News | Information | Highlight | Alert | Opportunity

SEPTEMBER 2023

SW NIHAO

Catalyst for success

DIGITAL

TRANSFORMATION, BANKING AND FIN TECH ON INFORMATION TECHNOLOGY GENERAL CONTROL

Finance | Audit | Investment | Tax | Hybrid

SEPTEMBER 2023

CONTENT

01
ITGC BY AUDITOR: PROCEDURES AND BENEFITS
Changes of IT environment encourage the ITGC as a crucial factor to be done by auditors to develop appropriate controls and mitigate risks.

02
ITGC IN BANKING AUDIT: PROCEDURES AND BENEFITS
IT development is a double-edged sword that provides efficiency, but also cybersecurity risk, which increases the needs of ITGC.

03
IT EXAMINATION FOR A BANKING COMPANY: LPS REGULATION
Compliance needs for banking companies with LPS regulations required them to have IT examinations from auditors to do SCV's data verification.

04
IT INSPECTION OF THE CRYPTO EXCHANGE IN INDONESIA
IT inspection performed by CISA-holder auditors is needed for creating a sense of security for customers/investors on the cryptocurrency exchange.

ITGC by Auditor: Procedures and Benefits

The Information Technology (IT) environment within a company has significantly changed with advancements in information systems (system and software) and technological advancement of utilized hardware. Due to these circumstances, understanding IT General Controls (ITGC), also known as General IT Controls, has become crucial. Additionally, information security frameworks from international organizations standards (COSO, ISACA, ISO) have seen substantial improvements.

Significant and continuous changes in the IT environment can result in increased risks to access and can impact financial reporting. Financial data (the source of financial reporting) is stored in systems like databases, and the functionality ensures that data can be accessed and processed. User access granted/obtained can affect data protection, including the following **SPAP 315, A64**:

a. **Authentication controls:** Ensuring that users accessing applications or other aspects within the IT environment have the appropriate credentials.
b. **Authorization controls:** Allowing users to access required information according to their job responsibilities and proper segregation of duties.
c. **Control over provisioning, revoking, and modifying access:** Authorizing new users and making changes to existing user access rights, including removing user access after termination (resignation).
d. **Control over privileged access:** Allowing administrative access (super admin) or users with elevated or special access to system or application administration.
e. **User access review controls:** Recertifying or evaluating user access for ongoing authorization.
f. **Control over security configuration:** Most technologies have key configuration settings that help restrict access and potential data loss or the inability to access data when needed.
g. **Control over physical access:** Physical access to data centers, hardware, or the physical assets of other IT assets.

Anthony Feryanto, *anthony.feryanto@shinewing.id*

Understanding the client's IT environment is mandatory for auditors through the identification of recommended ITGC frameworks, as set out in the guidelines published by the International Auditing and Assurance Standards Board (IAASB) in International Standards on Auditing (ISA) 315 (2019 revision), and focusing on data security. Auditors will assess risks and use professional judgment to determine the risk factors in the IT environment and the appropriate controls to mitigate them.

What is ITGC?

ITGC comprises policies and procedures that govern (control) an organization's IT system operations, ensuring data confidentiality, integrity, and availability. ITGC encompasses all aspects of IT, including software implementation, user account creation, and data management.

ITGC can be divided into several categories, including:

1. **General IT administration controls,** related to IT system management and oversight, long-term IT strategic planning, and IT risk assessment. These controls also encompass IT security.
2. **Access controls,** covering various methods to prevent unauthorized access and data manipulation. Access controls also include user authentication, data encryption, account locking, and audit trails.
3. **System Development Life Cycle (SDLC) controls,** related to the development, testing, implementation, and maintenance of a system. SDLC controls also include documentation, approvals, change tracking, and performance evaluation.
4. **Program change controls,** governing program and system configuration changes. Program change controls also involve impact analysis, regression testing, segregation of duties, and activity logging.
5. **Physical hardware and data center security controls,** covering security measures against external and internal threats to the physical environment (hardware), including damage, power disruptions, and natural disasters. Data center physical security controls include door and window locks, alarm and CCTV systems, smoke and fire detection, and air conditioning systems.
6. **Backup and system/data recovery controls,** related to periodic copying and backup of data (backup and restore) that can be quickly restored in case of loss or damage. Backup and system/data recovery controls also include backup scheduling, secure storage of backup media, routine recovery testing, and disaster recovery planning.
7. **Computer operations controls,** related to the efficient and effective operation of IT systems. Computer operations controls also involve system performance monitoring, technical issue resolution, capacity and availability management, and incident reporting (helpdesk).

Why is ITGC important?

ITGC is important because it helps companies ensure the effectiveness and compliance of information systems used in business processes and financial reporting. ITGC also enhances the security and integrity of data, programs, and outputs produced by information systems. ITGC helps prevent unauthorized access, data breaches, and operational disruptions. It can reduce the risk of errors, manipulation, or misuse of information technology that could negatively impact a company's performance and reputation. Effective ITGC can improve the reliability and accuracy of financial reporting and help mitigate fraud risk. ITGC is also a requirement to meet applicable audit standards and regulations.

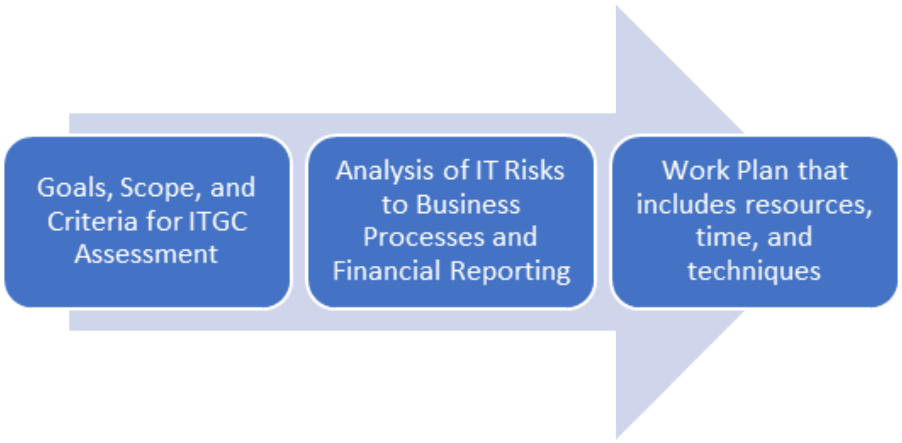
Who, When, and What Are the Benefits of ITGC Review?

A review or assessment of ITGC should ideally be conducted periodically by an independent external party, at least once a year (recommended before the general audit), or as needed based on the risks the company faces. ITGC must be reviewed and assessed by an independent external party because it is beneficial for the company, including:

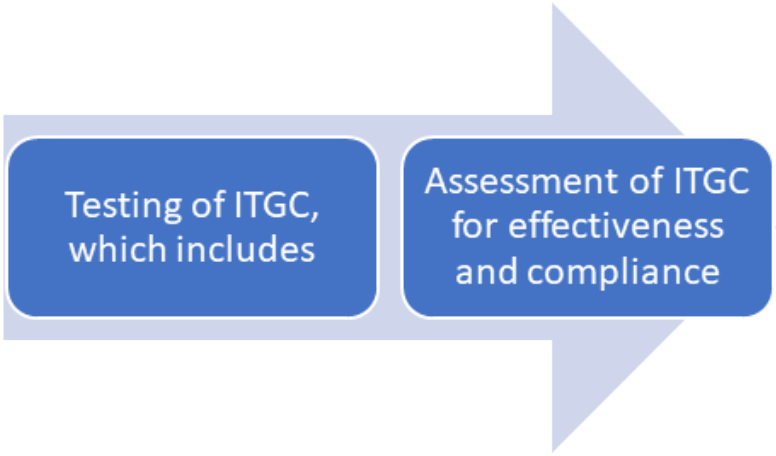
a. **Building trust and credibility** among stakeholders, regulators, auditors, and customers regarding the quality and compliance of the information systems used by the company.
b. **Receiving objective and professional input and advice** from external parties with competence and experience in IT auditing.
c. **Identifying weaknesses, risks, and improvement opportunities in the implementation of ITGC** and recommending appropriate corrective and preventive actions.
d. **Meeting applicable audit standards and regulations,** such as SOX Compliance, which requires companies to conduct periodic assessment of ITGC effectiveness.

