ISOCENTER INDONESIA
The Ultimate ISO and Management System Resources

FROM CHAOS TO CONTROL:

Mastering Digital Governance in Modern Enterprises

AGENDA PEMBAHASAN:

1. Pengertian Dasar
2. Fakta-Fakta Mengejutkan akibat Lemahnya Tata Kelola Digital
3. Membangun Tata Kelola Digital yang “Fit for Purpose dan Berbasis Risiko”
4. Kesimpulan

ISOCENTER INDONESIA
The Ultimate ISO and Management System Resources.

Bagian I

Pengertian Dasar

Apa Itu Digital Governance?

Digital Governance adalah kerangka aturan, proses, dan struktur pengambilan keputusan yang mengarahkan penggunaan teknologi digital suatu organisasi—baik di sektor publik maupun swasta.

Tujuannya adalah untuk memberikan jaminan secara *reasonable* bahwa teknologi, data, dan layanan digital dipergunakan secara etis, aman, transparan, dan bertanggung jawab sesuai visi dan tujuan organisasi.

Referensi: https://www.numberanalytics.com/, https://ideas.repec.org/, https://fiveable.me/, https://digital.gov/, https://www.sciencedirect.com/, https://www.good-governance.org.uk/

Digital Governance vs IT Governance

Aspek	Digital Governance	IT Governance
Cakupan	Lebih luas: mencakup TI, IOT, data, AI, layanan digital, konten digital, media sosial, transformasi digital	Fokus pada sistem dan fungsi TI dalam organisasi
Tujuan	Menjamin tata kelola semua inisiatif digital (termasuk pengalaman pengguna, keterbukaan publik, transparansi digital, dan partisipasi)	Menjamin bahwa TI mendukung strategi bisnis dan digunakan secara efektif dan efisien
Fokus	Strategi digital, manajemen data, layanan digital, kebijakan teknologi, keamanan digital, AI ethics	Struktur organisasi, investasi TI, manajemen risiko TI, nilai bisnis dari TI
Stakeholder	Semua pihak terkait digital (IT, data, komunikasi, publik, pelanggan)	Umumnya pemangku kepentingan internal (IT, manajemen, board)
Contoh Isu	Pengelolaan situs web pemerintah, data terbuka, privasi pengguna, digital ethics	Pengelolaan infrastruktur TI, layanan cloud, IT project portfolio, compliance ISO/IEC 27001

Bagian II

Fakta-Fakta Mengejutkan akibat Lemahnya Tata Kelola Digital

Statistik Ancaman yang Menyebabkan Insiden Digital (2023-2024)

Ancaman	% Global	Kasus di Indonesia	Keterangan
Phishing & Social Engineering	36%	4.046 insiden (2023–2024)	Email/telpon palsu menipu pengguna agar menyerahkan kredensial atau klik link berbahaya
Ransomware	17%	130+ kasus (2023–2024)	Malware mengenkripsi sistem, minta tebusan untuk memulihkan data
Credential Theft	14%	Tidak dirinci spesifik	Pencurian username/password lewat keylogger, phishing, atau exploit login session
Data Leak (Exfiltration)	12%	~200 juta data Indonesia bocor (2023–2024)	Data diekspor tanpa izin akibat sistem tak aman atau insider threat
DDoS (Distributed Denial-of-Service)	8%	43.879 serangan (2023)	Serangan trafik besar ke server agar layanan lumpuh
Insider Threat (fraud SDM internal)	6%	Tidak dijabarkan rinci	Pegawai atau vendor yang lalai atau berniat buruk
Malware umum (non-ransomware)	3%	Banyak kasus UKM/SME	Perangkat lunak jahat: trojan, adware, backdoor tanpa enkripsi

Statistik Kelemahan yang Mengakibatkan Insiden Digital (2023–2024)

