E-MATERI

YAYASAN PENDIDIKAN INTERNAL AUDIT

Konferensi Auditor Internal

BUILDING RESILIENCE IN TUNA WORLD:

"Control Your Future or Someone Else Will"

HOTEL TENTREM YOGYAKARTA

5-6 JULI 2023

KONFERENSI & WISUDA YPIA

PERTAMINA

PLN mobile

PLN

BRI

vedapraxis

Secure Digital Transformation toward Borderless Society

Syahraki Syahrir (RAKI), CISA, CISM, CDPSE, GRCP

CEO & Partner Veda Praxis

President ISACA Indonesia Chapter

July 2023

Disiapkan untuk:

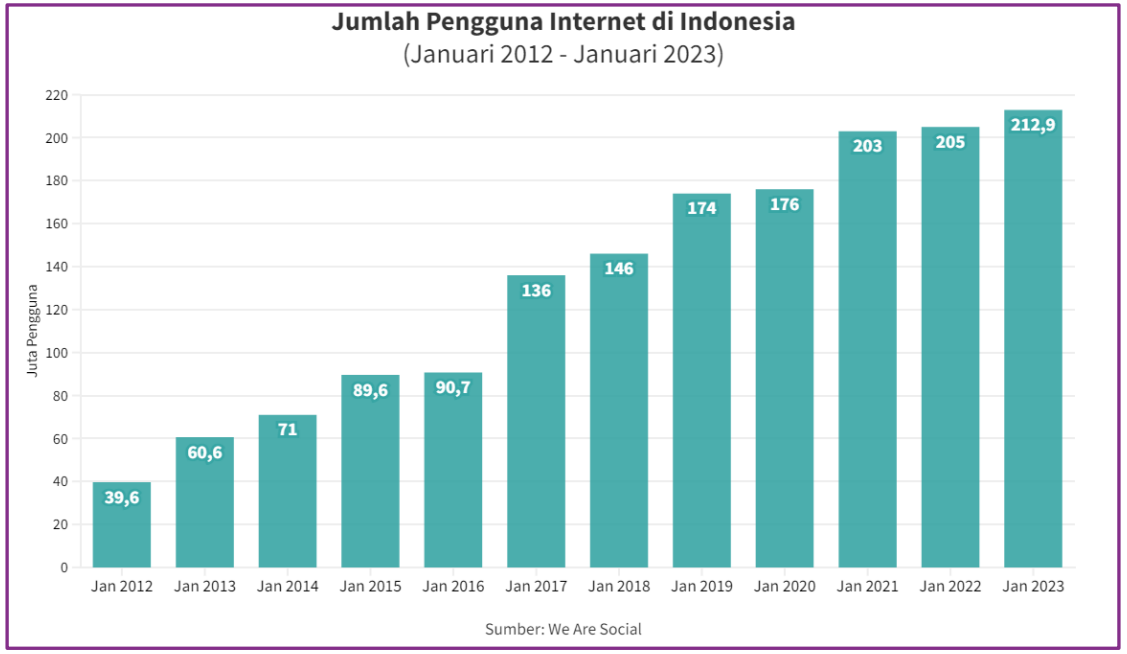
YAYASAN PENDIDIKAN INTERNAL AUDIT

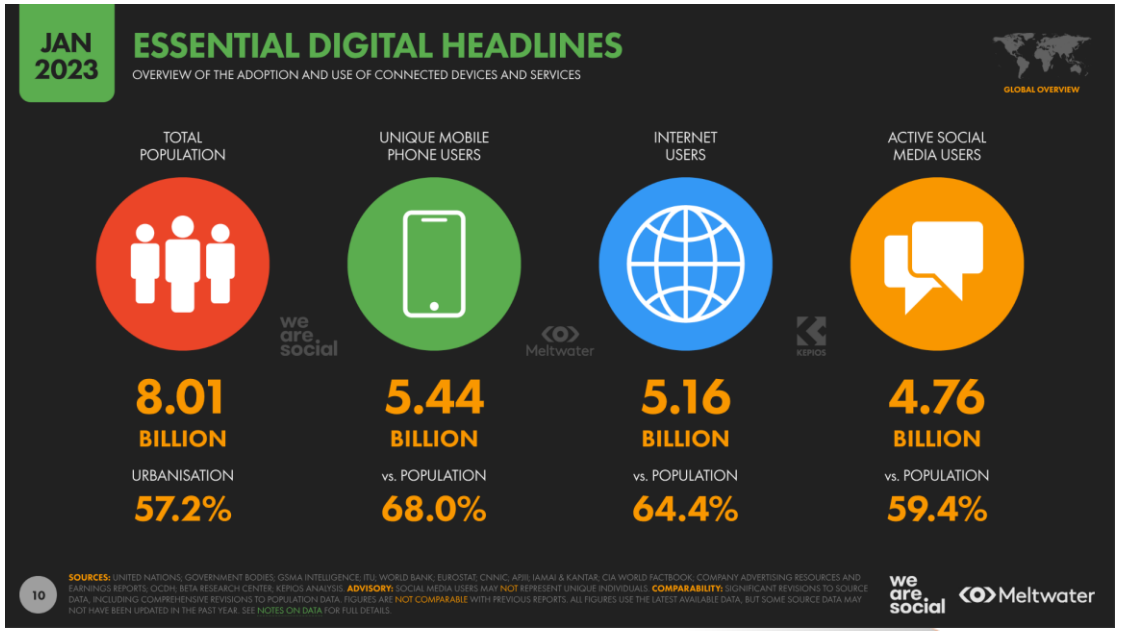
PENGGUNA INTERNET DI INDONESIA 2023 CAPAI 212 JUTA!

Berdasarkan laporan We Are Social, jumlah pengguna internet di Indonesia telah mencapai **212,9 juta** dari total 277,43 juta jiwa pada Januari 2023. Ini berarti sekitar **77% dari populasi** Indonesia telah menggunakan internet.

Melihat trennya, jumlah pengguna internet di Indonesia terus tumbuh setiap tahun. Adapun, lonjakan pengguna internet di dalam negeri terjadi pada 2017 & 2019 (Covid-19).

Lebih lanjut, rata-rata orang Indonesia menggunakan internet selama **7 jam 42 menit setiap harinya**. Selain itu, 98,3% pengguna internet di Indonesia menggunakan telepon genggam (HP).





Cross Border Data Transfer

Cross-border data transfer is simply the sharing of personal data from one national jurisdiction to another. Cross-border data transfer has been one of the most challenging aspects of data protection, particularly for international corporations.

"Adequate" Data Protection Practices.

The European Economic Area apply EU data protection rules: **When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data**.

The Need for Trusted Data Flows (DFFT)