How to Conduct ITGC Assessment Done by External Independent Party?

Planning



Fieldwork



Reporting and Recommendations

SW Digital Transformation and Cybertrust are often chosen by independent parties to assess the ITGC of their clients for the following reasons:

a. **Deep expertise** helps us understand the complexity of control systems and risks.
b. **Relevance and up-to-date knowledge** ensure that our services align with the latest international standards in technology and auditing.
c. **Measurable results** with data and facts regarding the successful implementation of ITGC will become an integral part of our services with real impact.
d. **Support for improvement** focuses not only on assessing ITGC but also on recommending improvements and enhancements to client control systems.

ITGC in Banking Audit: Procedures and Benefits

In the ever-evolving digital era, Information Technology (IT) has become the backbone of operations in many industries, including banking. Modern banks rely on robust and reliable IT systems to support their operations, from basic transactions to complex data analytics. Therefore, it is crucial for banks to have strong controls over their IT infrastructure, and Information Technology General Controls (ITGC) play a significant role. ITGC serves as a pillar of strength that helps banks navigate the digital landscape with confidence and reliability.

ITGC refers to a set of procedures and policies designed to ensure the integrity, reliability, and security of IT systems and data. ITGC encompasses various aspects, including access controls, change controls, operational controls, and system development management.

Why ITGC Is Important for Banking?

Banking is an industry highly regulated by strict laws and regulations, demanding high standards of security and accuracy. At the same time, banking is also a target for cyberattacks, making IT security a top priority. With an increasing number of transactions conducted electronically, cybersecurity threats become more tangible. If customer data or financial information were to leak or be stolen, it could damage the bank's reputation and result in significant financial losses.

Moreover, banking requires operational efficiency to conduct transactions swiftly and accurately. Without effective ITGC, banks may encounter hindrances in transaction processes, errors in reporting, or even financial losses.

Thomas Gunawan, *thomas.gunawan@shinewing.id*

ITGC comprises several key components that banking institutions need to understand to run secure and efficient operations:

- **Access Controls:** Ensure that only authorized individuals can access systems and data. This includes authentication, authorization, and audit trails.
- **Change Controls:** Monitor changes to systems and applications to ensure that all modifications have been tested and approved before implementation.
- **Operational Controls:** Ensure that day-to-day operations run smoothly, including data backup, disaster recovery, and routine maintenance.
- **System Development Management:** Oversee the development, testing and the implementation of new systems or updates to existing systems.

Implementation of ITGC in Banking

The implementation process of ITGC in the banking industry involves a series of careful and structured steps:

- **Access Controls:** Banks must ensure that sensitive information such as customer data and financial transactions can only be accessed by authorized parties. This is done by implementing multi-factor authentication, access control policies, intrusion detection systems, and logging and monitoring mechanisms. The presence of access logs and system monitoring can also be used to detect suspicious activities.
- **Change Controls:** Every change in IT systems should be recorded, tested, and approved before implementation. This is to prevent errors that can disrupt operations or create security vulnerabilities.
- **Operational Controls:** This includes backup and restore policies, hardware maintenance, system performance monitoring, and disaster recovery procedures to ensure operational continuity.
- **System Development Management:** Monitor the process from initial system development until its launch, ensuring that all code and infrastructure are analyzed thoroughly for potential risks. Processes such as needs analysis, design, and testing should be tightly managed to ensure quality and security.

Common Findings in ITGC Audits in Banking and Their Remediation

Some common findings that often arise in ITGC audits include:

- **Weaknesses in Access Controls:** Many banks have weaknesses in controlling access to their systems and data. Access granted may not align with individuals' roles, opening up potential security risks. To mitigate this, banks need to refine access control policies and their implementation, as well as provide employee training on the importance of information security.
- **Lack of Change Controls:** Some banks have not fully adopted change control principles, resulting in errors or disruptions. Changes to systems are not always followed by adequate testing, increasing the risk of vulnerabilities. To address this, banks need to implement change tracking systems and hold review sessions before each implementation. All changes should be documented, tested in a controlled environment, and applied after approval.
- **Inadequate Maintenance or Neglect of Routine Maintenance:** Outdated or poorly maintained IT infrastructure can be vulnerable to attacks. Additionally, periodic maintenance is often neglected, leading to potential operational failures. Therefore, banks need to schedule routine maintenance and regularly upgrade their systems.
- **Failure in Backup and Recovery:** Sometimes, banks lack adequate disaster recovery procedures. On the other hand, while many banks have such plans, they may not have tested them or updated them for an extended period. To mitigate this, banks need to establish comprehensive disaster recovery plans and regularly test them to ensure their effectiveness.

These ITGC findings in the banking sector can relate to core transaction functions such as interest calculations, loan processing, transaction recording, and more. Some advanced findings resulting from inadequate ITGC may include:

- Inaccuracies in Interest Calculations: Banking systems may have errors in logic or configurations that result in inaccurate interest calculations for customer accounts.
- Errors in Loan Processing: Systems may not process loan applications correctly, or there may be flaws in the automation of loan approvals, resulting in the granting of credit that does not meet criteria.
- Insufficient Transaction Authorization: Transactions may not require adequate authorization or verification before execution, increasing the risk of errors or misuse.
- Failure to Comply with Data Privacy Policies: Systems may not comply with data privacy policies, which can negatively impact the bank's reputation or result in significant fines.
- Transaction Errors: Errors may occur in transaction processing, such as duplicate fund transfers or transactions that do not align with customer instructions.

In all of these cases, active involvement from management is crucial. Management must support the IT team, understand associated risks, allocate necessary resources to mitigate those risks, and communicate the importance of compliance and controls to the entire organization. Awareness and commitment from management will help ensure successful and sustainable risk mitigation. By identifying and mitigating ITGC findings and with active support from management, banks can strengthen their IT infrastructure, enhance customer trust, and ensure smooth and secure operations.

ITGC is a critical element in maintaining the security, integrity, and operational efficiency in the banking industry. Through the effective implementation and maintenance of ITGC, banks can reduce security risks, enhance customer trust, and ensure operational smoothness. Regular evaluation of ITGC enables a bank to identify areas needing improvement. Audit findings should be followed up by management with recommended improvements and initiatives.

Furthermore, banking regulations by the Financial Services Authority (OJK) through POJK number 11/POJK.03/2022 regarding the Implementation of Information Technology by Commercial Banks, especially article 55 paragraph (2), also require banks to conduct a reassessment of the internal audit function of IT implementation at least once every three years using independent external services. SW Indonesia has years of experience in providing professional services to banking companies in Indonesia. SW Indonesia continues to develop competence and capacity to support clients in the banking industry, including ITGC audit services, internal audit function reassessment of IT implementation, cybersecurity, and other services.

IT Examination for a Banking Company: LPS Regulation

A banking company is in an industry that is full of regulations and involves complex information technology in its business processes. Information technology is fundamental to banking business activities, improving customer experience and operational efficiency. The transformation of information technology and digital technology brings challenges in maintaining security, complying with regulations and managing risk. IT examination in the banking sector are crucial and are regulated in The Indonesia Deposit Insurance Corporation (IDIC / LPS) regulations.

