan Praktik Kerja Lapangan, Penulis dapat menyimpulkan bahwa kegiatan ini sangat bermanfaat bagi Penulis untuk lebih mengenal dunia kerja. Penulis dapat mengetahui bagaimana budaya di dalam suatu instansi dan perusahaan dalam bekerja dan berkomunikasi. Pelaksanaan PKL ini juga melatih kedisiplinan, tanggung jawab, dan keahlian dalam berkomunikasi kepada rekan-rekan kerja. Selain itu, pelaksanaan PKL terutama di bidang penerjemahan telah memberikan banyak pengetahuan terkait dengan penerjemahan dan meningkatkan keahlian Penulis dalam menerjemahkan. Meskipun masih banyak kendala dalam menerjemahkan, Penulis berusaha untuk mencari dan memahami maksud pada teks sumber sehingga tidak menghasilkan makna yang salah.

Teknik penerjemahan yang cenderung sering digunakan dalam Artikel Keamanan Siber dan Akta Notaris adalah teknik penerjemahan harafiah dan teknik penerjemahan padanan lazim. Beberapa teknik penerjemahan lain juga digunakan untuk merubah tata bahasa atau menyederhanakan makna sehingga mudah dipahami dan pesan tersampaikan dengan baik.

4.2. Saran

Saran yang dapat Penulis berikan kepada perusahaan adalah untuk memiliki daftar glosarium istilah yang sering digunakan dalam lingkup perusahaan sehingga penerjemah mudah menemukan makna dari istilah yang dimaksud. Perusahaan juga dapat menggunakan alat bantu penerjemahan atau *CAT Tool* seperti aplikasi Trados.

DAFTAR PUSTAKA

Ardi, H. (2015). *Pengantar Penerjemahan (Introduction to Translation).* Padang: Sukabina Press.

Galingging , Y., & Tambunsaribu, G. (2021). PENERJEMAHAN IDIOMATIS PETER NEWMARK DAN MILDRED LARSON. *Jurnal Bahasa, Sastra, dan Budaya* , 59-61.

Molina , L., & Albir, A. H. (2002). Translation Techniques Revisited: A Dynamic and Functionalist Approach. *Meta, XLVII, 4*.

Supriyadi, A. (2016). KUALITAS HASIL PENERJEMAHAN KELOMPOK MAHASISWA S2 UNM-MALANG (Studi Kasus Hasil Penerjemahan Buku Teks "Approaches to Discourse" oleh Deborah Schriffrin. *Jurnal Pendidikan Bahasa dan Sastra*, 117-118.

DEWAN KETAHANAN NASIONAL RI
SEKRETARIAT JENDERAL
Jl. Medan Merdeka Barat No. 15 Jakarta Pusat 10110 - http://www.wantannas.go.id
Telepon (021) 3451066, Faksimile (021) 3451066

SURAT KETERANGAN
NOMOR : 82 /KH.01.02.11/IX/2022

1. Yang bertanda tangan di bawah ini :

a. Nama	:	Supendi, S.T., M.Tr. Opsla
b. Pangkat	:	Laksamana Pertama TNI
c. Jabatan	:	Kepala Biro Umum
d. Instansi	:	Sekretariat Jenderal Dewan Ketahanan Nasional

dengan ini menerangkan bahwa :

a. Nama	:	Annisa Fitria
b. NIM	:	1908411008
c. Universitas	:	Politeknik Negeri Jakarta
d. Fakultas	:	Administrasi Negara
e. Progam Studi	:	Bahasa Inggris untuk Komunikasi Bisnis dan Profesioanl
f. Bahwa	:	Mahasiswa tersebut benar telah melaksanakan Peraktik Kerja Lapangan (PKL) di Sekretariat Jenderal Dewan Ketahanan Nasional, selama 25 (Dua Puluh Lima) hari kerja terhitung mulai tanggal 1 Agustus s/d 2 September 2022.

2. Demikian Keterangan ini dibuat untuk dipergunakan seperlunya.

Jakarta, 5 September 2022
Kepala Biro Umum

Supendi, S.T., M.Tr. Opsla
Laksamana Pertama TNI

PT JAKARTA INTERNASIONAL MEDIA NUSANTARA
Alamat: Jl. Lenteng Agung Timur No. 22 Jakata Selatan
(Depan Universitas Pancasila)
Phone: 021-7868858, 021-28927295
Wa :082328922013 / 085842101111
Email: info@jits.co.id Website: www.jits.co.id

Nomor : JITS-002/01/2023 Jakarta, 19 Januari 2023

Perihal : Surat Keterangan Praktik Kerja Lapangan (PKL)

SURAT KETERANGAN

PRAKTIK KERJA LAPANGAN (PKL)

Yang bertanda tangan di bawat in

Nama : Syarif Hidayatulloh

Jabatan : Staff HRD

menerangkan bahwa:

Nama Mahasiswa : **Annisa Fitria**

NIM 1908411008

merupakan mahasiswa Polteknik Negeri Jakarta, Jurusan Administrasi Niaga, Program Studi Bahasa Inggris untuk Komunitas Bisnis dan Profesional, yang telah mengikut program Praktik Kerja Lapangan (PKL) di PT Jakarta Internasional Media Nusantara selama 3 (tiga) bulan dimulai pada tanggal 1 September 2022 dan berakhir pada tanggal 30 November 2022, di bawah bimbingan Bapak Moh. Ali Mahfudz, NIP A-0002, Penerjemah Bidang Umum dan Hukum.

Demikian surat keterangan ini dibuat dengan sebenarnya untuk dipergunakan sebagaimana mestinya.

Jakarta, 19 Januari 2023

PT Jakarta Internasional Media Nusantara

Syarif Hidayatulloh

Staff HRD

KEMENTERIAN RISET, TEKNOLOGI, DAN PENDIDIKAN TINGGI
POLITEKNIK NEGERI JAKARTA
ADMINISTRASI NIAGA
Jalan Prof. Dr. G. A.Siwabessy, Kampus UI, Depok 16425
Telepon (021) 7863534, 7864927, 7864926, 7270042, 7270035
Fax (021) 7270034, (021) 7270036 Hunting
Laman: http://www.pnj.ac.id e-pos: humas@pnj.ac.id

F8

FORM PEMBIMBING PKL (PENYELIA)

1. Nama Perusahaan : Dewan Ketahanan Nasional
2. Alamat : JI. Medan Merdeka Barat No.15, RT.2/RW.3, Gambir, Kecamatan Gambir, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10110
3. Judul PKL : Analisis Teknik Penerjemahan Artikel Keamanan Siber dan Akta Notaris
4. Nama Penyelia : Abdul Cholik, S.H., M.H.

No.	Minggu ke-	Aktivitas yang dilakukan	Tandatangan
1.	1 (1-5 Agustus 2022)	Menulis artikel bahasa inggris tentang "Asian Para Games 2022."	
2.	2 (8-12 Agustus 2022)	Menulis artikel bahasa inggris tentang "Kurikulum Merdeka."	
3.	3 (15-19 Agustus 2022)	Menyunting dan merevisi artikel tentang "Kurikulum Merdeka."	
4.	4 (22-26 Agustus 2022)	Menerjemahkan artikel berjudul "National Cyber-Informed Engineering Strategy" dari Bahasa Indonesia ke Inggris.	
5.	5 (29-2 September 2022)	Menerjemahkan artikel berjudul "National Cyber-Informed Engineering Strategy" dari Bahasa Indonesia ke Inggris.	