Kelemahan	Persentase/Angka	Penjelasan & Dampak
Pengabaian MFA	67 % dari insiden Q3 2024	Akses menggunakan kredensial valid tanpa MFA—via VPN, tidak aman
CVE yang tidak ditindaklanjuti	13 % dari insiden Q3 2024	Pemanfaatan celah umum seperti CVE-2024-3400 (Palo Alto), CVE-2020-14882 (WebLogic) yang tidak ditindaklanjuti berdampak kerentanan terbuka
Web app vulnerabilities	17 % dari serangan + 98 % aplikasi rentan	Banyak web app tidak aman—bug XSS, SQLi, config tidak aman.
Awareness yang lemah dari pengguna Email	75 % serangan mengekploitasi email (phishing)	Email phishing mendominasi awal serangan.
Anti-Malware yang kadaluarsa	81 % organisasi terkena malware/ransonware 2024	Trojans, backdoors, infostealer umum terjadi di kawasan Asia-Pasifik.
Kelemahan prosedural pengendalian internal	43 % breach global (internal threat)	Akses berlebihan, kecerobohan staf, tidak ada kontrol granular.
Kelemahan pengendalian vendor/pihak ketiga	54 % organisasi terpapar akibat kelemahan vendor/outsourcing	Kelemahan pada pihak ketiga jadi celah masuk serangan.
Cloud misconfigurations	17 % cyber serangan terhadap cloud	Konfigurasi keliru mempermudah exploit dan data exposure di cloud/public environments.
Rendahnya proteksi keamanan di Indonesia	Hanya 12 % organisasi siap hadapi ancaman maju	Mayoritas memiliki governance & proteksi siber yang belum matang.

Statistik Insiden yang Menggunakan AI

Waktu	Insiden	Modus Eksploit AI	Dampak utama & Penjelasan
Awal 2025	**Browser-based phishing via GenAI**	Impersonasi alat GenAI & zero-hour phishing	140% peningkatan serangan phishing pada browser vs 2023; 130% kenaikan zero-hour phishing
Okt-2024	**Deepfake & AI social engineering**	Deepfake & pesan AI disebarluaskan pada level regional	Serangan deepfake di Asia Tenggara naik +1.530% (2022–2023); AI-automated phishing meningkat tajam
Sep-24	**Deepfake-based voice scam (UK)**	AI-generated suara pimpinan perusahaan untuk influencer transfer dana	Perusahaan rugi USD 243.000 melalui instruksi palsu dari suara deepfake
Apr-24	**Change Healthcare (US)**	AI-driven automation membantu serangan – dapat exfiltrate data melalui login curian	Ransomware BlackCat, ~100 juta data pasien terekspos, tebusan USD 22 juta
Jan-24	**Snowflake (cloud provider)**	Eksfiltrasi cepat dideteksi lewat anomaly AI-monitored; AI-algoritma evasi	165 organisasi korban, termasuk Ticketmaster (560 juta pengguna); data terjual di dark web
2023–2024	**AI-driven phishing global**	Email/sms deep-personalized via NLP & ChatGPT generatif	Pesan phishing meningkat 202%, credential-phishing naik 703% di semester II 2024; >4.046 targeting Indonesia

Analisis Kelemahan Tata Kelola Digital (1)

Kelemahan Governance Digital	Akibat Langsung	Penjelaan
Pengabaian Multi-Factor Authentication (MFA)	Akses tidak sah via VPN, RDP, login session valid	Credential theft, ransomware, dan AI-driven login takeover (contoh: **Change Healthcare**)
Tidak ditindaklanjutinya CVE publik-known	Celah lama tetap terbuka meski diketahui secara publik	Eksploitasi zero-day & AI-driven reconnaissance tools memanfaatkan CVE (contoh: Palo Alto CVE-2024-3400, WebLogic CVE-2020-14882)
Cloud misconfiguration	Sistem cloud terbuka/exposed, tanpa enkripsi atau access control	Eksfiltrasi masif berbasis AI (contoh: **Snowflake**), serta DDoS cloud
Awareness & literasi pengguna rendah	Phishing berhasil, deepfake dipercaya sebagai realitas	AI-driven phishing (ChatGPT, NLP) berhasil mencuri kredensial; voice deepfake scam (**UK case**); 75% serangan eksploitasi email
Kelemahan kontrol vendor/pihak ketiga	Pintu masuk serangan dari vendor; minim due diligence	Banyak ransomware (termasuk **BSI**, PDN) disebabkan oleh integrasi sistem eksternal tanpa verifikasi kontrol keamanan