Today's global digital economy is fueled by data. Any action taken in the **digital economy**, whether it be buying a good, selling a service, or accessing a piece of information, **requires** the **creation** and **transfer of data**—and **lots** of it

Government of Indonesia has issued Government Regulation (GR) **regarding Implementation of Electronic System and Transaction regulates the implementation of electronic system, electronic agent, electronic transaction, electronic certification, reliability certification institutions as well as domain name management**.

The Digital Economy Working Group **(DEWG)** was initiated by Indonesia and other G20 countries **on how to take advantage of digital technology, through exchanging information and views, and seeking a common understanding on policies, which encourage a resilient digital economy, and develop in a sustainable and inclusive manner, with an environment digital services that are safe, secure, and connected, while mitigating the challenges and risks of digitalisation.**

Bank Indonesia has also conducted a **QR Cross-border trial** with **Malaysia** and **Thailand** which enables consumers and merchants in both countries **to make** and **receive payments for goods and services via the QR Code. QR Cross-border** has an important role to play in increasing **transaction efficiency, supporting the digitization of trade and investment, and maintaining macroeconomic stability** by expanding the use of local currency (LCS) transaction settlements.

Risiko Cyber pada Cross-Border Financial Services

Digital innovations for cross-border are creating new risks, especially concerning cybersecurity

Cyber attack against Banco de Chile in 2018 destroyed 9,000 workstations and 500 servers, as well as compromising endpoint handling transactions on the SWIFT network.