Jakarta, 5 September 2022

Supervisor Instansi,

Kol. Arh Abdul Cholik, S.H., M.H
NRP. 11050013800465

KEMENTERIAN RISET, TEKNOLOGI, DAN PENDIDIKAN TINGGI
POLITEKNIK NEGERI JAKARTA
ADMINISTRASI NIAGA
Jalan Prof. Dr. G. A.Siwabessy, Kampus UI, Depok 16425
Telepon (021) 7863534, 7864927, 7864926, 7270042, 7270035
Fax (021) 7270034, (021) 7270036 Hunting
Laman: http://www.pnj.ac.id e-pos: humas@pnj.ac.id

F8

FORM PEMBIMBING PKL (PENYELIA)

1. Nama Perusahaan/Industri : PT Jakarta International Translation Service
2. Alamat : Jl. Raya Lenteng Agung No.22, Jagakarsa, Jakarta Selatan
3. Judul PKL : Analisis Teknik Penerjemahan Artikel Keamanan Siber dan Akta Notaris
4. Nama Penyelia : M. Ali Mahfudz

No.	Hari/Tanggal	Aktivitas yang dilakukan	Tandatangan
1.	7 September 2022	Menerjemahkan Surat Keterangan Dokter dan Ijazah.	
2.	8 September 2022	Pembahasan dan revisi tugas bersama mentor.	
3.	15 September 2022	Bimbingan oleh alumni dan mentor.	
4.	20 September 2022	Menerjemahkan dokumen kontrak dari Inggris ke Indonesia.	
5.	3 Oktober 2022	Evaluasi dan bimbingan oleh mentor di kantor.	
6.	6 Oktober 2022	Menerjemahkan abstrak dari Indonesia ke Inggris.	
7.	11 Oktober 2022	Menerjemahkan abstrak, spt 1770S, dan akta	
8.	27 Oktober 2022	Menerjemahkan laporan keuangan, surat pernyataan&jaminan layanan bank, slip setoran, ikhtisar polis, dan teks IT.	

9.	3 November 2022	Evaluasi dan pembahasan tugas oleh mentor.	
10	9 November 2022	Evaluasi dan pembahasan tugas oleh mentor.	
11	25 November 2022	Evaluasi dan pembahasan tugas oleh mentor serta melakukan analisis kalimat.	
12	30 November 2022	Evaluasi dan pembahasan tugas oleh mentor.	

Jakarta, 06-01-2023

Supervisor Perusahaan,

(M. Ali Mukhtadi)

Introduction

Currently, cybersecurity for most critical infrastructure control systems is addressed separately from system design and engineering. This gap has resulted in an ever-growing list of additive security technologies that are introduced after the fact to mitigate cyber vulnerabilities. Adding security technologies after the fact is more costly and less effective. What if critical energy infrastructure systems were designed and operated with cybersecurity built in, rather than bolted on after deployment? CIE provides a way to greatly reduce, and in some cases eliminate, cyber risks from the outset and increase overall efficiency and effectiveness.

CIE is an emerging approach that aims to integrate cybersecurity considerations into the conception, design, build, and operation of *any* physical system that has digital connectivity, monitoring, or control.[3] CIE can be broadly defined as: The inclusion of cybersecurity considerations as a foundational element of engineering risk management for any function aided by digital technology.

Today, engineers and industrial control system technicians build energy systems with specific goals for safety, reliability, and functionality. While systems engineering includes considerable safety and failure mode analysis, cybersecurity risks are often not specifically addressed—particularly the risks of intentional cyber compromise, exploitation, and misuse. Simply put, traditional engineering risk management approaches rarely address the risks introduced by an intelligent and capable adversary with the goal of high-consequence cyber-enabled impacts.[4]

CIE Linkage to Zero Trust and Secure by Design

Cyber-informed engineering embraces "secure by design" and "zero trust" software security strategies, and expands these concepts beyond software engineering to the engineering of cyber-physical systems.

Secure-by-design software development shifts the security focus from finding and patching vulnerabilities to eliminating design flaws in the architecture of a software system. CIE expands this concept to build secure architectures into physical infrastructure systems that have digital access or control.

A zero-trust architecture removes any implicit trust from devices or user accounts, moving away from the concept of a security perimeter that keeps attackers out. CIE embodies this approach by assuming that compromise is likely, and deploying resilient layered defenses that minimize the consequences possible when an asset or credential is compromised.

CIE represents the Department of Energy's strategy for implementing these approaches into energy infrastructure.

As a result, most cybersecurity solutions are introduced late in the engineering lifecycle, if at all, providing inadequate and more costly protection for the nation's energy industrial control systems (ICS). This approach misses significant opportunities to "engineer out" cyber risk—that is, using early design decisions and engineering controls to mitigate or even eliminate avenues for cyber-enabled attack, or reduce the consequences when an attack occurs. CIE embraces many complementary security approaches today, such as "zero trust" and "secure by design," conceptually extending them beyond application to software systems to include application to cyber-physical infrastructure.

CIE proposes a shift in focus in the way the nation's engineers, control system technicians, manufacturers, and operators approach security in energy systems design. Researchers began to define

[3] See more information on CIE at http://inl.gov/cie.
[4] High-consequence impacts, achieved using cyber means, that may disrupt energy sector functions that are critical to the nation.

the CIE approach in 2017.[5] in the intervening years, the federal government has supported several efforts that reduce cyber risks to the nation by applying CIE principles to critical energy infrastructure and new system designs. However, there is not yet a mature engineering discipline for identifying and addressing cybersecurity risk early in in the concept and design phases. There are also few commonly applied standards or guidelines to perform systems engineering risk management for ICS cybersecurity risks throughout the systems lifecycle.

CIE remains a promising approach that is not yet widely known, understood, or implemented. This National CIE Strategy offers an integrated set of recommendations to bring about the awareness, education, and resources to integrate CIE as a common practice within the Energy Sector Industrial Base.

Defining the Problem

Engineers—and the technicians who support the engineering process—are critical to the design, implementation, and secure operation of complex energy infrastructure and control systems. Even in this critical role, engineers often lack training, a body of knowledge, and other reinforcement of cybersecurity practices to effectively address cyber threats in energy infrastructure. Given the current and increasing criticality of digital control systems within critical energy infrastructure, this is a priority gap that must be addressed by the engineering community and the nation.

Current State

The adoption of digital technology into critical operational and engineering functions can introduce vulnerabilities that could compromise the availability, integrity, trustworthiness, or authenticity of the complex control systems serving those functions. Unless cybersecurity risks are explicitly considered within current approaches to hazard evaluation,[6] these vulnerabilities are not typically captured, missing critical opportunities to reduce or eliminate them during engineering and design. The engineers who oversee, invent, design, create, install, maintain, and dispose of these complex cyber-physical systems may lack the necessary requirements, context,[7] education, practices, and tools (in order of descending importance) to identify, understand, and mitigate these risks. Instead, engineers and the technicians who support them too often rely on the external application of cybersecurity measures by specialized practitioners late in the system implementation lifecycle. This current state

Alignment of CIE with Industry Standards and Guidelines

The National CIE Strategy will inform the evolution and maturation of industry standards and guidelines to align with CIE principles and provide manufacturers and asset owners with essential tools to demonstrate their adoption of CIE. Recent guidance shows strong alignment with CIE. Alignment with CIE can be an early target for the standards specification activities recommended in the Development pillar. Examples include the International Society of Automation (ISA)/International Electrotechnical Commission (IEC) 62443 series of standards, the National Institute of Standards and Technology (NIST) SP 800-160 guideline, and the SAE International G-32 Cyber-Physical Systems Security Committee standards work.

[5] Robert S. Anderson, Jacob Benjamin, Virginia L. Wright, Luis Quinones, and Jonathan Paz, *Cyber-Informed Engineering*, Idaho National Laboratory, 2017. doi:10.2172/1369373.

[6] Such as: failure modes effects analysis (FMEA), What-If analysis, hazard and operability study (HAZOP), fault tree analysis (FTA), and event tree analysis (ETA).

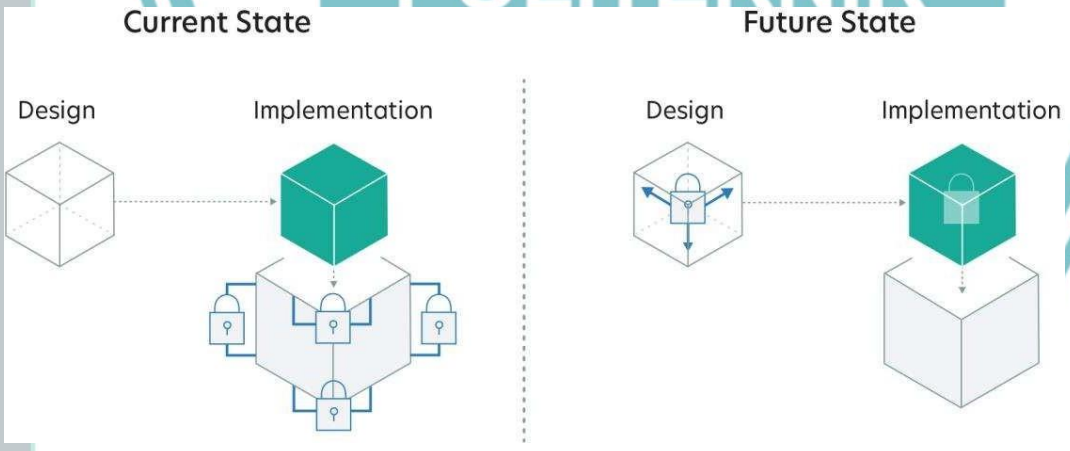
[7] *Context* refers to the broader environment in which the work of the engineer will be deployed for the benefit of society.

reduces the overall resilience and cost competitiveness of the systems supporting critical functions, increasing the risk of high-consequence cyber-enabled impacts that threaten national and economic security or public health and safety. This risk is magnified by the increase in well-resourced, sophisticated cyber adversaries who are targeting these cyber-physical systems to create damage or destruction.