The Important Role of Savings Insurance and LPS

In the realm of financial security, the role of deposit insurance institutions is now very important to build trust and maintain economic stability. LPS in Indonesia is known as the Indonesia Deposit Insurance Corporation (IDIC). LPS is an institution established based on Law Number 24 of 2004 concerning Deposit Insurance Corporation (LPS Law), which has been amended by Law Number 7 of 2009. Since its enactment on 22 September 2005, the implementation of LPS has marked a significant shift in guarantee policy. previous government between 1998 and 2005.

Although the policy initially provided confidence, it put a burden on public finances and raised concerns, which led to the policy's discontinuation. LPS emerged as a response to ensure deposit insurance protection, maintain trust in the banking sector and manage risk.

The real impact of LPS is the transfer from general guarantees to limited guarantees. Article 11 of the LPS Law sets a maximum guarantee of IDR 100 million for each deposit in the bank by a customer. This is in line with international practice seen in 72 countries, including countries with developed economies. The transition to limited collateral balances depositor confidence and mitigates systemic risk, strengthening the banking system's resilience to market fluctuations.

Bryant Junevan, *bryant.mulia@shinewing.id*

LPS's Functions and Authorities

LPS operates with specific functions and authorities to safeguard depositors' interests and contribute to banking system stability. Its primary role is guaranteeing customer deposit security while maintaining overall banking system stability. LPS formulates deposit insurance policies, executes the insurance process, and shapes banking system stability policies. Moreover, LPS's authority spans various aspects, from determining insurance premiums to conducting deposit insurance awareness initiatives.

SCV Reporting: PLPS No. 5 of 2019

In the realm of banking regulations, LPS Regulation (PLPS) No. 5 of 2019 holds a significant position, specifically in relation to Article 3 and Article 10. This regulation addresses the imperative matter of customer-based deposit guarantee data reporting, referred to as Single Customer View (SCV).

Article 3

(1) Banks are required to possess and maintain:
   a. Raw Data;
   b. SCV Detail Data Per Customer;
   c. SCV Data Per Customer; and
   d. Summary Data SCV Per Bank.

(2) The Bank is responsible for the correctness of the data as intended in paragraph (1) in accordance with provisions of laws and regulations in the field banking.

Article 10

(1) Internal bank examination must conduct reviews on the quality of data and the reliability of systems used in the processing and retention of data as referred to in Article 3 paragraph (1).

(2) The review mentioned in paragraph (1) must be conducted at least once in 1 (one) year.

(3) In addition to internal bank examination, reviews of the system's reliability as referred to in paragraph (1) must also be conducted by independent external parties in accordance with the provisions of regulations, at least once every 3 (three) years.

- **Raw Data**
  Raw data set by Bank Indonesia, The Otoritas Jasa Keuangan (OJK), and LPS that provides customer information reported through the Integrated Reporting portal, among others, is used as the basis for preparing the SCV. The Data is submitted monthly.
- **SCV Data Per Customer**
  Data containing at least the total value of deposits categorized in accordance with Total of the LPS Guarantee Program. The Data is submitted annually for positions as of the end of the year.
- **SCV Detail Data Per Customer**
  a. Ownership of savings, loans, or equivalent to deposits or loans; and
  b. The value of Deposits categorized according to the provisions of the LPS Guarantee Program for the relevant Customer Deposits.
- **Summary Data**
  Summary Data from SCV Per Bank is the most rarely used data to calculate the number of customers and deposits in accordance with the category of SCV Data per customer. The Data is submitted monthly for positions as of the end of the month.

This regulatory framework reveals the complexities and responsibilities associated with reporting customer-based deposit insurance data for commercial banks. This regulation introduces us to different customer categories, namely Category 1, Category 2 and Category 3. These categories determine how customer savings data is managed. Category 1 includes customers whose data is carefully recorded by the bank and does not pose a risk to its stability. In contrast, Category 2 refers to customers whose data is not recorded by the bank, and they may create an unhealthy banking environment. Category 3 includes customers outside the previous two categories.

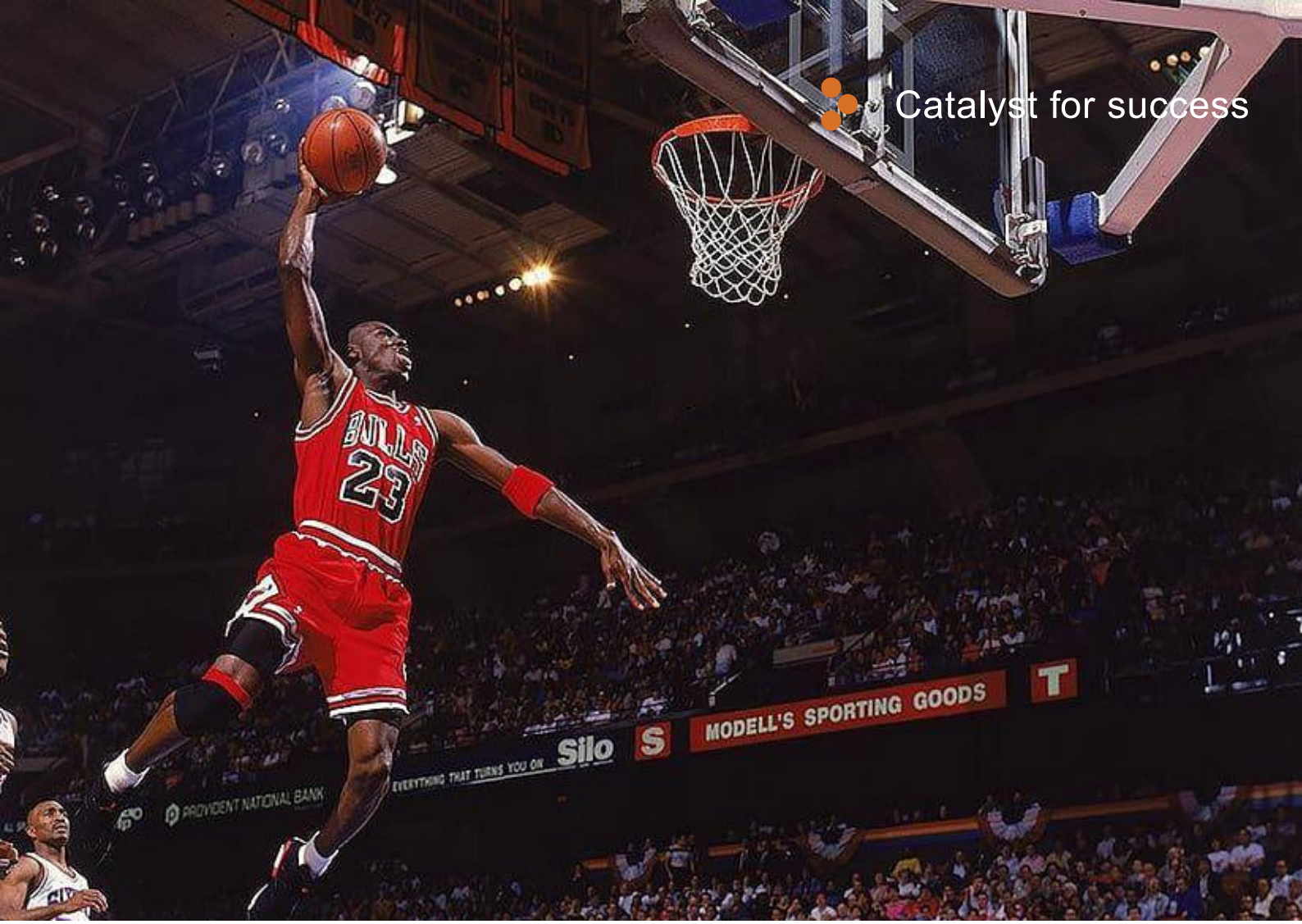
One of the key components of this framework is the Single Customer View (SCV) concept, which is an integrated view of a customer's financial relationship with the bank. The importance of SCV data and the reliability of the data processing system is felt in the context of IT Examination for banking companies, especially in ensuring compliance with LPS regulations. Regulations such as LPS Regulation (PLPS) no. 5 of 2019, emphasizes the importance of accurate SCV data reporting and the integrity of the data processing system.

