

gaskita
Juaranya Gas Ngalir Terus

by **PGN**



PLN

Konferensi Auditor Internal **GOVERNANCE 5.0** Redefining Board Oversight and Internal Audit in a Digital-First Era



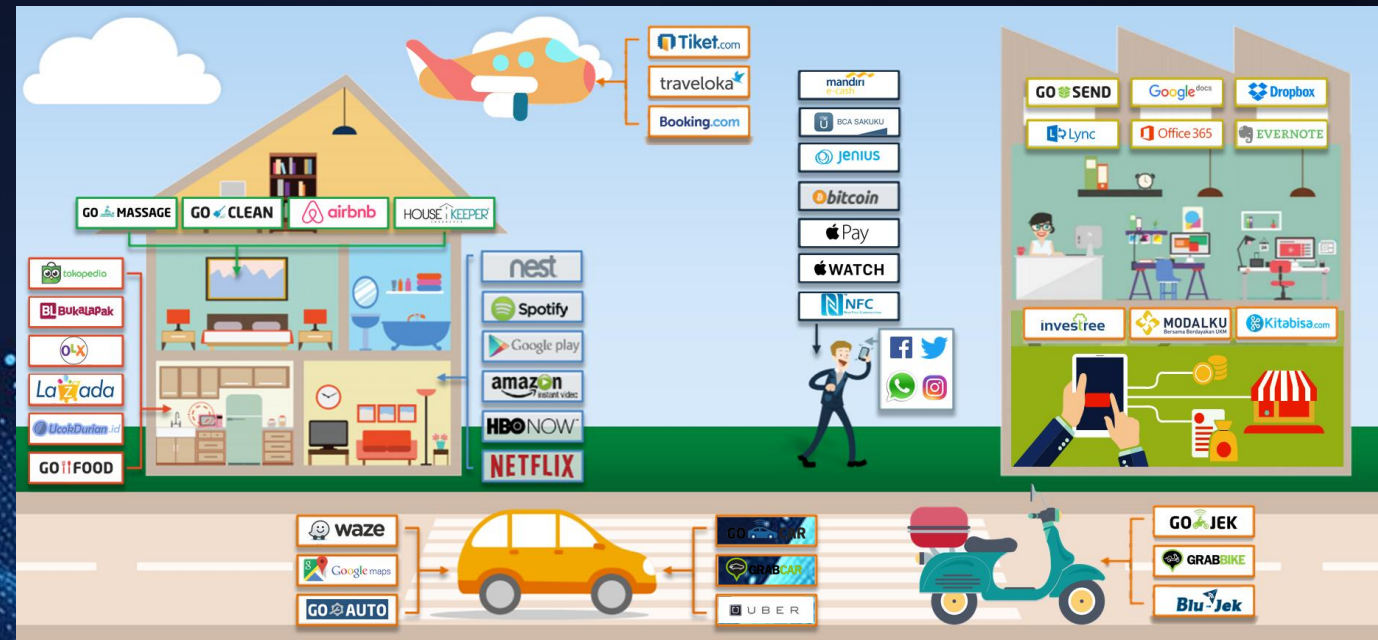


Building Digital Trust In the Hyperconnected World

Jogyakarta, 9 Juli 2026

Dr. Eng. Hary Budiarto MKom. QGIA
Pusat Pengembangan Aparatur Komdigi
BPSDM Komdigi - Kementerian Komunikasi dan Digital

> Ruang Digital Global



Disinformasi adalah suatu informasi yang dengan sengaja dirancang untuk menyebabkan kerugian.

Disinformasi

Malinformasi adalah informasi asli atau benar, namun penyebarannya dimaksudkan untuk menyebabkan kerugian bagi pihak tertentu.

Malinformasi

Misinformasi adalah informasi atau berita palsu yang beredar, namun orang yang berbagi tidak menyadarinya bahwa itu salah atau menyesatkan.