Desired End State

What does CIE look like when fully implemented? Engineers incorporate cybersecurity practices into their body of knowledge, including engineering minimum requirements and specifications, for physical energy infrastructure systems that incorporate digital controls. Engineers and technicians fully evaluate the potential for disruption and harm from cyber attacks when designing and integrating digital components into energy systems. Control systems are chosen and integrated into physical systems only when a complete assessment of risks has been performed and the organization accepts any residual risk after being accurately informed of potential consequences. There is effective and continuing communication among owners, operators, designers, maintainers, device manufacturers, and system integrators to support risk-informed decisions concerning the use of control systems in energy infrastructure. Future technology is designed to be cyber resilient from the initiation of research through the development lifecycle. Cyber risk management early in the system lifecycle results in a more effective and efficient application of cybersecurity controls, and enables resilient operation of critical functions during potential cyber compromise. The broad range of stakeholders influencing energy infrastructure all are appropriately informed about cyber risks and have a culture of responsibility and agency for cybersecurity. Engineered systems are more cost-effective to operate securely over their life cycle, and security controls are more effective because they were built in at the design phase.

Figure 2. Current State vs. Desired End State

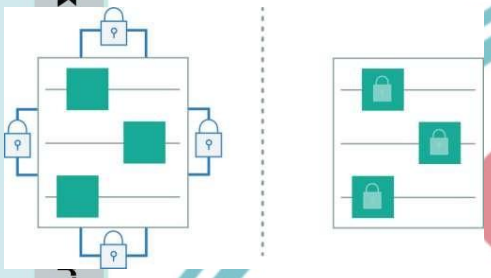


Principles of CIE

There are fundamental principles of CIE that should be considered for any energy sector infrastructure project that relies upon a digital industrial control system. By principles we mean the ideas, rules, or concepts that need to be kept in mind when solving an engineering problem. The principles identified here are not exhaustive but do serve as important elements within an ICS engineering risk management process. Principles identified as key considerations for CIE implementation are grouped into Design and Organizational principles, and are enumerated below.

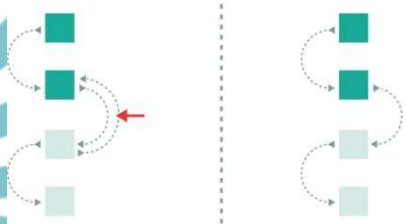
Design and Operational Principles

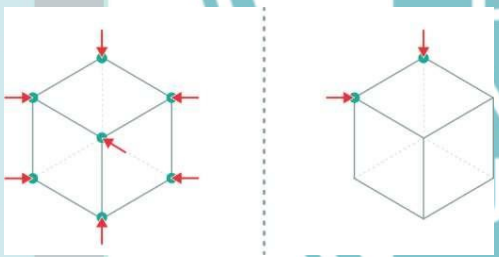
Consequence-Focused Design — Apply CIE strategies first and foremost to the critical functions where cyber manipulation could result in unacceptable consequences. Use a structured and thorough process to identify where cyber attacks may result in high-consequence impacts and examine how to avoid such consequences through secure design, implementation, and operation.



Engineered controls—Identify engineering changes and process controls early in system design to eliminate or mitigate cyber risk, reducing the need to bolt on additive IT security controls during implementation. Taken together, coordinated controls and processes are used to eliminate high-consequence cyber-enabled impacts. This requires integrating cyber experts and expertise into systems design, engineering, and modification.

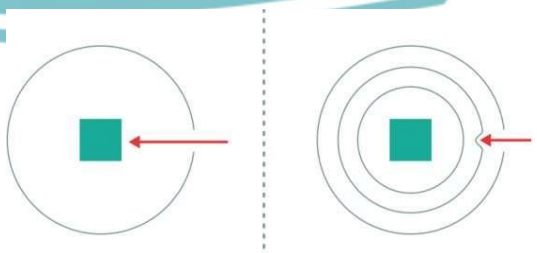
Secure information architecture—Design information pathways to ensure data flows only in desired ways and use proper architectural controls to enforce those information flows. This limits an attacker's ability to use the system or its information in undesired ways.



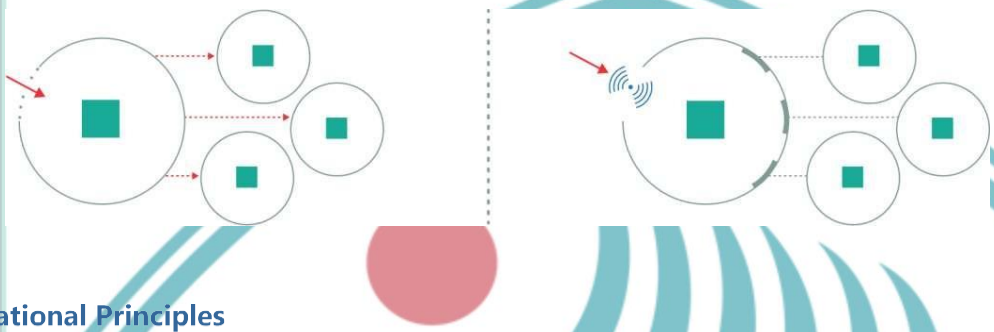


Design simplification—Simplify the system, component, or architecture design and limit high-consequence, low-value complexity within digital functions at the outset, reducing the opportunity for attackers to misuse digital functionality. Design simplification includes reducing latent capabilities in digital systems that operators may disable or may not even be aware of, but which attackers could leverage.

Resilient layered defenses—Assume compromise and employ a defense-in-depth strategy, reducing the opportunity for a single failure to impact critical functions or create cascading failures. This includes building in diversity, redundancy, and system hardening for adequate defense and predictable degradation during a cyber incident.



Active defense—Employ dynamic elements in the design of systems that detect and defend against cyber threats, enabling the system to continue operating resiliently when an intruder is detected, and isolate or remove the threat without compromising critical operations.



Organizational Principles

Interdependency evaluation—Integrate input from multiple disciplines and operational departments (e.g., safety, quality, maintenance, chemical) to understand how digital misuse could affect their area of operations. This ensures engineers can adequately plan for risks introduced by system interdependencies that may be outside of the engineer's traditional purview.

Digital asset awareness—Maintain a complete and accurate digital asset inventory, enabling engineers to track hardware, firmware, and software over time, and actively analyze the vulnerabilities that may reside within them.

Cyber-secure supply chain controls—Use procurement language and contract requirements to ensure that vendors, integrators, and third-party contractors deliver products that meet design specifications and adhere to organizational processes and controls that support cybersecurity.

Planned resilience with no assumed security—Expect that any digital component or system may be compromised at some point during its lifecycle, and plan for continued operation during and after a cyber attack that degrades digital controls. Implement a zero-trust architecture to the greatest degree possible.

Engineering information control—Protect sensitive engineering records—including requirements, specifications, designs, configurations, testing, etc.—that if released may provide attackers critical information that places those systems at greater risk.

Cybersecurity culture—Build cybersecurity into the organizational culture by leveraging a cross-functional and cross-disciplinary team to consider cyber-related concerns in the system design and implementation. Adopt continuous cybersecurity training across the organization to collectively empower all staff to participate in cybersecurity.

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Pendahuluan

Saat ini, keamanan siber untuk sebagian besar sistem kontrol infrastruktur penting ditangani secara terpisah dari desain dan rekayasa sistem. Perbedaan ini telah menghasilkan daftar teknologi keamanan tambahan yang diperkenalkan setelah fakta untuk mengurangi kerentanan siber. Menambahkan teknologi keamanan yang kenyataannya lebih mahal dan kurang efektif. Bagaimana jika sistem infrastruktur energi penting dirancang dan dioperasikan dengan keamanan siber yang terpasang di dalamnya, bukan dibaut setelah penggunaan? CIE menyediakan cara yang mampu untuk mengurangi dan dalam beberapa kasus menghilangkan risiko siber dan meningkatkan efisiensi dan efektivitas secara keseluruhan.