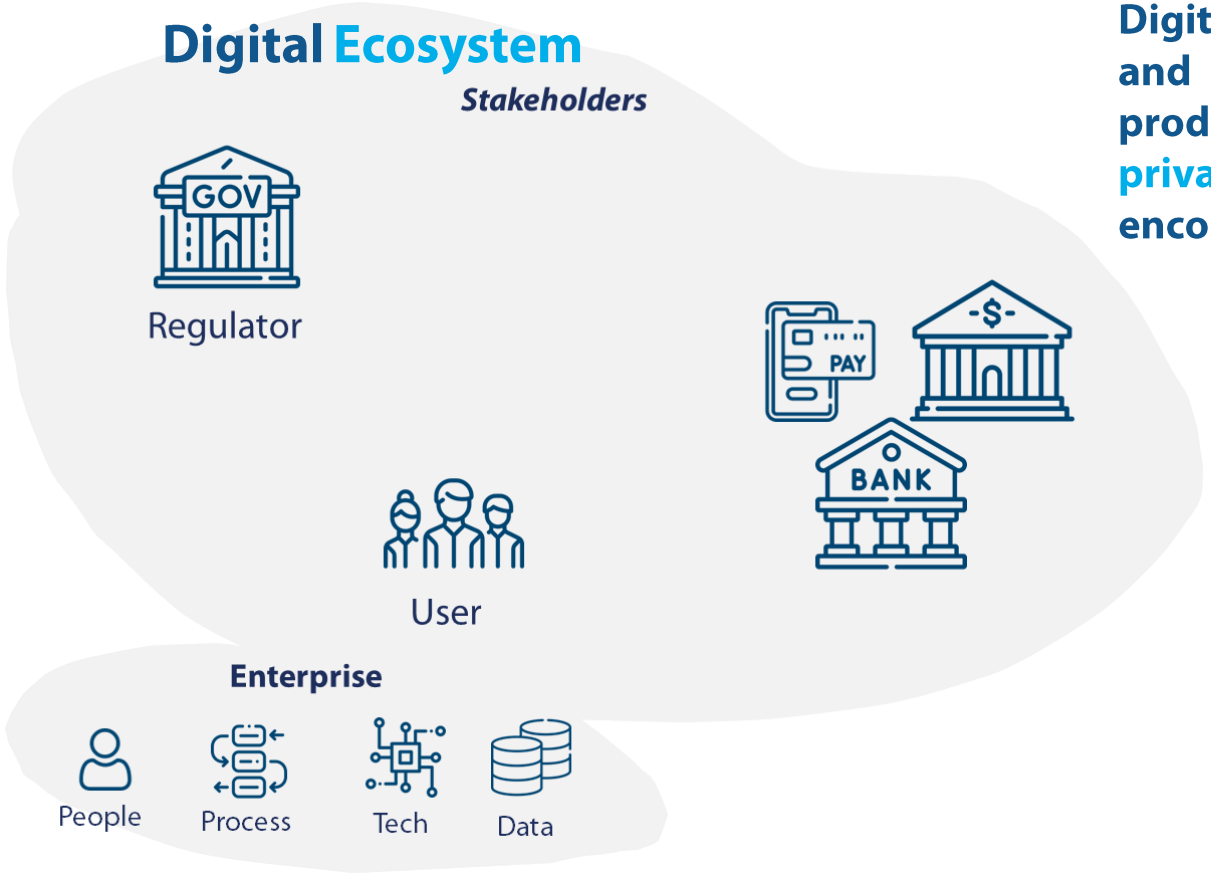
The actions of the cybercriminals that breached the Russian Regional Bank resulted in the enormous fluctuations of the ruble-dollar exchange rate in 2015

Hackers can use the cross-border "messaging" system to send false transactions.
In the 2016 Bangladesh central bank heist, and breached the bank's network to send fraudulent transfer requests through the SWIFT network, resulting in $81 million of direct losses.

"The increasing use of these technologies, though, should be coupled with a strengthening of regulatory oversight over financial activities to safeguard financial stability, as new risks may surface […] Financial digitalization trends heighten the need for cybersecurity to protect financial consumers and producers ", **highlighted** by the IMF report submitted to G20 in 2018 (IMF, 2018)

Digital Trust

Digital Trust is the confidence in the integrity of the relationships, interactions and transactions among providers and consumers within an associated digital ecosystem. This includes the ability of people, organizations, processes, information and technology to create and maintain a trustworthy digital world.



Digital trust is the basis of the relationship between a provider and an end-user that gives the user confidence that the product or service is honest, safe, effective, reliable, secure, private and transparent. Digital trust must be all-encompassing for all organizations

Digital Trust Ecosystem: Why an Ecosystem?