Analisis Kelemahan Tata Kelola Digital (2)

Kelemahan Governance Digital	Akibat Langsung	Penjelaan
Tidak adanya prosedur internal yang ketat (internal control)	Staf bisa lalai atau menyalahgunakan akses	Insider threat, exfiltration data sensitif secara manual, atau kolaborasi dengan aktor eksternal
Aplikasi web tidak aman (web vulnerability)	Bug seperti SQLi, XSS dimanfaatkan bot/AI crawler	AI bot dapat memindai dan mengeksploitasi web secara otomatis (zero-hour)
Anti-malware & proteksi usang	Sistem tidak mengenali ancaman modern (AI-generated malware, infostealer)	Terutama di organisasi dengan endpoint yang tidak dikelola secara proaktif
Ketiadaan governance khusus untuk penggunaan AI	AI dapat digunakan bebas tanpa kendali, termasuk oleh penyerang	**Deepfake**, **ChatGPT-phishing**, dan **AI-as-a-Service** makin marak, tanpa regulasi, deteksi, atau pelatihan untuk menghadapinya
Tidak adanya backup, DRP, dan response plan	Setelah serangan (seperti ransomware), pemulihan gagal atau memakan waktu lama	Kasus **PDN Surabaya**, **BSI**, dll — serangan LockBit atau BlackCat menyebabkan downtime hari-hari karena tidak ada rencana pemulihan

Bagian III

Membangun Tata Kelola Digital yang “Fit for Purpose dan Berbasis Risiko”

Beberapa Framework Acuan (1)

No	Framework / Standar	Diterbitkan Oleh	Cakupan Relevan	Keterangan
1	**ISO/IEC 38500**	ISO	IT & Digital Governance	Kerangka tata kelola TI pada tingkat eksekutif; fondasi umum untuk digital governance
2	**COBIT 2019**	ISACA	IT Governance & Management	Framework komprehensif untuk tata kelola dan manajemen TI yang juga relevan untuk digital enterprise
3	**Digital Nations Charter**	Digital Nations (OECD, dsb)	E-Government & Public Digital Services	Prinsip global untuk tata kelola digital di sektor pemerintahan
4	**TOGAF** (The Open Group Architecture Framework)	The Open Group	Enterprise Architecture	Menyediakan kerangka arsitektur TI & digital sebagai dasar tata kelola transformasi digital
5	**ITIL 4**	AXELOS	IT Service Management	Praktik terbaik untuk pengelolaan layanan digital (IT services) dalam konteks governance
6	**UN E-Government Development Index (EGDI)**	United Nations (UNDESA)	Digital Governance Pemerintah	Indeks dan panduan pengembangan tata kelola digital di sektor publik

Beberapa Framework Acuan (2)

No	Framework / Standar	Diterbitkan Oleh	Cakupan Relevan	Keterangan
7	**OECD Digital Government Framework**	OECD	Policy & Governance	Panduan kebijakan tata kelola digital sektor publik (transparansi, keterbukaan, partisipasi digital)
8	**World Bank Digital Government Framework**	World Bank	Digital Transformation Governance	Digunakan untuk mengembangkan kerangka kebijakan digital dan layanan publik digital
9	**NIST Digital Identity Guidelines**	NIST (US)	Identitas Digital & Keamanan	Standar untuk tata kelola identitas digital dan keamanan dalam platform digital
10	**AI Governance Framework (Model OECD)**	OECD	Tata Kelola AI	Sub-bagian dari digital governance yang fokus pada kebijakan dan tata kelola penggunaan AI
	ISO/IEC 27001	ISO	Keamanan Informasi	Kerangka tata kelola Keamanan Informasi