CIE adalah pendekatan yang muncul untuk mengintegrasikan pertimbangan keamanan siber ke dalam gagasan, desain, pengembangan, dan pengoperasian sistem fisik apa pun yang memiliki konektivitas, pemantauan, atau kontrol digital. CIE pada umumnya didefinisikan sebagai: Pengikutsertaan pertimbangan keamanan siber sebagai elemen dasar dari manajemen risiko rekayasa untuk setiap fungsi yang dibantu oleh teknologi digital.

Saat ini, para insinyur dan teknisi sistem kontrol industri membangun sistem energi dengan tujuan khusus untuk keselamatan, keandalan, dan fungsionalitas. Saat rekayasa sistem mencakup analisis mode keselamatan dan kegagalan yang cukup besar, risiko keamanan siber sering kali tidak ditangani secara khusus—terutama risiko kompromi, eksploitasi, dan penyalahgunaan siber yang disengaja. Sederhananya, pendekatan manajemen risiko rekayasa tradisional jarang menangani risiko yang ditimbulkan oleh pihak lawan yang cerdas dan cakap dengan tujuan dampak yang memungkinkan siber dengan ancaman tinggi.[4]

Akibatnya, sebagian besar solusi keamanan siber diperkenalkan di akhir siklus hidup rekayasa,jika memungkinkan, memberikan perlindungan yang tidak memadai dan lebih mahal untuk sistem kontrol industri *(Industrial Control Systems (ICS)* energi.

Keterkaitan CIE dengan *Zero Trust* dan Perancangan yang aman secara mendasar.

Rekayasa informasi siber mencakup strategi keamanan perangkat lunak yang aman secara mendasar dan "*zero trust*", serta memperluas konsep-konsep ini di luar rekayasa perangkat lunak hingga rekayasa sistem siber fisik.

Pengembangan perangkat lunak yang dirancang dengan aman mengalihkan fokus keamanan dari penemuan serta perbaikan kerentanan menghilangkan kelemahan desain dalam arsitektur sistem perangkat lunak. CIE memperluas konsep ini untuk membangun model yang aman ke dalam sistem infrastruktur fisik yang memiliki akses atau kontrol digital.

Model zerp-trust menghilangkan kepercayaan implisit dari perangkat atau akun pengguna, pindah dari konsep perimeter keamanan yang mencegah serangan. CIE mewujudkan pendekatan ini dengan mengasumsikan bahwa kompromi mungkin terjadi, dan menerapkan pertahanan berlapis yang tangguh yang meminimalkan ancaman yang mungkin terjadi ketika aset atau kredensial disetujui.

CIE mewakili strategi Departemen Energi dalam

Pendekatan

Ini kehilangan peluang signifikan untuk "merekayasa" risiko siber, yaitu menggunakan keputusan desain awal dan kontrol teknik untuk mengurangi atau bahkan menghilangkan jalan untuk serangan yang diaktifkan dunia maya, atau mengurangi dampak saat serangan terjadi. CIE mencakup banyak pendekatan keamanan

yang saling melengkapi saat ini, seperti "*zero trust*" dan "keamanan secara mendasar," secara konseptual perluasan di luar aplikasi ke sistem perangkat lunak untuk memasukkan aplikasi ke

infrastruktur fisik siber.

CIE mengusulkan perubahan fokus dalam cara para insinyur, teknisi sistem kontrol, pabrikan, dan operator nasional mendekati keamanan dalam desain sistem energi. Para peneliti mulai mendefinisikan

[3] Lihat informasi lebih lanjut tentang CIE di http://inl.gov/cie.

[4] Dampak yang memiliki konsekuensi yang tinggi dicapai dengan menggunakan sistem siber, yang dapat mengganggu fungsi sektor energi yang sangat penting bagi bangsa.

pendekatan CIE pada tahun 2017. [5] pada tahun-tahun berikutnya, pemerintah federal telah mendukung beberapa upaya yang mengurangi risiko siber bagi negara dengan menerapkan prinsip-prinsip CIE pada infrastruktur energi kritis dan desain sistem baru. Namun, belum ada disiplin rekayasa yang matang untuk mengidentifikasi dan menangani risiko keamanan siber di awal fase konsep dan desain. Ada juga beberapa standar atau pedoman yang umum diterapkan untuk melakukan manajemen risiko rekayasa sistem untuk risiko sistem kontrol industri keamanan siber di seluruh siklus hidup sistem.

CIE mempertahankan pendekatan yang menjanjikan yang belum diketahui, dipahami atau diimplementasikan secara luas Strategi CIE Nasional ini menawarkan serangkaian rekomendasi terpadu untuk mewujudkan kesadaran, pendidikan, dan sumber daya untuk mengintegrasikan CIE sebagai praktik umum dalam Basis Industri Sektor Energi.

Menentukan Permasalahan

Insinyur dan teknisi yang mendukung proses perekayasaan sangatlah penting dalam desain, implementasi, dan pengoperasian yang aman dari sistem kontrol dan infrastruktur energi yang kompleks. Dalam peran penting ini, para insinyur sering kekurangan pelatihan, pengetahuan, dan dukungan lain dari praktik keamanan siber untuk secara efektif mengatasi ancaman siber dalam infrastruktur energi. Ini adalah kesenjangan prioritas yang harus diatasi oleh komunitas teknik dan bangsa, mengingat saat ini dan meningkatnya keutamaan sistem kontrol digital dalam infrastruktur energi yang penting.

Keadaan Saat Ini

Penerapan teknologi digital ke dalam fungsi operasional dan rekayasa penting dapat menimbulkan kerentanan yang dapat membahayakan ketersediaan, integritas, kepercayaan, atau keaslian sistem kontrol kompleks yang menjalankan fungsi tersebut. Kecuali jika risiko keamanan siber secara eksplisit dipertimbangkan dalam pendekatan evaluasi bahaya saat ini,[6] kerentanan ini biasanya tidak didapatkan, kehilangan peluang penting untuk mengurangi atau menghilangkannya selama rekayasa dan desain. Para insinyur yang mengawasi, menemukan, merancang, membuat, memasang, memelihara, dan menghilangkan sistem fisik siber yang kompleks ini mungkin kekurangan persyaratan, konteks,[7] pendidikan, praktik, dan alat yang diperlukan (dalam urutan yang semakin penting) untuk mengidentifikasi, memahami , dan mengurangi risiko ini. Sebaliknya, para insinyur dan teknisi yang mendukung mereka terlalu sering mengandalkan penerapan eksternal tindakan keamanan siber oleh praktisi khusus di akhir siklus hidup implementasi sistem. Keadaan Saat Ini

Penyesuaian CIE dengan Standar dan Pedoman Industri

Strategi CIE Nasional akan menginformasikan evolusi dan perkembangan standar dan pedoman industri untuk menyelaraskan dengan prinsip-prinsip CIE dan memberikan pabrikan dan pemilik aset alat penting untuk menunjukkan penggunaan CIE. Pedoman terbaru menunjukkan keselarasan dengan CIE yang kuat. Penyelarasan dengan CIE dapat menjadi target awal untuk kegiatan spesifikasi standar yang direkomendasikan dalam pilar Pengembangan. Contohnya termasuk Standar Otomatisasi Industri (ISA)/Komisi Elektroteknik Internasional (IEC) 62443 seri standar, pedoman Institut Nasional Standar dan Teknologi(NIST) SP 800-160, dan SAE International G-32 *Cyber-Physical Systems Security* Standar komite bekerja.

[5] Robert S. Anderson, Jacob Benjamin, Virginia L. Wright, Luis Quinones, and Jonathan Paz, *Cyber-Informed Engineering*, Idaho National Laboratory, 2017. doi:10.2172/1369373.

[6] Seperti: Mode Kegagalan dan Analisis Efek (Failure Modes Effects Analysis (FMEA)), Analisis *What-If*, Studi Potensi Bahaya dan Operasional (Hazard and Operability Study (HAZOP)), Analisis Pohon Patah (Fault Tree Analysis (FTA)), and Analisis Pohon Kejadian (Event Tree Analysis (ETA)).