1. **Enterprises don't operate in a vacuum**
2. **Dependence on third-party goods and services**
3. **Key stakeholders in the ecosystem:**
   - **Service/Product/Information provider**
   - **Service/Product/Information consumer**
   - **Third-party Service/Product/Information providers**
   - **Proxy technology**
   - **Digital peers**

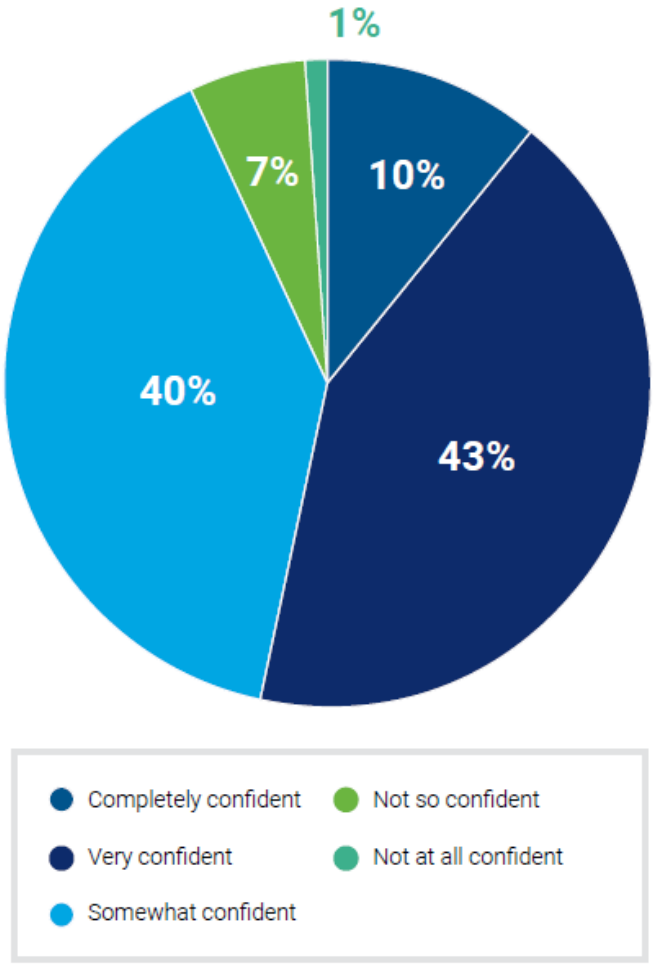
Source: ISACA

KEY FACTORS THAT CONTRIBUTE TO DIGITAL TRUST INCLUDE:

- **Quality:** Assure products and services meet or exceed expectations.
- **Availability:** Enable access to information and services in a timely manner.
- **Security and privacy:** Ensure all data are protected and kept confidential.
- **Ethics and integrity:** Live up to all promises.
- **Transparency and honesty:** Be truthful in how information is used and if it is compromised.
- **Resiliency:** Take steps to ensure organizational stability and agility.

FIGURE 4 – Digital Trustworthiness of Organizations

How confident are you in the digital trustworthiness of your organization?