Roles of IT Examination

An effective IT examination is pivotal in achieving these objectives. IT examination plays a vital role in ensuring a banking company's compliance with LPS regulations, particularly regarding SCV data reporting. By rigorously reviewing and assessing operations, IT auditor verify the accuracy, confidentiality and reliability of SCV data. This compliance not only upholds legal standards but also mitigates risks tied to inaccuracies.

Furthermore, IT examination is essential for maintaining data integrity and confidentiality. Given the sensitive nature of SCV data encompassing customer information and financial details, the examination evaluates confidentiality measures throughout the data lifecycle. It also ensures data integrity from collection to reporting, aligning with LPS goals. Additionally, IT examination bolsters operational resilience by scrutinizing IT infrastructure, system robustness and security. This approach minimizes risks, enhances compliance and fosters a secure environment aligned with LPS regulations.

Through rigorous evaluation and verification, IT Examination improves compliance, confidentiality, integrity, and availability of SCV data. Ultimately increasing operational resilience and contributing to effective risk mitigation strategies for banks. The experience of CISA holders in SW Indonesia has proven the effectiveness of the IT Examination.



IT Inspection of the Crypto Exchange in Indonesia

Terminologically, the word cryptocurrency originates from two words, cryptography and currency. As reported by *Investopedia.com*, cryptocurrency is a digital currency based on cryptography within a distributed network among computers on a large scale. Cryptography is a security system that makes cryptocurrency safe from counterfeiting and double spending issues.

Most cryptocurrencies are built using blockchain technology. Blockchain technology allows various entities to store, record, and verify transactions in a ledger transparently and securely in a decentralized system without the involvement of third parties. This blockchain technology forms the foundation for the largest cryptocurrency, Bitcoin.

Bitcoin is the first-generation cryptocurrency that has achieved success. Bitcoin was born in 2009, precisely a year after the global financial crisis. Initially, many doubted and questioned Bitcoin's ability to survive. However, to this day, the resilience of the Bitcoin network is considered excellent and has never been hacked. This is due in part to the fact that the Bitcoin network is built on many nodes.

Nodes are computer networks that operate the Bitcoin network. Nodes are interconnected and communicate to build and update the blockchain database. Hacking one node does not disrupt the entire network because other nodes will quickly remove the compromised node from the overall network.

Despite this revolutionary technology, the emergence of cryptocurrencies has brought technological disruption to the financial sector. The exponential growth in global cryptocurrency usage has led to the emergence of various cryptocurrency exchanges. At the end of 2022, FTX, the second-largest cryptocurrency exchange in the world, experienced a collapse. Sam Bankman-Fried (SBF), the owner of FTX exchange, who was touted as 'The Next Warren Buffet,' lost his entire $16 billion fortune within 24 hours.

FTX was suspected of misusing customer funds. Through its subsidiary, Alameda Research, the company diverted customer funds for various activities such as campaign funding, social funds, and trading. FTX practiced fractional reserve, so when there were large withdrawals, FTX could not return customer funds.

This incident prompted various financial authorities worldwide to oversee cryptocurrency exchanges. The largest cryptocurrency exchange in Indonesia, Indodax, has implemented a Agreed Upon Procedures (AUP) verification of Proof of Reserve (PoR) and Liquidity Adequacy Calculation. This step was taken to enhance customer confidence in conducting transactions.
Bappebti Regulation No. 4 of 2023 has provided a framework for cryptocurrency exchanges. The regulation stipulates that Prospective Physical Crypto Asset Traders must place all customer funds with a Futures Clearing Institution in an account specifically used to facilitate the placement of funds and settlement of Physical Crypto Asset Market transactions. The provision of buying and selling facilities and online trading systems must be examined or audited by independent institutions with expertise in information systems. In addition, Prospective Physical Crypto Asset Traders must report all managed wallets before registering as a Prospective Physical Crypto Asset Trader.

To support operational activities, Prospective Physical Crypto Asset Traders are required to provide employment contracts with employees holding Certified Information System Security Professional (CISSP) and Certified Information System Auditor (CISA) certificates when registering with Bappebti. SW Indonesia is often asked to assist Prospective Physical Crypto Asset Traders in complying with the regulations and frameworks provided by the regulator.

Through Law No. 4 of 2023 on Cryptocurrency, cryptocurrency regulations in Indonesia will undergo significant changes with the transition of supervisory authority from Bappebti to OJK. Subsequently, OJK will oversee the entire financial sector, including banking, capital markets, pension funds, insurance, fintech, cryptocurrencies, and cooperatives. The transition of supervisory authority is expected to take between 6 months and 2 years. During this transition period, Prospective Physical Crypto Asset Traders are expected to prepare for compliance with the applicable regulations.

The Indonesian government itself launched a cryptocurrency exchange on July 17, 2023, in accordance with the Decision of the Head of Bappebti Number 01/BAPPEBTI/SP-BBAK/07/2023, named the Commodity Future Exchange (CFX), under PT Bursa Komoditi Nusantara. The Indonesian government, through the Ministry of Trade, hopes that the domestic cryptocurrency exchange will increase the number of cryptocurrency transactions and create a secure transaction ecosystem for customers. IT examinations conducted by CISA holders become one of the alternatives to creating a sense of security for customers or investors on the cryptocurrency exchange.

SW INDONESIA

WE ARE HIRING

FINANCE LIAISON - CHINESE SPEAKING

Jakarta Tangerang

JOIN OUR TEAM

recruitment@shinewing.id

Catalyst for success

SW Indonesia @shinewing.indonesia sw-indonesia.com

KAP Suharli, Sugiharto & Rekan | SW Tax Consulting | SW Business Advisory | SW Business Process Outsourcing

ITGC Oleh Auditor: Prosedur dan Manfaat

Lingkungan dalam Teknologi Informasi (IT) Perusahaan banyak berubah signifikan dengan perubahan pada sistem informasi (system dan software) dan kecanggihan dari perangkat keras yang diutilisasi. Akibat keadaan tersebut, pemahaman akan Pengendalian Umum IT atau biasa disebut IT General Controls (ITGC), menjadi hal yang sangat penting. Di samping itu, kerangka kerja atas keamanan informasi dari standar organisasi internasional (COSO, ISACA, ISO) juga mengalami peningkatan secara besar-besaran.