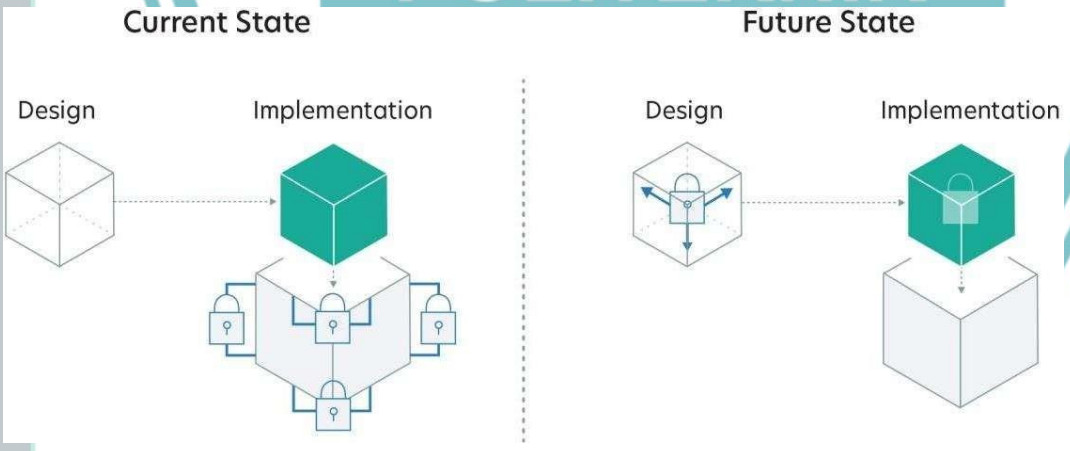
[7] Konteks mengacu pada lingkungan yang lebih luas di mana pekerjaan insinyur akan digunakan untuk kepentingan masyarakat.

mengurangi ketahanan secara keseluruhan dan daya saing biaya dari sistem yang mendukung fungsi-fungsi penting, meningkatkan risiko konsekuensi tinggi dari dampak siber yang kemungkinan dapat mengancam keamanan nasional, ekonomi, kesehatan, dan keselamatan publik. Risiko ini diperbesar oleh peningkatan musuh siber yang memiliki sumber daya baik dan canggih yang membuat sistem fisik siber ini untuk menciptakan kerusakan atau kehancuran.

Keadaan Akhir yang Diinginkan

Seperti apa CIE saat diimplementasikan sepenuhnya? Insinyur memberikan praktik keamanan siber ke dalam pengetahuan mereka, termasuk persyaratan dan spesifikasi minimum rekayasa, untuk sistem infrastruktur energi fisik yang menggabungkan kontrol digital. Insinyur dan teknisi sepenuhnya mengevaluasi potensi gangguan dan bahaya dari serangan siber saat merancang dan mengintegrasikan komponen digital ke dalam sistem energi. Sistem kontrol dipilih dan diintegrasikan ke dalam sistem fisik hanya ketika penilaian risiko yang lengkap telah dilakukan dan organisasi menerima risiko residual setelah diberitahu secara akurat tentang konsekuensi potensial. Ada komunikasi yang efektif dan berkelanjutan di antara pemilik, operator, perancang, pemelihara, produsen perangkat, dan pengembangan sistem untuk mendukung keputusan berdasarkan informasi risiko terkait penggunaan sistem kontrol dalam infrastruktur energi. Teknologi masa depan dirancang untuk menjadi ketangguhan siber dari inisiasi penelitian melalui siklus hidup pengembangan. Manajemen risiko siber di awal siklus hidup sistem menghasilkan aplikasi kontrol keamanan siber yang lebih efektif dan efisien, dan memungkinkan pengoperasian fungsi-fungsi penting yang tangguh selama potensi bahaya siber. Berbagai pemangku kepentingan yang mempengaruhi infrastruktur energi semuanya mendapat informasi yang tepat tentang risiko siber dan memiliki budaya tanggung jawab dan lembaga untuk keamanan siber. Sistem yang direkayasa dapat lebih menghemat biaya untuk beroperasi dengan aman selama siklus hidupnya, dan kontrol keamanan lebih efektif karena dibangun pada fase desain.

Gambar 2. Keadaan Saat Ini vs. Keadaan Akhir yang Diinginkan

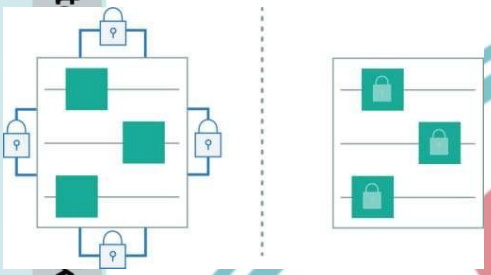


Prinsip-prinsip CIE

Ada prinsip-prinsip dasar CIE yang harus dipertimbangkan untuk setiap proyek infrastruktur sektor energi yang bergantung pada sistem kontrol industri digital. Yang kami maksud dengan prinsip adalah ide, aturan, atau konsep yang perlu diingat saat memecahkan masalah rekayasa. Prinsip-prinsip yang diidentifikasi di sini tidak lengkap tetapi berfungsi sebagai elemen penting dalam proses manajemen risiko rekayasa ICS. Prinsip-prinsip yang diidentifikasi sebagai pertimbangan utama untuk implementasi CIE dikelompokkan ke dalam prinsip-prinsip Desain dan Organisasi, dan disebutkan di bawah ini.

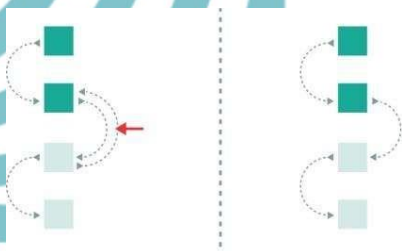
Prinsip-Prinsip Operasional dan Desain

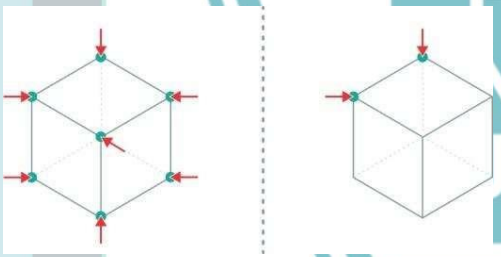
Desain yang Berfokus pada Dampak— Terapkan strategi CIE terlebih dahulu dan terutama pada fungsi penting di mana manipulasi siber dapat mengakibatkan dampak yang tidak dapat diterima. Gunakan proses yang terstruktur dan menyeluruh untuk mengidentifikasi di mana serangan siber dapat mengakibatkan dampak konsekuensi tinggi dan periksa cara menghindari konsekuensi tersebut melalui desain, implementasi, dan operasi yang aman.



Kontrol rekayasa—Identifikasi perubahan rekayasa dan kontrol proses di awal desain sistem untuk menghilangkan atau mengurangi risiko siber, mengurangi kebutuhan untuk memasang kontrol keamanan TI tambahan selama implementasi. Secara bersamaan, kontrol dan proses terkoordinasi digunakan untuk menghilangkan dampak-dampak yang memungkinkan dalam siber yang berkonsekuensi tinggi. Hal ini membutuhkan integrasi pakar dan keahlian siber ke dalam desain, rekayasa, dan modifikasi sistem.

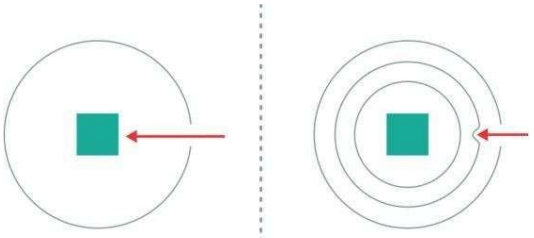
Model informasi yang aman—Merancang jalur informasi untuk memastikan aliran data hanya dengan cara yang diinginkan dan menggunakan kontrol model yang tepat untuk memberlakukan aliran informasi tersebut. Hal ini membatasi kemampuan penyerang untuk menggunakan sistem atau informasinya dalam cara-cara yang tidak diinginkan.