Tahapan Pembangunan Tata Kelola Digital: Risk Based Approach (1)

Tahapan	Mekanisme
1. Asesmen Risiko Digital	- Risiko Digital adalah ketidakpastian yang disebabkan dari interaksi/aktivitas digital yang berdampak terhadap pencapaian tujuan organisasi. - Asesmen risiko digital menggunakan metode yang didefinisikan di ERM (Enterprise Risk Mgt) organisasi (mis: berbasis ISO 31000). - Untuk identifikasi penyebab risiko dapat menggunakan kombinasi threat-vulnerability. - Bilamana diperlukan, disusun kriteria dampak Risiko Digital
2. Penentuan Risk Treatment Stratagy	- Petakan risk treatment sesuai domain tata kelola (mis: man, method, technology, atau bisa juga mengacu ke domain Annex A ISO 27001 seperti: organization, man, physical, technology) agar mudah. - Petakan domain2 tersebut ke framework praktik terbaik yang sesuai (mis: ISO 27001 klausul abc, COBIT 2019 objective abc, dst). Framework dapat redundan (lebih dari satu framework) untuk pengendalian satu risiko. Catatan: pemetaan ini seperti membangun SoA dalam penerapan ISO 27001. - Akhiri dengan risk treatment type sesuai pedoman ERM (mis: avoid, transfer, reduce, dsb.)

Tahapan Pembangunan Tata Kelola Digital: Risk Based Approach (2)

Tahapan	Mekanisme
3. Formulasi Risk Control (jika treatment type-nya adalah "reduce")	- Jika treatment type nya adalah "reduce", maka formulasikan control design sesuai dengan arahan yang tercantum di framework praktik terbaik. - Kaji implementasi control design, apakah menggunakan technologycal control, procedural control, atau hal lainnya, sesuai dengan cost-benefit analysis.
4. Implementasi kontrol	Bangun dan terapkan control (mis: membangun pedoman/kebijakan tata kelola digital, membangun sistem otomasi kontrol, membangun dan menerapkan prosedur pengendalian, dsb.)
5. Evaluasi Efektivitas Pengendalian	Menilai efektivitas penerapan kontrol (control design, control implementation, dsb.) sesuai dengan kaidah penilaian efektivitas pengendalian yang didefinsiikan dalam ERM organisasi
6. Continual Improvement	Meningkatkan efektivitas pengendalian secara berkelanjutan

Contoh Register Risiko Digital

No	Aktivitas Digital	Aset Digital yang Terdampak	Ancaman (Threat)	Kerentanan (Vulnerability)	Even Risiko	Dampak Risiko	Pemilik Risiko	Level Kemungkinan	Level Dampak	Level Risiko
R01	Pengiriman email eksternal	Sistem email & kredensial pengguna	Phishing & rekayasa sosial	Kurangnya pelatihan pengguna, tidak ada filter email cerdas	Pencurian kredensial, akses tidak sah	Kehilangan data, akses ke sistem internal	Divisi IT Governance	Tinggi	Ekstrem	Ekstrem
R02	Akses VPN dari luar kantor	Jaringan internal dan file server	Credential stuffing, brute force	Tidak ada MFA, password reuse	Akses tidak sah ke sistem internal	Eksfiltrasi data, sabotase sistem	Tim Infrastruktur	Sedang	Tinggi	Tinggi
R03	Hosting aplikasi publik (e.g. portal layanan)	Aplikasi web dan database	Exploit OWASP vulnerability (XSS, SQLi)	Kode tidak diuji, tidak ada web app firewall	Modifikasi data, downtime layanan	Kerugian reputasi, tuntutan hukum	Tim Pengembang Aplikasi	Tinggi	Tinggi	Tinggi
R04	Penggunaan layanan cloud pihak ketiga	Data pelanggan & transaksi	Data leak via cloud misconfigura-tion	Kurangnya pengaturan IAM dan proteksi data	Kebocoran massal data pelanggan	Denda regulator, kehilangan kepercayaan pelanggan	Tim Keamanan Data	Tinggi	Ekstrem	Ekstrem
R05	Penyimpanan log aktivitas pengguna	Log server & file tracking	Insider threat, log tampering	Tidak ada segregasi akses, tidak ada alert log	Hilangnya jejak audit, manipulasi data	Tidak terdeteksinya pelanggaran	Unit Audit Internal	Sedang	Tinggi	Tinggi