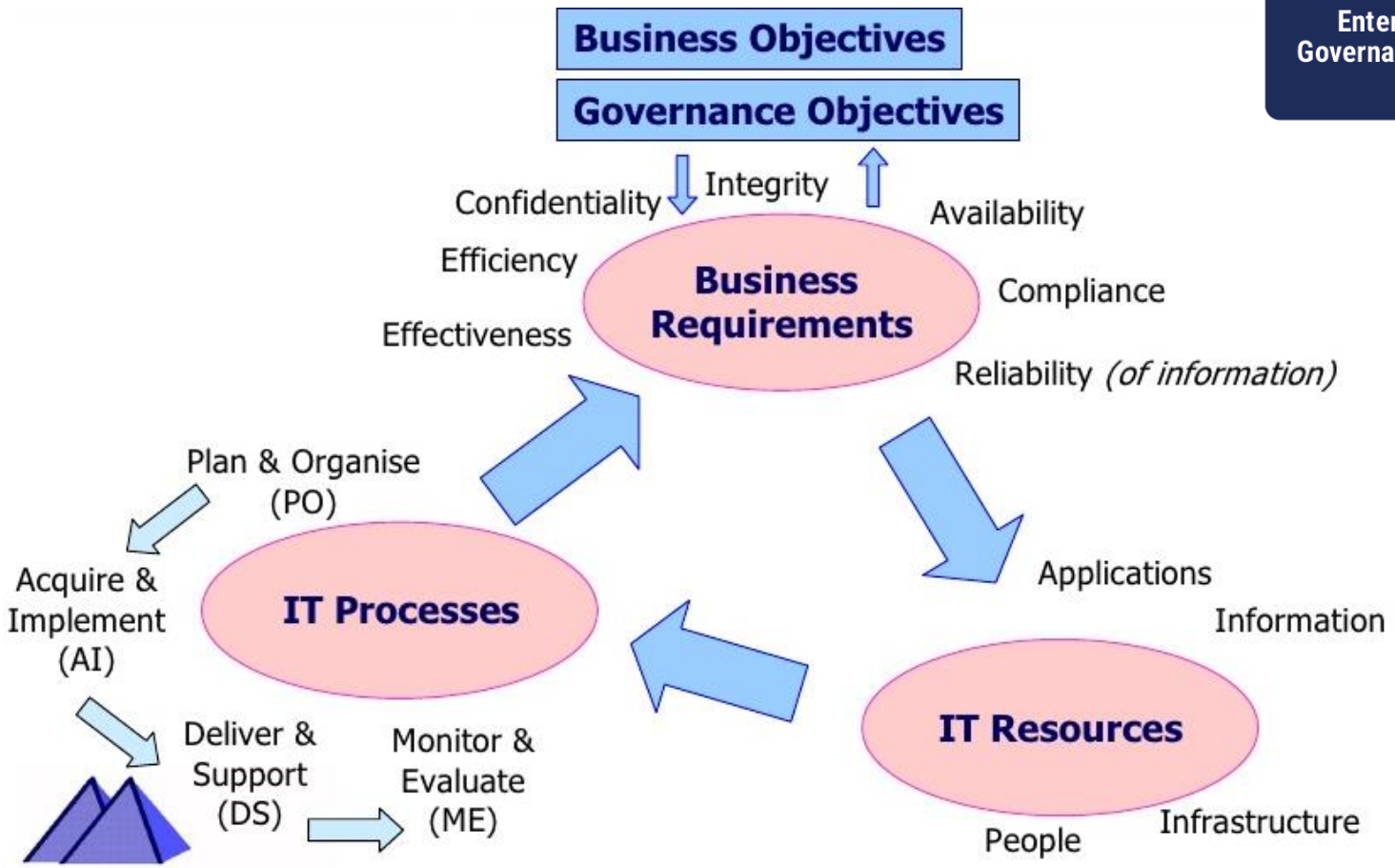


Tantangan Internal dan Eksternal Organisasi

Common Challenges/ Issues

- Poor data/ information quality (integrity, validity, etc)
- Low availability of data/ information
- Unclear role & responsibility, policy, and procedure for managing data/ information
- Digital Literacy
- Failure in technology adoption for managing data/ information
- High expectation/ requirement from business partners
- Cyber security threat and Data Privacy Issues
- Complex Regulation