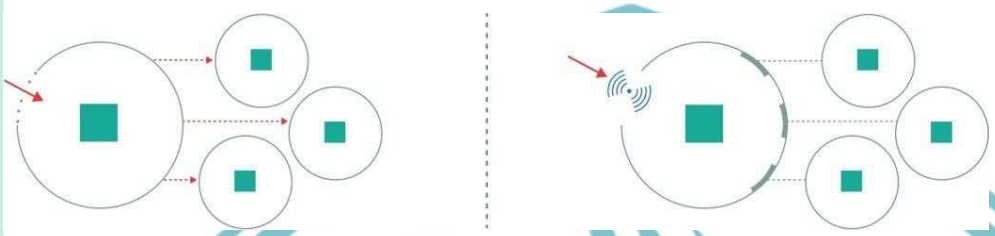


Penyederhanaan desain—Menyederhanakan sistem, komponen, atau desain model dan membatasi konsekuensi yang tinggi, kompleksitas bernilai rendah dalam fungsi digital sejak awal, mengurangi peluang bagi penyerang untuk menyalahgunakan fungsionalitas digital. Penyederhanaan desain mencakup pengurangan kemampuan tersembunyi dalam sistem digital yang mungkin dinonaktifkan atau bahkan tidak disadari oleh operator, tetapi dapat dimanfaatkan oleh penyerang.

Pertahanan berlapis yang tangguh—Asumsikan tujuan dan terapkan strategi pertahanan yang mendalam, mengurangi peluang kegagalan tunggal untuk memengaruhi fungsi penting atau membuat kegagalan bertingkat. Hal ini termasuk membangun keragaman, redundansi, dan pengerasan sistem untuk pertahanan yang memadai dan degradasi yang dapat diprediksi selama serangan



Pertahanan aktif—Gunakan elemen dinamis dalam desain sistem yang dapat mendeteksi dan tangguh melawan
ancaman siber, memungkinkan sistem untuk terus beroperasi dengan tangguh ketika penyusup terdeteksi, dan memisahkan atau menghapus ancaman tanpa menghilangkan operasi penting.



Prinsip-Prinsip Organisasi

Evaluasi interdependensi—Gabungkan masukan dari berbagai disiplin ilmu dan departemen operasional (misalnya, keselamatan, kualitas, pemeliharaan, bahan kimia) untuk memahami bagaimana penyalahgunaan digital dapat memengaruhi area operasi. Hal Ini memastikan para insinyur mampu merencanakan risiko yang ditimbulkan oleh interdependensi sistem yang mungkin berada di luar lingkup insinyur tradisional.

Kesadaran aset digital—Mempertahankan inventaris aset digital yang lengkap dan akurat, memungkinkan para insinyur melacak perangkat keras, *firmware*, dan perangkat lunak dari waktu ke waktu, dan secara aktif menganalisis kerentanan yang mungkin ada di dalamnya.

Kontrol rantai pasokan keamanan siber—Gunakan bahasa pengadaan dan persyaratan kontrak untuk memastikan bahwa vendor, perantara, dan kontraktor pihak ketiga mengirimkan produk yang memenuhi spesifikasi desain dan mematuhi proses dan kontrol organisasi yang mendukung keamanan siber.

Ketahanan yang direncanakan tanpa keamanan yang diasumsikan—Berharap bahwa setiap komponen atau sistem digital dapat disetujui di beberapa titik selama siklus hidupnya, dan merencanakan operasi lanjutan selama dan setelah serangan siber yang menurunkan kontrol digital. Menerapkan model *zero-trust* semaksimal mungkin.

Kontrol informasi rekayasa—Lindungi catatan rekayasa yang sensitif—termasuk persyaratan, spesifikasi, desain, konfigurasi, pengujian, dll.—yang jika dirilis dapat memberikan informasi penting kepada penyerang yang menempatkan sistem tersebut pada risiko yang lebih besar.

Budaya keamanan siber—Bangun keamanan siber ke dalam budaya organisasi dengan memanfaatkan tim lintas fungsi dan lintas disiplin untuk mempertimbangkan masalah terkait siber dalam desain dan implementasi sistem. Menetapkan pelatihan keamanan siber berkelanjutan di seluruh organisasi untuk secara bersamaan memberdayakan semua staf untuk berpartisipasi dalam keamanan siber.

AKTA

BSu	BSa
NOTARIS	NOTARY
XXXXX	XXXXX
S.K. Menteri Hukum Dan Hak Asasi Manusia Republik Indonesia	Decree of the Minister of Law and Human Rights of the Republic of Indonesia
Tanggal: xx xxx xxxx	On: xx xxx xxxx
Nomor: xxxxxxxx	Number: xxxxxxxx
SALINAN	COPY
Akta: PERNYATAAN KEPUTUSAN RAPAT UMUM PEMEGANG SAHAM LUAR BIASA "XXXXX"	Deed: RESOLUTIONS OF THE EXTRAORDINARY GENERAL MEETING OF SHAREHOLDERS “XXXXX”
Nomor: xxxx,-	Number: xxxx,-
Tanggal: xx xxx xxxx	Date: xx xxx xxxx
JI.xxxx - Kabupaten xxxxx Telp. xxxxxxxx E-mail: xxxxx@gmail.com	JI.xxxx - xxxxx Regency Phone. xxxxxxxx E-mail: xxxxx@gmail.com
PERNYATAAN KEPUTUSAN PARA PEMEGANG SAHAM XXXXX	RESOLUTIONS OF THE EXTRAORDINARY GENERAL MEETING OF SHAREHOLDERS XXXXX
Nomor: xxxx.-	Number: xxxx.-
Pada hari ini, Jumat, tanggal xx xxx xxxx (xx-xxx-xxxx).	On this day, Friday, the xx day of xxx xxxx (xx-xxx-xxxx).
Pukul 10.15 WIB (sepuluh limabelas menit Waktu – Indonesia Barat).	At 10.15 WIB (ten fifteen minutes West Indonesian Time)
Berhadapan dengan saya, XXXXX, Sarjana Hukum, Magister Kenotariatan, Notaris di Kabupaten xxxxx, dengan dihadiri oleh saksi-saksi yang -- nama namanya akan disebutkan pada bagian akhir akta ini dan telah dikenal oleh saya, Notaris:	Appearing before me, XXXXX, Bachelor of Law, Master of Notary, Notary of xxxxx Regency, in the presence of witnesses who have been known by me, Notary, and whose names will be mentioned at the end of this deed:
Tuan XXXXX, lahir di------Jakarta, pada tanggal	Mr. XXXXX, born in Jakarta, on the xx day of

xx xxx xxxx (xx-xxx-xxxx),----- Warga Negara Indonesia, Karyawan Swsata, bertempat tinggal di xxxxx, pemegang Kartu Tanda Penduduk dengan Nomor Induk Kependudukan xxxxxxxx;	xxx xxxx (xx-xxx-xxxx), Citizen of Indonesia, Private Employee, residing in xxxxx, holder of Resident Identity Card with Resident Identity Number xxxxxxxx;
Menurut keterangannya dalam hal ini bertindak dalam jabatannya selaku Direktur yang mewakili Direksi perseroan dibawah ini dan atas kekuatan kuasa yang diberikan dalam Notulen Keputusan RAPAT UMUM PEMEGANG SAHAM (CIRCULAR RESOLUTION OF SHAREHOLDERS) Perseroan XXXXX, berkedudukan di Jakarta Selatan, yang Anggaran dasarnya, sebagaimana dimuat dalam akta pendirian tertanggal xx xxx xxxx (xx-xxx- xxxx), Nomor xx, yang dibuat dihadapan saya, -- Notaris, akta mana telah mendapat persetujuan dari Menteri Hukum dan Hak Asasi Manusia Republik Indonesia dengan Surat Keputusannya tertanggal xx xxx xxxx (xx-xxx- xxxx), Nomor: xxxxx; -- Anggaran dasar mana telah mengalami perubahan sebagaimana ternyata dalam:	According to his statement in this case, acting as the Director representing the Board of Directors of the company below and based on the power granted in the Minutes of Meeting of CIRCULAR RESOLUTION OF SHAREHOLDERS of Company XXXXX, domiciled in South Jakarta, the articles of association of which were as contained in the establishment deed dated the xx day of xxx xxxx (xx-xxx-xxxx), Number xx, created before me, Notary, the deed of which obtained approval from the Minister of Law and Human Rights of the Republic of Indonesia as contained in the Decree dated the xx day of xxx xxxx (xx-xxx- xxxx) Number: xxxxx, the articles of association of which were amended several times as contained in:
Akta tertanggal xx xxx xxxx (xx-xxx-xxxx), Nomor xx, dibuat dihadapan XXXXX, Sarjana Hukum, Magister Kenotariatan, Notaris di Tangerang, perubahan mana telah ----- mendapatkan pengesahan dari Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia sebagaimana - ternyata dalam Surat Keputusannya tertanggal xx xxx xxxx (xx-xxx-xxx) Nomor xxxxx dan perubahan mana telah diterima dan dicatat dalam Sistem Administrasi Badan Hukum sebagaimana ternyata dalam Surat Penerimaan Pemberitahuan Perubahan Data Perseroan tertanggal xx xxx xxxx (xx-xxx-xxx) Nomor xxxxx;	The deed dated the xx day of xxx xxxx (xx-xxx-xxxx) Number xx, created before XXXXX, Bachelor of Law, Master of Notary, Notary of Tangerang, the amendment of which obtained approval from the Minister of Law and Human Rights of the Republic of Indonesia as contained in the Decree dated the xx day of xxx xxxx (xx-xxx- xxx) Number: xxxxx, as well as were received and registered at the database of Administration System of Departement of Law and Human Rights of the Republic of Indonesia by the Receipt of Notice of the changes to the Articles of Association of Company dated the xx day of xxx xxxx (xx-xxx- xxx), Number xxxxx;
Anggaran dasar terakhir perseroan termuat dalam akta tertanggal xx xxx xxxx (xx-xxx-xxxx), Nomor xx, yang dibuat dihadapan XXXXX, Sarjana Hukum, Magister Kenotariatan, Notaris di Tangerang, perubahan mana telah mendapatkan pengesahan dari Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia sebagaimana ternyata dalam Surat Keputusannya tertanggal xx xxx xxxx (xx-xxx-xxxx), Nomor xxxxx; dan menurut keterangannya tidak ada akta-akta yang	The latest Articles of Association of Company are contained in the deed dated the xx day of xxx xxxx (xx-xxx- xxx), Number xx, created before XXXXX, Bachelor of Law, Master of Notary, Notary of Tangerang, the amendment of which obtained approval from the Minister of Law and Human Rights of the Republic of Indonesia as contained in the Decree dated the xx day of xxx xxxx (xx-xxx- xxx), Number xxxxx; and according to his statement there are no other deeds