Contoh Penentuan Risk Treatment Strategy

No	Aktivitas Digital	Risk Treatment Strategy	Domain Tata Kelola	Framework Referensi (Klausal/Kontrol)
R01	Pengiriman email eksternal	**Reduce** – kontrol untuk mencegah dan mendeteksi	**Manusia (Awareness), Teknologi (Email Security)**	ISO/IEC 27001: A.6.1.2, A.12.2.1, COBIT: APO12, DSS05
R02	Akses VPN dari luar kantor	**Reduce** – kontrol teknis akses & autentikasi	**Teknologi, Prosedur, Identity & Access Governance**	ISO/IEC 27001: A.9.4.2, A.13.1.1, NIST SP 800-63B
R03	Hosting aplikasi publik (e.g. portal layanan)	**Reduce** – hardening aplikasi & proteksi perimeter	**Teknologi, Tata Kelola Aplikasi**	OWASP ASVS, ISO 27001: A.14.2.1, A.14.2.5, COBIT: DSS05
R04	Penggunaan layanan cloud pihak ketiga	**Reduce & Transfer** – kontrol cloud + SLA vendor	**Teknologi, Pihak Ketiga, Cloud Governance**	ISO 27017: 9.4, 11.1; ISO 27001: A.15; COBIT BAI03
R05	Penyimpanan log aktivitas pengguna	**Reduce** – kontrol akses, alerting log, segregasi	**Teknologi, Prosedur, Audit Governance**	ISO 27001: A.12.4, A.9.2.3, COBIT: MEA03, DSS06

Contoh Formulasi Risk Control

No	Aktivitas Digital	Risk Treatment Strategy	Control Teknis	Control Prosedural	Substansi Kebijakan (yang Akan Dituangkan dalam Pedoman)
R01	Pengiriman email eksternal	Reduce	- Implementasi Email Security Gateway (spam & link scanner) - Anti-phishing AI-based filter - DMARC/DKIM/SPF enforcement	- SOP pelaporan email mencurigakan - Simulasi phishing berkala	- Kebijakan keamanan email & komunikasi eksternal - Penunjukan data protection officer
R02	Akses VPN dari luar kantor	Reduce	- MFA (Multi-Factor Authentication) - Password policy enforcement - VPN client dengan endpoint protection	- SOP otorisasi akses jarak jauh - Log dan review aktivitas VPN	- Kebijakan akses jarak jauh & BYOD - Review akses berkala (access recertification)
R03	Hosting aplikasi publik	Reduce	- Web Application Firewall (WAF) - Input validation & secure coding - SSL/TLS enforced with HSTS	- Change management untuk aplikasi web - Prosedur uji keamanan aplikasi (pentest/DAST)	- Kebijakan pengembangan aplikasi aman (secure SDLC) - Penunjukan roles dalam AppSec
R04	Penggunaan cloud pihak ketiga	Reduce + Transfer	- IAM granular di cloud (role-based access) - Enkripsi data at rest & in transit - CASB (Cloud Access Security Broker)	- Prosedur onboarding vendor dan review SLA - Checklist pengamanan cloud	- Kebijakan cloud governance & vendor management - Kontrak SLA dengan kewajiban keamanan
R05	Penyimpanan log aktivitas pengguna	Reduce	- Log tamper protection (SIEM/Syslog immutability) - Alert untuk aktivitas abnormal - Segregasi hak akses log	- SOP pemantauan dan review log - Prosedur pelaporan anomali	- Kebijakan log management dan retensi log - Penanggung jawab pemantauan log