1. Governing IT sebagai bagian dari GCG Perusahaan

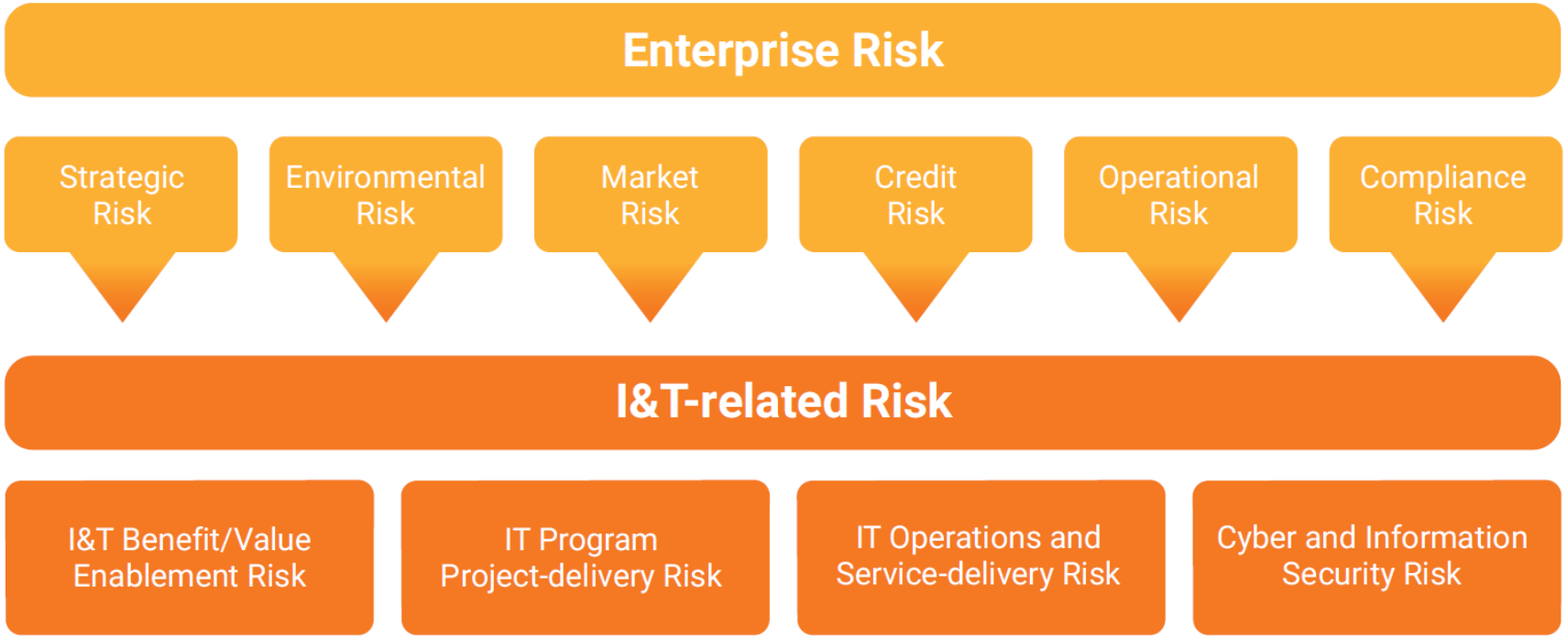


Source: ISACA

IT Governance helps aligned IT to business and governance objectives by managing IT Resources and IT Processes to achieve the objectives of:

- Benefits Realization
- Risk Optimization
- Resource Optimization

2. Information and Technology related Risks adalah bagian dari Enterprise Risk Management



- Information Security Risk as part of Enterprise Risk
- Information security should be embedded in Enterprise Risk Management

Source: ISACA

3. Adopsi Kerangka Governance dan Keamanan yang Banyak Digunakan

An IT security framework is a series of documented processes that define policies and procedures around the implementation and ongoing management of information security controls. These frameworks are a blueprint for managing risk and reducing vulnerabilities. Some internationally recognised information security standards, guidelines and effective security practices for reference:

ISO 27001

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

COBIT 2019

The framework is business focused and defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model

4. Peran Audit Sistem Informasi menjadi makin diperlukan

Selain dorongan dari regulasi, memperoleh keyakinan internal maupun eksternal atas pengelolaan risiko teknologi informasi merupakan suatu kebutuhan yang semakin meningkat saat ini.
IT auditor yang kompeten dan professional diperlukan untuk dapat memastikan kecukupan pelaksanaan audit baik dalam mendukung audit internal perusahaan, maupun audit yang dilakukan oleh eksternal.

CISA Certified Information Systems Auditor®
An ISACA® Certification

Cybersecurity Audit
An ISACA® Certificate

CCAK
A Cloud Security Alliance® and ISACA® Certificate

Cybersecurity Audit?

5. Digital Leadership yang juga fokus kepada pengelolaan risiko siber

Security Is Not Only For Security Teams, Because Attackers Will Look For And Exploit The Weakest Link In The Enterprise. Leadership is a critical component of cybersecurity, and CEOs must make it clear that every stakeholder shares responsibility for ensuring the enterprise's safety. The Human Role in Ensuring Security:

Employees	• Be vigilant, report suspicious emails and links. • Comply with security policies
C-Level Executives	• Embed security into the business DNA. • Take the lead on funding and endorsing cybersecurity
Security Personnel	• Organize, design and implement security programs. • Proactively monitor and manage cyberthreats
The Board	• Take oversight of cybersecurity strategies. • Authorize security budgets and initiatives
Human Resources	• Set cybersecurity expectations for new employees. • Endorse controls to protect employee data

Source: ISACA


Q
A

vedapraxis

HEAD OFFICE

AD Premier, 8th floor
Jl. TB. Simatupang No. 5 Pasar Minggu
Jakarta 12540

Veda Praxis | @VedaPraxis | @veda_praxis | Veda Praxis | Veda Praxis

Phone: +62 21 227 08982 | www.vedapraxis.com | info@vedapraxis.com