Perubahan lingkungan IT yang signifkan dan terus menerus dapat mengakibatkan peningkatan risiko dalam akses, serta berdampak pada penyusunan laporan keuangan. Data keuangan (sumber laporan keuangan) disimpan dalam sistem seperti database, juga fungsionalitas memastikan bahwa data dapat diakses dan diproses. Akses pengguna yang diberikan/diperoleh dapat berdampak pada perlindungan data meliputi hal-hal berikut **SPAP 315, A64:**

a. **Pengendalian secara autentikasi:** Memastikan bahwa pengguna yang mengakses aplikasi atau aspek lain dalam lingkungan IT sesuai kredensial yang ditetapkan.
b. **Pengendalian secara otorisasi:** Memungkinkan pengguna mengakses informasi yang diperlukan sesuai dengan tanggung jawab pekerjaan dan pemisahan tugas yang tepat.
c. **Pengendalian atas penyediaan, pencabutan dan perubahan akses:** Memberi otorisasi kepada pengguna baru dan perubahan pada hak akses pengguna yang sudah ada. Termasuk, menghapus akses
d. pengguna setelah penghentian (berhenti).
Pengendalian atas akses istimewa: Mengizinkan akses administratif (super admin) atau pengguna
e. yang memiliki akses lebih atau istimewa atas administrasi system atau aplikasi.
f. **Pengendalian secara peninjauan akses pengguna:** Sertifikasi ulang atau mengevaluasi akses pengguna untuk otorisasi secara berkelanjutan.
Pengendalian atas konfigurasi keamanan: Setiap teknologi umumnya memiliki pengaturan konfigurasi utama yang membantu membatasi akses dan potensi kehilangan data atau ketidakmampuan untuk
g. mengakses data ketika dibutuhkan.
Pengendalian atas akses fisik—Akses fisik ke pusat data, perangkat keras atau fisik dari aset IT lain.

Anthony Feryanto, *anthony.feryanto@shinewing.id*

Pemahaman terhadap Lingkungan IT klien merupakan hal yang wajib bagi auditor melalui identifikasi atas kerangka ITGC (yang disarankan), seperti yang ditetapkan dalam pedoman yang diterbitkan oleh *International Auditing and Assurance Standards Board* (IAASB) dalam *International Standards on Auditing* (ISA) 315 (revisi 2019), serta berfokus pada keamanan data. Auditor akan melakukan penilaian risiko dan menggunakan pertimbangan profesional untuk menentukan faktor risiko dalam lingkungan IT dan pengendalian yang tepat untuk memitigasinya.

Apa itu ITGC?

ITGC adalah kumpulan kebijakan dan prosedur yang mengatur (pengendalian) terhadap sistem IT di suatu Perusahaan yang beroperasi dengan menjamin kerahasiaan, integritas dan ketersediaan data. ITGC mencakup setiap aspek IT, termasuk implementasi perangkat lunak, pembuatan akun pengguna dan pengelolaan data.

ITGC dapat dibagi menjadi beberapa kategori, antara lain:

1. **Pengendalian administrasi IT umum,** yang berkaitan dengan pengelolaan dan pengawasan sistem IT, rencana jangka panjang IT (IT strategic planning), penilaian risiko terkait IT. Pengendalian ini juga mencakup keamanan IT (IT security).
2. **Pengendalian atas akses,** yang mencakup berbagai metode untuk mencegah akses tidak sah dan manipulasi data. Pengendalian atas akses juga meliputi otentikasi pengguna, enkripsi data, penguncian akun dan audit jejak.
3. **Pengendalian siklus hidup pengembangan sistem (SDLC),** yang terkait atas pengembangan, pengujian, implementasi dan pemeliharaan suatu sistem. Pengendalian SDLC juga meliputi dokumentasi, persetujuan, pelacakan perubahan dan evaluasi kinerja.
4. **Pengendalian perubahan program,** yang mengatur perubahan program dan konfigurasi sistem. Pengendalian perubahan program juga meliputi analisis dampak, pengujian regresi, pemisahan tugas dan pencatatan aktivitas.
5. **Pengendalian keamanan fisik perangkat keras dan pusat data,** yang mencakup pengamanan terhadap lingkungan fisik (hardware) dari ancaman eksternal maupun internal, termasuk kerusakan, gangguan listrik dan bencana alam. Pengendalian keamanan fisik pusat data meliputi penguncian pintu dan jendela, sistem alarm dan CCTV, deteksi asap dan api, serta sistem pendingin udara.
6. **Pegendalian cadangan dan pemulihan sistem dan data,** yang terkait atas penyalinan dan pencadangan (backup & restore) secara berkala dan dapat dipulihkan dalam waktu singkat jika terjadi kehilangan atau kerusakan. Pengendalian cadangan dan pemulihan sistem dan data juga meliputi penjadwalan cadangan, penyimpanan media cadangan di lokasi aman, pengujian pemulihan secara rutin, serta rencana pemulihan bencana.
7. **Pengendalian operasi komputer,** yang berkaitan dengan pengoperasian sistem IT secara efisien dan efektif. Pengendalian operasi komputer juga meliputi pemantauan kinerja sistem, penyelesaian masalah teknis, manajemen kapasitas dan ketersediaan, serta pelaporan insiden (helpdesk).

Mengapa ITGC penting?

ITGC penting karena dapat membantu perusahaan dalam memastikan efektivitas dan kepatuhan sistem informasi yang digunakan untuk proses bisnis dan pelaporan keuangan. ITGC juga dapat meningkatkan keamanan dan integritas data, program, dan output yang dihasilkan oleh sistem informasi. ITGC membantu mencegah akses tidak sah, pelanggaran data, dan gangguan operasional. ITGC juga dapat mengurangi risiko terjadinya kesalahan, manipulasi, atau penyalahgunaan teknologi informasi yang dapat berdampak negatif pada kinerja dan reputasi perusahaan. ITGC yang efektif dapat meningkatkan keandalan dan akurasi pelaporan keuangan dan mengurangi risiko kecurangan. ITGC juga menjadi salah satu persyaratan dalam memenuhi standar audit dan regulasi yang berlaku.

Siapa, Kapan dan Apa Manfaat reviu ITGC?

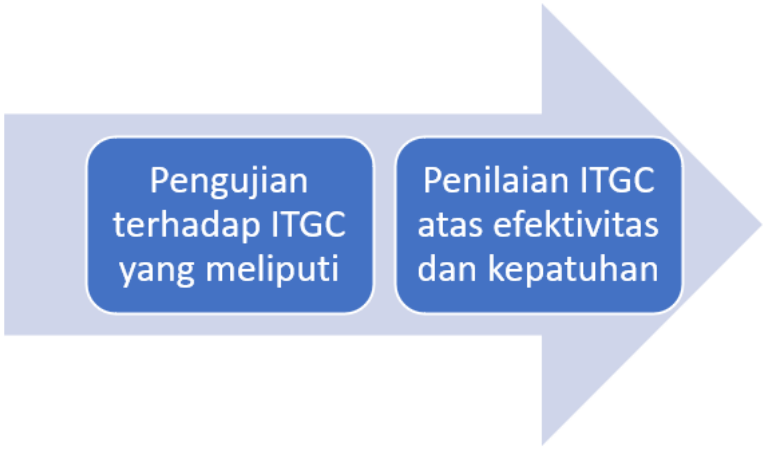
Reviu atau penilaian atas ITGC idealnya dilakukan secara berkala oleh pihak eksternal independen, setidaknya sekali dalam setahun (disarankan sebelum audit umum), atau sesuai dengan kebutuhan dan risiko yang dihadapi oleh perusahaan. ITGC perlu direviu dan dinilai oleh pihak eksternal yang independen karena hal ini dapat memberikan manfaat bagi perusahaan, antara lain:

1. **Meningkatkan kepercayaan dan kredibilitas** dari stakeholder, regulator, auditor, dan pelanggan terhadap kualitas dan kepatuhan sistem informasi yang digunakan oleh perusahaan.
2. **Mendapatkan masukan dan saran yang objektif dan profesional** dari pihak eksternal yang memiliki kompetensi dan pengalaman dalam bidang IT audit.
3. **Mengidentifikasi kelemahan, risiko, dan peluang perbaikan dalam penerapan ITGC,** serta merekomendasikan tindakan korektif dan preventif yang sesuai.
4. **Memenuhi standar audit dan regulasi yang berlaku,** seperti SOX Compliance, yang mengharuskan perusahaan untuk melakukan penilaian atas efektivitas ITGC secara berkala.