Misinformasi



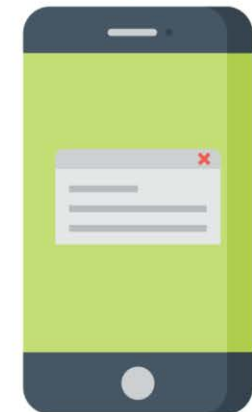
Radikalisme

Hate speech

#HATE

#BULLY

Cyber bullying



Penipuan online



Pornografi

TANTANGAN DUNIA HYPERCONNECTED



Dampak Utama:

Kehilangan Data

Penurunan Kepercayaan

Kerugian Reputasi

Kerugian Finansial

WASPADA KEJAHATAN SIBER CARDING

Kejahatan siber berupa penyalahgunaan nomor dan kartu kredit/debit orang lain atau *carding* menjadi salah satu ancaman dalam perkembangan layanan digital perbankan. Literasi digital dan kewaspadaan nasabah diperlukan untuk mencegah terjadinya *carding*.

WAJAHMU BISA DIPALSUKAN!

ANCAMAN DEEPFAKE AI YANG MENGINTAI



MODUS BARU DI ERA DIGITAL

AI dapat memanipulasi foto atau video seseorang hingga tampak nyata untuk menyebarkan konten intim tanpa persetujuan. Ini termasuk Kekerasan Berbasis Gender dan diatur dalam UU No. 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual.

Tekanan Psikologis

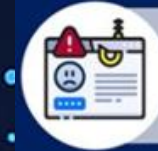
Jaga Privasi & Waspada

Tingkatkan Literasi Keamanan

MODUS



Penyalahgunaan kartu tanpa disadari pemilik.



Wiretapping atau penyadapan untuk memperoleh informasi pribadi pemilik kartu.



Phishing dengan cara mengirim tautan laman internet palsu.



Counterfeiting atau penggunaan kartu palsu yang dibuat mirip dengan kartu asli.

Bank

70%

Perusahaan asuransi

16%

Sektor keuangan lainnya

14%

➤ Mengapa diperlukan Digital Trust ?



- In a world defined by hyper-connectivity, cybersecurity has become central to trust, resilience, and digital continuity.
- As cyber threats grow more complex, pervasive, and increasingly invisible, preparing the next generation to be cyber-ready is no longer optional, it is imperative.
- How applied, industry-linked cybersecurity education, grounded in real-world threat detection, risk mitigation, and responsible digital innovation, is critical to securing the future.

➤ Pengertian Digital Trust

DIGITAL TRUST

Fondasi Ekonomi & Ekosistem Digital Modern



PENTINGNYA DIGITAL TRUST:

E-Commerce & Fintech



Inovasi Teknologi



Keamanan Ekosistem



Kepercayaan Pengguna



Digital Trust adalah kepercayaan masyarakat terhadap keamanan, privasi, dan integritas teknologi digital yang meliputi keyakinan pada perlindungan data pribadi, sistem yang bekerja secara transparan, dan layanan digital yang dapat diandalkan.

Digital Trust sebagai Fondasi Ekonomi & Ekosistem Digital Modern :

- E-commerce & Fintech: Mendorong transaksi online yang aman.
- Inovasi Teknologi: Memacu pengembangan solusi baru berbasis data.
- Keamanan Ekosistem: Melindungi ekonomi digital dari ancaman siber.
- Kepercayaan Pengguna: Meningkatkan loyalitas dan adopsi layanan digital.

➤ Framework Membangun Building Digital Trust (1)



Pilar	Makna	Contoh Implementasi
Security and Reliability – sistem harus aman dan konsisten.		
Safety (Keamanan)	Menjamin keselamatan pengguna dalam interaksi digital.	Perlindungan dari konten berbahaya, keamanan transaksi online.
Cybersecurity (Keamanan Siber)	Perlindungan sistem dari ancaman digital seperti malware dan serangan Siber.	Firewall, deteksi intrusi, autentikasi multi faktor.
Privacy (Privasi)	Perlindungan data pribadi pengguna dari akses tidak sah.	Kebijakan privasi yang jelas, enkripsi data, kontrol akses pengguna.
Accountability and Oversight – ada tanggung jawab dan pengawasan yang jelas.		
Transparency (Transparansi)	Keterbukaan dalam kebijakan, proses, dan penggunaan data.	Laporan publik, penjelasan algoritma, komunikasi terbuka.
Redressability (Pemulihan Hak)	Mekanisme untuk memperbaiki kesalahan atau pelanggaran.	Prosedur pengaduan, kompensasi atas pelanggaran data.
Auditability (Auditabilitas)	Kemampuan untuk meninjau dan memverifikasi proses digital.	Log aktivitas, audit keamanan, pelaporan transparan.
Inclusive, Ethical, and Responsible Use – teknologi digunakan secara inklusif, etis, dan bertanggung jawab.		
Fairness (Keadilan)	Perlakuan yang adil dan tidak diskriminatif dalam sistem digital.	Algoritma tanpa bias, akses setara terhadap layanan digital.
Interoperability (Interoperabilitas)	Kemampuan sistem berbeda untuk bekerja sama secara efisien.	Standar terbuka, API yang kompatibel antar platform.