lain yang telah disebutkan diatas, yang telah diperlihatkan kepada saya, Notaris. (selanjutnya dalam akta ini disebut "Perseroan");	besides the deeds mentioned above, shown to me, Notary. (hereinafter in this deed shall be referred to as the “Company”);
Penghadap telah dikenal oleh saya, Notaris, dari - identitas yang diperlihatkan;	The Appearer has been known by me, Notary, from the identity submitted;
Bahwa pada hari xx xxx xxxx (xx-xxx-xxxx). bertempat di Kantor Perseroan Terbatas XXXXX, telah diadakan Rapat Umum Pemegang Saham Luar Biasa (untuk selanjutnya disebut "Rapat"),	that on the xx day of xxx xxxx (xx-xxx- xxx). at the office of Limited Liability Company XXXXX, Extraordinary General Meeting of Shareholders of Limited Liability Company was held (hereinafter referred to as the “Meeting”),
Telah hadir dalam rapat:	The Meeting was attended by:
I. Tuan Doktorandus XXXXX, lahir di Singkawang, pada tanggal xx xxx xxxx (xx-xxx-xxxx), Warga Negara Indonesia, Karyawan Swasta, bertempat tinggal di --- xxxxx, pemegang Nomor Induk Kependudukan xxxxxxxx;	I. Mr Doktorandus XXXXX, born in Singkawang, on the xx day of xxx xxxx (xx-xxx- xxx), Citizen of Indonesia, private, residing in xxxxx, holder of Resident Identity Card with Resident Identity Number: xxxxxxxx;
a. Selaku Komisaris perseroan	a. as the Commissioner of Company
b. Selaku pemegang saham sejumlah 74.000 (tujuh puluh empat ribu) lembar saham disetor dan ditempatkan dalam perseroan.	b. as the shareholder of 74,000 (seventy four thousand) paid and subscribed shares in the company.
II. Tuan XXXXX, lahir di Jakarta, pada tanggal xx xxx xxxx (xx-xxx-xxxx), Warga Negara -- Indonesia, Karyawan Swasta, bertempat tinggal di xxxxx, pemegang Nomor Induk Kependudukan xxxxxxxx.--	II. Mr. XXXXX, born in Jakarta, on the xx day of xxx xxxx (xx-xxx- xxx), Citizen of Indonesia, Private Employee, residing in xxxxx, holder of Resident Identity Card Number xxxxxxxx.
a. selaku Direktur;	a. as the Director
b. selaku pemegang saham sejumlah 1.000 - (seribu) lembar saham disetor dan ditempatkan dalam perseroan.	b. as the shareholder of 1,000 (one thousand) paid and subscribed shares in the company.
III. Tuan XXXXX, lahir di -- Jakarta, pada tanggal xx xxx xxxx (xx-xxx-xxxx), --- Warga Negara Indonesia, Karyawan Swasta, bertempat tinggal di xxxxx, pemegang Kartu Tanda Penduduk Nomor Induk Kependudukan (NIK) xxxxxxxx;	III. Mr. XXXXX, born in Jakarta, on the xx day of xxx xxxx (xx-xxx- xxx), Citizen of Indonesia, Private Employee, residing in xxxxx, holder of Resident Identity Card with Resident Identity Number (NIK): xxxxxxxx;

Menurut keterangannya dalam hal ini bertindak -dalam jabatannya selaku Direktur yang mewakili -- Direksi perseroan dibawah ini dan atas kekuatan kuasa yang diberikan dalam Keputusan PEMEGANG SAHAM (CIRCULAR RESOLUTION OF SHAREHOLDERS) Perseroan XXXXX, berkedudukan di -- Jakarta Selatan, yang Anggaran dasarnya telah -- mengalami beberapa kali perubahan dan telah disesuaikan dengan Undang-Undang Nomor 40 Tahun 2007 (duaribu tujuh) tentang Perseroan Terbatas, sebagaimana dimuat dalam akta tertanggal xx xxx xxxx (xx-xxx-xxxx) Nomor xx, yang dibuat dihadapan XXXXX, Sarjana Hukum, Notaris di Serang, dan telah mendapat persetujuan dari Menteri Hukum dan Hak Asasi Manusia Republik Indonesia dengan Surat -- Keputusannya tertanggal xx xxx xxxx Nomor: xxxxx, serta telah diterima dan dicatat di dalam database Sisminbakum Departemen Hukum dan Hak Asasi Manusia Republik Indonesia dengan Surat Penerimaan Pemberitahuan Perubahan Data Perseroan tertanggal xx xxx xxxx (xx-xxx-xxxx) Nomor xxxxx, kemudian diubah berturut-turut dengan:	According to his statement in this case is acting as the Director representing the Board of Directors of the company below and based on the power granted in the CIRCULAR RESOLUTION OF SHAREHOLDERS of Company XXXXX, domiciled in South Jakarta, the articles of association of which were amended several times and were adjusted to Law Number 40 of 2007 (two thousand and seven) on Limited Liability Company, as contained in the deed dated the xx day of xxx xxxx (xx-xxx- xxx) Number xx, created before XXXXX, Bachelor of Law, Notary of Serang, and obtained approval from the Minister of Law and Human Rights of the Republic of Indonesia as contained in the Decree dated the xx day of xxx xxxx (xx-xxx- xxx) Number: xxxxx, as well as were received and registered at the database of Administration System of Departement of Law and Human Rights of the Republic of Indonesia by the Receipt of Notice of the changes to the Articles of Association of Company dated the xx day of xxx xxxx (xx-xxx- xxx), Number xxxxx, were then amended consecutively by:
Akta tertanggal xx xxx xxxx -- (xx-xxx-xxxx) Nomor xx, yang telah diterima dan dicatat di dalam database Sistem Administrasi -- Badan Hukum Kementerian Hukum Dan Hak Asasi-Manusia Republik Indonesia dengan Surat -- Penerimaan Pemberitahuan Perubahan Data Perseroan tertanggal xx xxx xxxx (xx-xxx- xxxx) Nomor xxxxx dan Surat -- Penerimaan Pemberitahuan Perubahan Anggaran Dasar tertanggal xx xxx xxxx (xx-xxx- xxxx) Nomor: xxxxx;---	The deed dated the xx day of xxx xxxx (xx-xxx-xxx) Number xx, received and registered at the database of Legal Entity Administration System at the Ministry of Law and Human Rights of the Republic of Indonesia by the Receipt of Notice of the changes to Company's Data dated the xx day of xxx xxxx (xx-xxx- xxx), Number: xxxxx and the Receipt of Notice of the changes to the Articles of Association dated the xx day of xxx xxxx (xx-xxx- xxx), Number: xxxxx.
Akta-akta mana tersebut kelimanya dibuat dihadapan XXX, Sarjana Hukum, Notaris di Jakarta;	Such five deeds were created by XXX, Bachelor of Law, Notary in Jakarta;
Akta tertanggal xx xxx xxxx -- (xx-xxx-xxxx) Nomor: xx, yang merupakan ---- penegasan dari Akta tertanggal xx xxx xxxx -- (xx-xxx-xxxx) Nomor: xx, yang keduanya dibuatdihadapan XXX, -- Sarjana Hukum, Notaris di Jakarta Selatan, akta mana telah mendapat persetujuan	The deed dated xx xxx xxxx -- (xx-xxx-xxxx) Number xx, which was the affirmation of the Deed dated xx xxx xxxx -- (xx-xxx-xxxx) Number xx, both of which were created by XXXX, Bachelor of Law, Notary in South Jakarta, the Deed of which obtained approval from the