Contoh Isi Pedoman Tata Kelola Digital (yang Diturunkan dari Langkah no 3 – Formulasi Risk Control) (1)

📘 Pedoman Tata Kelola Digital – Struktur dan Isi

I. Pendahuluan

1. **Latar Belakang**
   - Penjelasan tentang pentingnya tata kelola digital dalam mendukung tujuan organisasi.
2. **Tujuan Pedoman**
   - Memberikan arahan pengelolaan aktivitas digital secara aman, terkendali, dan terukur.
3. **Ruang Lingkup**
   - Mencakup seluruh aktivitas digital: email, akses jarak jauh, aplikasi publik, cloud, log.
4. **Dasar Hukum & Referensi**
   - ISO/IEC 27001, ISO 38500, COBIT 2019, NIST CSF, UU PDP (jika di Indonesia), OWASP, dsb.

Contoh Isi Pedoman Tata Kelola Digital (yang Diturunkan dari Langkah no 3 – Formulasi Risk Control) (2)

II. Prinsip-Prinsip Tata Kelola Digital

1. **Akuntabilitas** – Kejelasan peran dan tanggung jawab tata kelola sistem digital.
2. **Transparansi** – Pelaporan dan pelacakan aktivitas digital dilakukan terbuka dan auditabel.
3. **Kepatuhan** – Selaras dengan regulasi internal maupun eksternal.
4. **Pengelolaan Risiko Digital** – Berbasis risk-informed decision making.
5. **Kepemilikan Aset Digital** – Penunjukan data owner, system owner, log owner, dsb.

Contoh Isi Pedoman Tata Kelola Digital (yang Diturunkan dari Langkah no 3 – Formulasi Risk Control) (3)

III. Organisasi Tata Kelola Digital

1. **Struktur Tata Kelola Digital**
   - Dewan atau Komite Keamanan Informasi / Digital Governance Committee.
   - Fungsi operasional: IT Security, Data Protection Officer, Pemilik Proses, dll.
2. **Peran & Tanggung Jawab**
   - Rinci per stakeholder: manajemen, IT, audit, pengguna, vendor.
3. **Rantai Eskalasi & Komunikasi**
   - Alur pelaporan insiden, pelanggaran, dan eskalasi keamanan digital.

Contoh Isi Pedoman Tata Kelola Digital (yang Diturunkan dari Langkah no 3 – Formulasi Risk Control) (4)

IV. Domain Kebijakan dan Kontrol Tata Kelola Digital

1. Pengelolaan Email & Komunikasi Digital

- Semua komunikasi eksternal harus melalui kanal resmi.
- Email harus melalui filtering: spam, virus, phishing detection.
- Kebijakan penggunaan tanda tangan digital dan enkripsi jika diperlukan.
- Simulasi phishing minimal 2x setahun.

2. Akses Jarak Jauh & Autentikasi

- Semua akses VPN/WFH wajib MFA.
- Tidak boleh menggunakan password default.
- Akses bersifat role-based dan dievaluasi setiap 6 bulan.
- BYOD (Bring Your Own Device) tunduk pada standar keamanan perangkat.

Contoh Isi Pedoman Tata Kelola Digital (yang Diturunkan dari Langkah no 3 – Formulasi Risk Control) (5)

3. Pengembangan dan Hosting Aplikasi Publik

- Semua aplikasi wajib mengikuti secure SDLC.
- Aplikasi diuji keamanan (pentest) minimal sekali sebelum go-live.
- Wajib gunakan WAF, SSL/TLS, dan konfigurasi minimal bug OWASP Top 10.