Bagaimana melakukan penilaian atas ITGC oleh pihak eksternal independen?

Perencanaan

Pekerjaan Lapangan



Pelaporan dan Rekomendasi

SW Digital Transformation and Cybertrust kerapkali menjadi pilihan pihak independen melakukan penilaian ITGC klien-klien kami karena pertimbangan sebagai berikut:

1. **Pengalaman yang Mendalam** membantu kami memahami kerumitan sistem kontrol dan risiko.
2. **Relevansi dan Kekinian** mengikuti perkembangan terbaru dalam dunia teknologi dan audit, memastikan bahwa layanan kami sesuai dengan standar internasional terbaru.
3. **Hasil yang Terukur** dengan data dan fakta mengenai keberhasilan implementasi ITGC akan menjadi bagian integral dari layanan kami yang berdampak secara nyata.
4. **Dukungan untuk Peningkatan** yang tidak hanya fokus pada penilaian ITGC semata, melainkan rekomendasi untuk perbaikan dan peningkatan sistem kontrol klien.

ITGC Dalam Audit Sebuah Bank: Prosedur dan Manfaat

Dalam era digital yang semakin berkembang, Teknologi Informasi (TI) telah menjadi tulang punggung operasional banyak industri, termasuk perbankan. Bank-bank modern bergantung pada sistem TI yang kuat dan handal untuk mendukung operasi mereka, mulai dari transaksi dasar hingga analisis data yang rumit. Oleh karena itu, penting bagi bank untuk memiliki pengendalian yang kuat atas infrastruktur TI mereka dan *Information Technology General Controls* (ITGC) memainkan peran penting. ITGC hadir sebagai pilar kekuatan yang membantu bank menavigasi lautan digital dengan kepercayaan dan keandalan.

ITGC merujuk pada serangkaian prosedur dan kebijakan yang dirancang untuk memastikan integritas, keandalan, dan keamanan sistem dan data TI. ITGC mencakup berbagai aspek, termasuk pengendalian akses, pengendalian perubahan, pengendalian operasional dan manajemen pengembangan sistem.

Mengapa ITGC Penting untuk Perbankan?

Perbankan adalah industri yang sangat diatur oleh undang-undang dan regulasi yang ketat, yang menuntut standar keamanan dan akurasi yang tinggi. Pada saat yang sama, perbankan juga menjadi target serangan siber, membuat keamanan TI menjadi prioritas. Dengan semakin banyaknya transaksi yang dilakukan secara elektronik, ancaman keamanan siber menjadi semakin nyata. Jika data pelanggan atau informasi keuangan bocor atau dicuri, maka hal tersebut bisa merusak reputasi bank dan menimbulkan kerugian finansial yang signifikan.

Selain itu, perbankan memerlukan efisiensi operasional untuk menjalankan transaksi dengan cepat dan akurat. Tanpa ITGC yang efektif, bank mungkin menghadapi hambatan dalam proses transaksi, kesalahan dalam laporan, atau bahkan kerugian finansial.

Thomas Gunawan, *thomas.gunawan@shinewing.id*

ITGC mencakup sejumlah komponen kunci yang harus dipahami oleh perbankan untuk menjalankan operasi yang aman dan efisien:

- **Pengendalian Akses:** Memastikan bahwa hanya individu yang berwenang yang dapat mengakses sistem dan data. Ini mencakup otentikasi, otorisasi dan audit trail.
- **Pengendalian Perubahan:** Mengawasi perubahan pada sistem dan aplikasi untuk memastikan bahwa semua modifikasi telah diuji dan disetujui sebelum diterapkan.
- **Pengendalian Operasional:** Memastikan bahwa operasi sehari-hari berjalan dengan lancar, termasuk backup data, pemulihan bencana dan pemeliharaan rutin.
- **Manajemen Pengembangan Sistem:** Mengawasi pengembangan, pengujian dan penerapan sistem baru atau pembaruan sistem yang ada.

Pelaksanaan ITGC di Perbankan

Proses pelaksanaan ITGC dalam industri perbankan melibatkan serangkaian langkah yang cermat dan **terstruktur:**

- **Pengendalian Akses:** Bank harus memastikan bahwa informasi sensitif seperti data pelanggan dan transaksi keuangan hanya dapat diakses oleh pihak yang berwenang. Ini dilakukan dengan mengimplementasikan otentikasi multi-faktor, pengendalian hak akses, sistem deteksi intrusi, serta mekanisme logging dan pemantauan. Keberadaan log akses dan pemantauan sistem ini juga dapat digunakan untuk mendeteksi aktivitas yang mencurigakan.
- **Pengendalian Perubahan:** Setiap perubahan dalam sistem TI harus direkam, diuji, dan disetujui sebelum implementasi. Hal ini untuk menghindari kesalahan yang dapat mengganggu operasi atau menciptakan celah keamanan.
- **Pengendalian Operasional:** Meliputi kebijakan backup dan restore, pemeliharaan perangkat keras, pemantauan kinerja sistem, serta prosedur pemulihan bencana untuk memastikan kelangsungan operasional.
- **Manajemen Pengembangan Sistem:** Mengawasi proses dari pengembangan awal hingga peluncuran (system launch), memastikan semua kode dan infrastruktur dianalisis secara menyeluruh terhadap potensi risiko. Proses seperti analisis kebutuhan, desain dan pengujian harus dikelola dengan ketat untuk memastikan kualitas dan keamanan.

Temuan Umum dalam Audit ITGC di Perbankan dan Tindaklanjutnya

Beberapa temuan umum yang sering muncul dalam audit ITGC di antaranya:

- **Kelemahan dalam Pengendalian Akses:** Banyak bank memiliki kelemahan dalam mengendalikan akses ke sistem dan data mereka. Akses yang diberikan tidak sesuai dengan peran individu sehingga membuka potensi risiko keamanan. Untuk memitigasinya, bank perlu melakukan penyempurnaan kebijakan hak akses dan penerapannya, serta pelatihan karyawan mengenai pentingnya keamanan informasi.
- **Kurangnya Pengendalian Atas Perubahan:** Beberapa bank belum sepenuhnya mengadopsi prinsip pengendalian perubahan, sehingga terjadi kesalahan atau gangguan. Perubahan pada sistem tidak selalu diikuti oleh pengujian yang memadai, meningkatkan risiko kerentanan. Untuk mengatasinya, bank perlu menerapkan sistem pelacakan perubahan dan mengadakan sesi review sebelum setiap implementasi. Semua perubahan harus didokumentasikan, diuji di lingkungan yang terkontrol dan diterapkan setelah mendapatkan persetujuan.
- **Pemeliharaan yang Tidak Memadai atau Pengabaian Pemeliharaan Rutin:** Infrastruktur TI yang ketinggalan zaman atau tidak terawat dapat menjadi rentan terhadap serangan. Selain itu, pemeliharaan berkala juga sering diabaikan, mengarah pada potensi kegagalan operasional. Karena itu, bank perlu menjadwalkan pemeliharaan rutin dan melakukan peningkatan sistem secara berkala.
- **Kegagalan Dalam Backup dan Pemulihan:** Kadang-kadang, bank tidak memiliki prosedur pemulihan bencana yang memadai. Di sisi lain, meskipun banyak bank memiliki rencana ini, beberapa mungkin belum mengujinya atau memperbarui rencananya dalam waktu yang lama. Untuk memitigasinya, bank perlu menyusun rencana pemulihan bencana yang komprehensif dan secara rutin menguji rencana pemulihan bencana tersebut untuk memastikan efektivitasnya.