➤ Framework Membangun Building Digital Trust (2)



Komponen	Penjelasan	Contoh Implementasi
Governance (Tata Kelola)	Menetapkan kebijakan, struktur, dan tanggung jawab untuk mengelola risiko dan keamanan digital.	Framework GRC (Governance, Risk, Compliance), kebijakan keamanan informasi.
Application Security (Keamanan Aplikasi)	Melindungi aplikasi dari kerentanan dan serangan siber.	Pengujian keamanan aplikasi, patching, secure coding.
Data Security & Privacy (Keamanan dan Privasi Data)	Menjamin perlindungan data pribadi dan sensitif dari akses tidak sah.	Enkripsi, kontrol akses, kebijakan privasi.
Risk Management (Manajemen Risiko)	Mengidentifikasi, menilai, dan memitigasi risiko digital.	Analisis risiko, penilaian dampak, rencana mitigasi.
Vulnerability Management (Manajemen Kerentanan)	Mengelola dan memperbaiki kelemahan sistem sebelum dimanfaatkan oleh pihak berbahaya.	Pemindaian kerentanan, patch management.
Threat Management (Manajemen Ancaman)	Mendeteksi dan merespons ancaman siber secara proaktif.	Threat intelligence, SOC (Security Operations Center).
Compliance (Kepatuhan)	Memastikan organisasi mematuhi regulasi dan standar keamanan.	ISO 27001, GDPR, UU Perlindungan Data Pribadi.
Audit Readiness (Kesiapan Audit)	Menyiapkan bukti dan dokumentasi untuk memastikan transparansi dan akuntabilitas.	Audit trail, laporan keamanan, kontrol internal.

Enterprise Architecture: Integrating Strategy, Business, and Technology



IT Governance

➤ Strategi Organisasi untuk Digital Trust



Transparansi adalah Organisasi harus memastikan bahwa setiap proses digital dapat dipahami dan diawasi oleh pengguna maupun regulator antara lain :

- Menyusun kebijakan privasi yang jelas dan mudah diakses.
- Menyampaikan cara pengumpulan, penggunaan, dan penyimpanan data secara terbuka.
- Melakukan audit berkala dan mempublikasikan hasilnya untuk menunjukkan akuntabilitas.
- Menggunakan teknologi seperti blockchain untuk mencatat transaksi secara transparan dan tidak dapat diubah.

➤ Strategi Organisasi untuk Digital Trust

Keamanan adalah organisasi perlu melindungi sistem dan data dari ancaman eksternal maupun internal antara lain:

- Menerapkan enkripsi end-to-end dan autentikasi multifaktor.
- Menggunakan sistem deteksi ancaman berbasis AI untuk memantau aktivitas mencurigakan.
- Melatih karyawan tentang keamanan siber dan kebijakan penggunaan data.
- Menyusun rencana pemulihan bencana (disaster recovery plan) untuk menjaga kontinuitas layanan.

Integritas adalah memastikan bahwa sistem digital beroperasi sesuai tujuan tanpa manipulasi atau kesalahan antara lain:

- Melakukan penetration testing dan vulnerability assessment secara rutin.
- Menjaga keaslian data melalui kontrol akses dan verifikasi identitas.
- Mengimplementasikan sistem audit internal untuk mendeteksi anomali.
- Menetapkan standar etika dan tata kelola teknologi agar keputusan digital tetap adil dan akuntabel.

Kolaborasi Pemangku Kepentingan

EKOSISTEM DIGITAL TERPERCAYA



**Building Trust
and Credibility
in a Digital World**

Terima Kasih

KEMENTERIAN
KOMDIGI

Gedung Kementerian Komdigi
Jl. Medan Merdeka Barat No. 9,
Jakarta, 10110



www.kominfo.go.id



Kemkomdigi TV



Kementerian Komunikasi dan Digital RI



@kemkomdigi



@kemkominfo