4. Tata Kelola Penggunaan Cloud dan Vendor

- Cloud provider harus memenuhi standar ISO 27017/27018.
- Semua layanan cloud tunduk pada SLA dengan klausul keamanan & retensi data.
- Data penting wajib dienkripsi dan tidak boleh disimpan secara publik default.

5. Pengelolaan Log dan Monitoring Aktivitas

- Semua aktivitas sistem yang berdampak keamanan/logic harus dicatat.
- Log harus disimpan minimal 1 tahun dan tidak boleh dimodifikasi.
- Pemantauan dilakukan oleh pihak independen atau sistem SIEM.

Contoh Isi Pedoman Tata Kelola Digital (yang Diturunkan dari Langkah no 3 – Formulasi Risk Control) (6)

V. Mekanisme Evaluasi dan Review

1. **Audit Tata Kelola Digital** – Internal audit berkala dan audit kontrol teknis.
2. **Kaji Ulang Kebijakan** – Pedoman ini direview setiap tahun atau bila terjadi insiden besar.
3. **Pelaporan Kinerja & Efektivitas Kontrol** – Mengacu ke KRI (Key Risk Indicator) dan KCI.

VI. Penutup

1. **Sanksi dan Kepatuhan** – Pelanggaran terhadap pedoman dikenakan tindakan sesuai peraturan organisasi.
2. **Penetapan dan Tanggal Berlaku** – Disahkan oleh Top Management / Direktur terkait.

ISOCENTER INDONESIA
The Ultimate ISO and Management System Resources.

Bagian VI

Kesimpulan

Kesimpulan

- Pembangunan dan Penerapan Tata Kelola Digital (Digital Governance) **sudah menjadi keniscayaan di organisasi modern yang semakin terpapar risiko digital.**
- Digital Governance adalah perluasan dari IT Governance, **yang fokusnya bukan hanya penyelarasan antara bisnis dengan IT tetapi juga memberikan jaminan yang *reasonable* bahwa teknologi, data, dan layanan digital dipergunakan secara etis, aman, transparan, dan bertanggung jawab.**
- Pembangunan Digital Governance **dapat dilakukan berbasis risiko,**

About Us

ISO CENTER INDONESIA adalah penyedia layanan terkait ISO dan Sistem Manajemen yang komprehensif. Kami adalah The Ultimate ISO and Management System Resources yang siap meningkatkan kinerja organisasi Anda melalui penyediaan informasi, pelatihan, implementasi, dan asesmen standar internasional berbasis ISO dan sistem manajemen yang efektif, efisien, out of the box, dan menggunakan metode terkini yang di-enable oleh teknologi dan AI.Jangan lupa untuk selalu kunjungi situs kami dan mengakses tautan Articles yang memuat kajian-kajian terkini kami dan Download yang berisi video-video pembalajaran, e-book hasil riset kami, dan alat-alat bantu yang berupa kertas-kertas kerja dan template yang selau kami kinikan.

Semua itu kami persembahkan untuk Anda!

ISOCENTER INDONESIA

Thank You!

ISO Center Indonesia (Jakarta)

Permata Kuningan Building
17th Floor, HR Rasuna Said.
Kuningan Mulia, Menteng Atas,
Setia Budi, South Jakarta City,
Jakarta 12920

East Office (Surabaya)

AMG Tower Lantai 17,
Jl. Raya Dukuh Menanggal
No 1A, East Java, Gayungan
Surabaya, Indonesia 60234

Contact Us :

Website : https://isoindonesiacenter.com/
email : admin@isoindonesiacenter.com
telepon : +62 813-184-5942 (Sinthia - WhatsApp/Call)
+62 895-2956-5008 (Louqman – WhatsApp/Call)
+62 89-6551-88175 (Ardi - WhatsApp/Call)

ISOCENTER INDONESIA