Temuan ITGC dalam sektor perbankan di atas dapat berkaitan dengan fungsi transaksi inti seperti perhitungan bunga, proses pinjaman, pencatatan transaksi, dan lainnya. Beberapa temuan lanjutan yang bisa disebabkan oleh ITGC yang tidak memadai di antaranya:

- **Ketidakakuratan dalam Perhitungan Bunga:** Sistem perbankan mungkin memiliki kesalahan dalam logika atau konfigurasi yang mengakibatkan perhitungan bunga yang tidak akurat untuk rekening nasabah.
- **Kesalahan dalam Proses Pinjaman:** Sistem mungkin tidak memproses aplikasi pinjaman dengan benar atau ada kelemahan dalam otomatisasi persetujuan pinjaman yang mengakibatkan pemberian kredit yang tidak memenuhi kriteria.
- **Pengesahan Transaksi yang Tidak Memadai:** Transaksi mungkin tidak memerlukan otorisasi yang memadai atau verifikasi sebelum dieksekusi, meningkatkan risiko kesalahan atau penyalahgunaan.
- **Kegagalan dalam Memenuhi Kebijakan Privasi Data:** Sistem mungkin tidak mematuhi kebijakan privasi data, yang dapat berakibat negatif pada reputasi bank ataupun denda yang signifikan.
- **Kesalahan dalam Transaksi:** Terjadi kesalahan dalam pemrosesan transaksi, seperti transfer dana ganda, atau transaksi yang tidak sesuai dengan instruksi nasabah.

Dalam semua kasus ini, keterlibatan aktif dari manajemen sangat penting. Manajemen harus mendukung tim TI, memahami risiko yang terkait, dan mengalokasikan sumber daya yang diperlukan untuk memitigasi risiko tersebut, serta mengkomunikasikan pentingnya kepatuhan dan pengendalian kepada seluruh organisasi. Kesadaran dan komitmen manajemen akan membantu memastikan bahwa mitigasi risiko dilaksanakan dengan sukses dan berkelanjutan.Dengan mengidentifikasi dan memitigasi temuan-temuan ITGC, serta dengan dukungan aktif dari manajemen, bank dapat memperkuat infrastruktur TI mereka, meningkatkan kepercayaan pelanggan, dan memastikan operasi yang efisien dan aman.

ITGC merupakan elemen penting dalam menjaga keamanan, integritas, dan efisiensi operasional dalam industri perbankan. Implementasi dan pemeliharaan ITGC yang efektif, bank dapat mengurangi risiko keamanan, meningkatkan kepercayaan pelanggan, dan memastikan kelancaran operasi. Ealuasi ITGC secara berkala memampukan sebuah bank mengidentifikasi area yang memerlukan perbaikan. Hasil audit harus ditindaklanjuti oleh manajemen dengan perbaikan dan inisiatif yang direkomendasikan.

Selain itu, regulasi perbankan oleh Otoritas Jasa Keuangan (OJK) melalui POJK nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, khususnya pasal 55 ayat (2), juga mewajibkan bank untuk melakukan kaji ulang terhadap fungsi audit intern atas penyelenggaraan TI paling sedikit satu kali dalam tiga tahun dengan menggunakan jasa pihak ekstern yang independen. SW Indonesia memiliki pengalaman bertahun-tahun dalam memberi layanan professional kepada perusahaan-perusahaan perbankan di Indonesia. SW Indonesia terus mengembangkan kompetensi dan kapasitas untuk mendukung klien di industri perbankan, termasuk pemberian layanan audit ITGC, kaji ulang fungsi audit intern atas penyelenggaraan TI, kemanan siber dan layanan lain.

Pemeriksaan IT untuk Perusahaan Perbankan: Regulasi LPS

Sebuah perusahaan perbankan berada dalam industri yang penuh regulasi dan melibatkan teknologi informasi yang rumit dalam proses bisnisnya. Teknologi informasi menjadi fundamental dari aktivitas usaha perbankan, meningkatkan pengalaman nasabah dan efisiensi operasional. Transformasi teknologi informasi dan teknologi digital membawa tantangan dalam menjaga keamanan, mematuhi regulasi dan mengelola risiko. Pemeriksaan IT dalam sektor perbankan menjadi krusial dan diatur dalam regulasi Lembaga Penjamin Simpanan (LPS).

Peran Penting Asuransi Simpanan dan LPS

Dalam ranah keamanan keuangan, peran lembaga asuransi simpanan sekarang ini menjadi sangat penting untuk membina kepercayaan dan menjaga stabilitas ekonomi. LPS di Indonesia dikenal sebagai *Indonesia Deposit Insurance Corporation* (IDIC). LPS adalah sebuah institusi yang didirikan berdasarkan Undang-Undang Nomor 24 Tahun 2004 tentang Lembaga Penjamin Simpanan (UU LPS), yang telah diamandemen oleh Undang-Undang Nomor 7 Tahun 2009. Sejak berlakunya di 22 September 2005, implementasi LPS menandai pergeseran signifikan dari kebijakan jaminan pemerintah sebelumnya antara tahun 1998 hingga 2005.

Meskipun awalnya kebijakan tersebut memberikan kepercayaan, kebijakan ini memberatkan keuangan publik dan menimbulkan kekhawatiran, yang berujung pada penghentian kebijakan tersebut. LPS muncul sebagai respon untuk memastikan perlindungan asuransi simpanan, menjaga kepercayaan dalam sektor perbankan dan mengelola risiko.

Dampak nyata dari LPS adalah pengalihan dari jaminan umum ke jaminan terbatas. Pasal 11 UU LPS menetapkan jaminan maksimum sebesar IDR 100 juta untuk setiap simpanan di bank oleh nasabah. Hal ini sejalan dengan praktik internasional yang terlihat di 72 negara, termasuk negara yang ekonominya tergolong maju. Transisi ke jaminan terbatas mengimbangi kepercayaan deposan dan mitigasi risiko sistemik, memperkuat ketahanan sistem perbankan terhadap fluktuasi pasar.fluctuations.

Bryant Junevan, *bryant.mulia@shinewing.id*

Fungsi dan Otoritas LPS

LPS beroperasi dengan fungsi dan otoritas khusus untuk menjaga kepentingan nasabah dan berkontribusi pada stabilitas sistem perbankan. Peran utama LPS adalah menjamin keamanan simpanan nasabah dan menjaga stabilitas keseluruhan sistem perbankan. LPS merumuskan kebijakan asuransi simpanan, melaksanakan proses asuransi, dan membentuk kebijakan stabilitas sistem perbankan. Selain itu, otoritas LPS meliputi berbagai aspek, mulai dari menentukan premi asuransi hingga melakukan inisiatif kesadaran asuransi simpanan.

Pelaporan SCV: PLPS No. 5 Tahun 2019

Dalam ranah regulasi perbankan, Peraturan LPS (PLPS) No. 5 Tahun 2019 memiliki posisi penting, khususnya dalam Pasal 3 dan Pasal 10. Regulasi ini membahas hal penting pelaporan data jaminan simpanan berbasis nasabah, yang disebut sebagai Single Customer View (SCV).

Pasal 3

(1) Bank wajib memiliki dan mempertahankan:
   a. Data Mentah *(Raw Data);*
   b. Data Rinci SCV Per Nasabah *(SCV Detail Data Per Customer);*
   c. Data SCV Per Nasabah *(SCV Data Per Customer);* dan
   d. Data Ringkasan SCV Per Bank *(Summary Data SCV Per Bank).*

(2) Bank bertanggung jawab atas kebenaran data sebagaimana dimaksud pada ayat (1) sesuai dengan ketentuan peraturan perundang-undangan di bidang perbankan.