dari Menteri --- Hukum dan Hak Asasi Manusia Republik ---------- Indonesiadengan Surat Keputusannya tertanggal -- xx xxx xxxx -- (xx-xxx-xxxx), Nomor xxxx	Minister of Law and Human Rights of the Republic of Indonesia as contained in the Decree dated xx xxx xxxx -- (xx-xxx-xxxx), Number: xxxx;
Akta tertanggal xx xxx xxxx -- (xx-xxx-xxxx), Nomor xxx, dibuat------dihadapan XXX, Sarjana Hukum,-------Magister Kenotariatan, Notaris di Kota Tangerang Selatan, akta perubahan mana telah diterima dan dicatat dalam Database Sistem Administrasi Badan Hukum Kementerian Hukum dan Hak Asasi Manusia -- Republik Indonesia, sebagaimana ternyata dalam -- Surat Penerimaan Pemberitahuan Perubahan Data -- Perseroan tertanggal xx xxx xxxx -- (xx-xxx-xxxx), Nomor xxxx;	The deed dated xx xxx xxxx -- (xx-xxx-xxxx) Number xxx, created by XXX, Bachelor of Law, Master of Notary, Notary in South Tangerang City, received and registered at the database of Legal Entity Administration System at the Ministry of Law and Human Rights of the Republic of Indonesia by the Receipt of Notice of the changes to Company's Data dated xx xxx xxxx -- (xx-xxx-xxxx), Number: xxxx;
Sedangkan Susunan Direksi dan Dewan Komisaris -- yang terakhir termuat dalam akta tertanggal xx xxx xxxx -- (xx-xxx-xxxx), Nomor xxx, dibuat dihadapan saya, Notaris, akta mana telah mendapat pengesahan sebagaimana ternyata dalam Surat Keputusan menteri Hukum dan Hak Asasi Manusia Republik Indonesia tertanggal xx xxx xxxx -- (xx-xxx-xxxx) dan telah dicatat dalam Database Sistem Administrasi Badan Hukum Kementerian Hukum dan -- Hak Asasi Manusia Republik Indonesia, sebagaimana ternyata dalam Surat Penerimaan Pemberitahuan -- Perubaha Data Perseroan tertanggal xx xxx xxxx -- (xx-xxx-xxxx), Nomor xxx;	While the latest Composition of Board of Directors and Commissioners is contained in the deed dated xx xxx xxxx -- (xx-xxx-xxxx), Number xxx, created before me, Notary, the Deed of which obtained approval as contained in the Decree of the Minister of Law and Human Rights of the Republic of Indonesia dated xx xxx xxxx -- (xx-xxx-xxxx) and registered at the database of Legal Entity Administration System at the Ministry of Law and Human Rights of the Republic of Indonesia is contained in the Receipt of Notice of the changes to Company's Data dated xx xxx xxxx -- (xx-xxx-xxxx), Number: xxx;
Akta tertanggal xx xxx xxxx -- (xx-xxx-xxxx), Nomor xx, dibuat ---- dihadapan saya, Notaris, akta mana telah mendapat pengesahan sebagaimana ternyata dalam Surat----- Keputusan menteri Hukum dan Hak Asasi Manusia -- Republik Indonesia tertanggal xx xxx xxxx -- (xx-xxx-xxxx), Nomor xxxx;	The deed dated xx xxx xxxx -- (xx-xxx-xxxx) Number xx, created before me, Notary, the Deed of which obtained approval as contained in the Decree of the Minister of Law and Human Rights of the Republic of Indonesia dated xx xxx xxxx -- (xx-xxx-xxxx), Number: xxxx;
Akta tertanggal xx xxx xxxx -- (xx-xxx-xxxx), Nomor xx, dibuat --- dihadapan XXX, Sarjana Hukum, Magister Kenotariatan, Notaris di Tangerang, akta ------- perubahan mana telah diterima dan dicatat di----dalam Sistem Administrasi Badan Hukum Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia --	The deed dated xx xxx xxxx -- (xx-xxx-xxxx) Number xx, created before XXX, Bachelor of Law, Master of Notary, Notary in Tangerang, the deed of amendment of which was received and registered at the database of Legal Entity Administration System at the Ministry of Law and Human Rights of the Republic of Indonesia dated xx xxx xxxx -- (xx-xxx-xxxx), Number: xxx;

tertanggal xx xxx xxxx -- (xx-xxx-xxxx) Nomor xxx;	
akta tertanggal xx xxx xxxx -- (xx-xxx-xxxx), Nomor xxx, dibuat --- dihadapan XXX, Sarjana Hukum, Magister Kenotariatan, Notaris di Tangerang, akta ------- perubahan mana telah diterima dan dicatat di---- dalam Sistem Administrasi Badan Hukum Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia -- tertanggal xx xxx xxxx -- (xx-xxx-xxxx) Nomor xxx;	The deed dated xx xxx xxxx -- (xx-xxx-xxxx) Number xxx, created before XXX, Bachelor of Law, Master of Notary, Notary in Tangerang, the deed of amendment of which was received and registered at the database of Legal Entity Administration System at the Ministry of Law and Human Rights of the Republic of Indonesia dated xx xxx xxxx -- (xx-xxx-xxxx), Number: xxx;
Sedangkan anggran dasar terakhir termuat dalam -- Akta tertanggal xx xxx xxxx -- (xx-xxx-xxxx) Nomor xxx, dibuat --- dihadapan saya, Notaris, akta mana telah mendapat pengesahan sebagaimana ternyata dalam Surat----- Keputusan menteri Hukum dan Hak Asasxx xxx xxxx -- (xx-xxx-xxxx), Nomor xxx.	While the latest articles of association are contained in the Deed dated xx xxx xxxx -- (xx-xxx-xxxx) Number xxx, created before me, Notary, the deed of which obtained approval as contained in the Decree of the Minister of Law and Human Rights of the Republic of Indonesia dated xx xxx xxxx -- (xx-xxx-xxxx), Number: xxx;
Selaku Undangan Rapat;	As the Meeting Guest;
Bahwa telah hadir/diwakili dalam Rapat tersebut ---- sebanyak tujuh puluh lima ribu (75.000) saham yang merupakan seluruh saham yang hingga saat itu telah dikeluarkan oleh Perseroan, sehingga Rapat tersebut adalah sah susunannya dan dapat mengambil keputusan yang mengikat tentang semua hal yang dibicarakan --- walaupun tidak diadakan panggilan terlebih dahulu -- kepada para pemegang saham, satu dan lain hal sesuai dengan ketentuan yang tercantum dalam pasa 82 ayat 5 Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas.	That, the said meeting is attended/represented by seventy five thousand (75,000) shares which are the entire shares that have been issued by the Company up to this day, therefore the meeting is valid and can make binding decisions even though there was no preliminary invitation to the shareholders, one and other in accordance with the provisions contained in the Article 82 paragraph 5 of the Law 40 of 2007 on Limited Liability Company.
Bahwa saham-saham dari perseroan hingga saat ------ ini belum dicetak, akan tetapi Ketua Rapat ------ menerangkan menanggung dan menjamin tentang adanya pemilikan saham-saham seperti diuraikan diatas.	Whereas the shares of the company have not yet been issued, however, the Chairman of the Meeting explains that he bears and guarantees the ownership of the shares as described above.