Pasal 10

(1) Audit internal Bank harus melakukan pemeriksaan atas kualitas data dan keandalan sistem yang digunakan dalam pengolahan dan penyimpanan data sebagaimana dimaksud dalam Pasal 3 ayat (1)
(2) Pemeriksaan sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun
(3) Selain dilakukan oleh audit internal Bank, pemeriksaan terhadap keandalan sistem sebagaimana dimaksud pada ayat (1) juga dilakukan oleh pihak eksternal yang independen sesuai dengan ketentuan peraturan perundang-undagan, paling sedikit 1 (satu) kali dalam 3 (tiga) tahun.

- **Data Mentah *(Raw Data)***
  Data mentah yang ditetapkan oleh Bank Indonesia, Otoritas Jasa Keuangan (OJK), dan LPS yang memberikan informasi nasabah yang dilaporkan melalui portal Pelaporan Terintegrasi, di antara lain, digunakan sebagai dasar untuk menyusun SCV. Data ini disampaikan setiap bulan.
- **Data SCV Per Nasabah *(SCV Data Per Customer)***
  Data yang berisi setidaknya total nilai simpanan yang dikategorikan sesuai dengan Total Program Jaminan LPS. Data ini disampaikan setiap tahun untuk posisi pada akhir tahun.
- **Data Rinci SCV Per Nasabah *(SCV Data Per Customer)***
  a. Kepemilikan tabungan, pinjaman, atau setara dengan simpanan atau pinjaman; dan
  b. Nilai Simpanan yang dikategorikan sesuai dengan ketentuan Program Jaminan LPS untuk Simpanan Nasabah yang bersangkutan.
- **Data Ringkasan *(Summary Data)***
  Data Ringkasan dari SCV Per Bank adalah data yang paling jarang digunakan untuk menghitung jumlah nasabah dan simpanan sesuai dengan kategori data SCV per nasabah. Data ini disampaikan setiap bulan untuk posisi pada akhir bulan.

Kerangka regulasi ini mengungkap kompleksitas dan tanggung jawab yang terkait dengan pelaporan data jaminan simpanan berbasis nasabah bagi bank komersial. Regulasi ini memperkenalkan kepada kita kategori nasabah yang berbeda, yaitu Kategori 1, Kategori 2 dan Kategori 3. Kategori-kategori ini menentukan bagaimana data simpanan nasabah dikelola. Kategori 1 mencakup nasabah yang data-datanya dicatat dengan cermat oleh bank dan tidak menimbulkan risiko terhadap stabilitasnya. Sebaliknya, Kategori 2 mengacu pada nasabah yang data-datanya tidak tercatat oleh bank, dan mereka mungkin dapat menciptakan lingkungan perbankan yang tidak sehat. Kategori 3 mencakup nasabah di luar dua kategori sebelumnya.

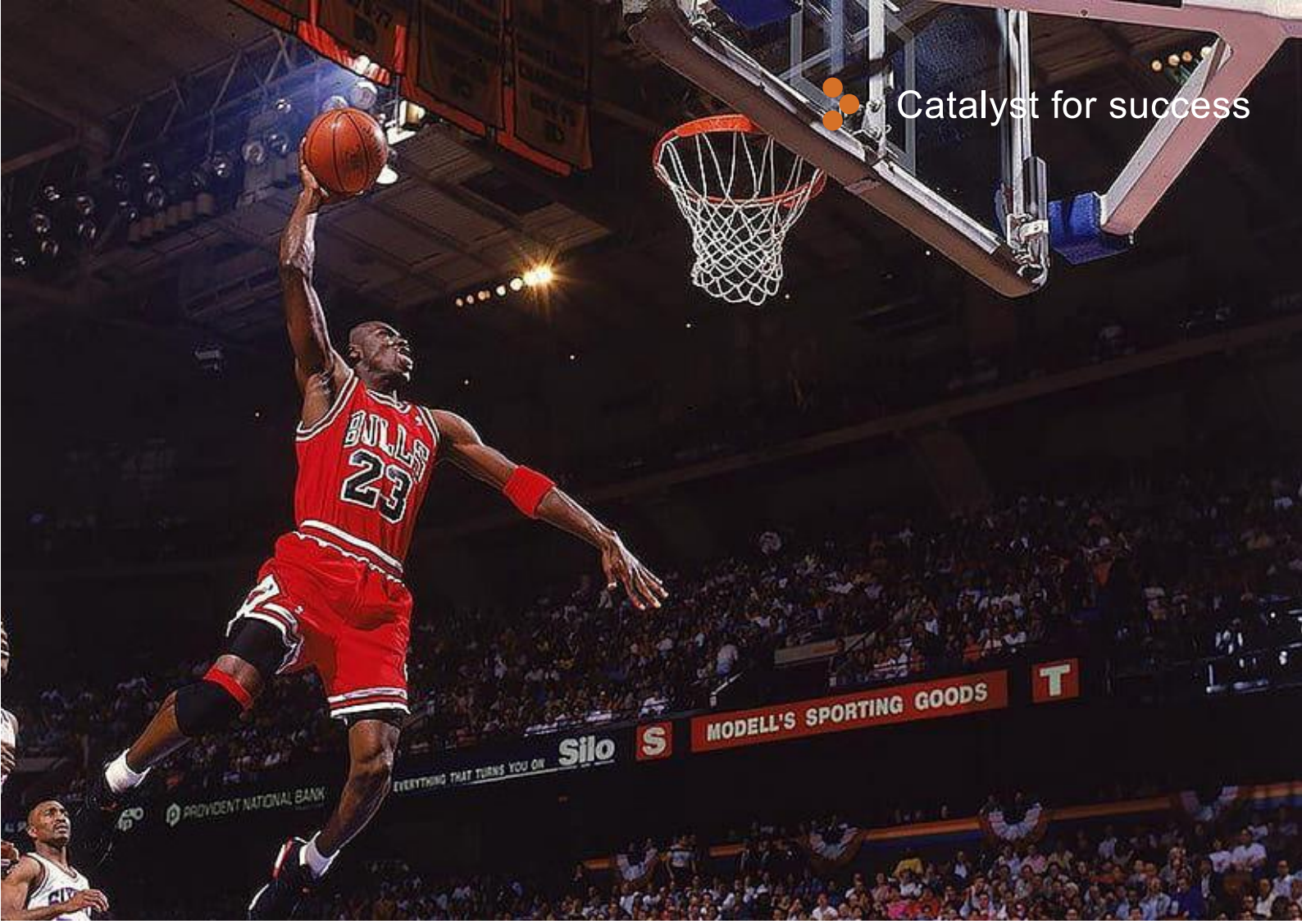
Salah satu komponen kunci dari kerangka ini adalah konsep Single Customer View (SCV), yang merupakan tampilan terpadu dari hubungan keuangan nasabah dengan bank. Pentingnya data SCV dan kehandalan sistem pemrosesan data sangat terasa dalam konteks Pemeriksaan IT untuk perusahaan perbankan, terutama dalam memastikan kepatuhan regulasi LPS. Regulasi seperti Peraturan LPS (PLPS) No. 5 Tahun 2019, menegaskan pentingnya pelaporan data SCV yang akurat dan integritas sistem pemrosesan data.

Peran Pemeriksaan IT

Peran pemeriksaan IT sangat penting dalam mencapai tujuan ini. Pemeriksaan IT memainkan peran penting dalam memastikan kepatuhan perusahaan perbankan terhadap regulasi LPS, khususnya dalam hal pelaporan data SCV. Melalui tinjauan dan penilaian yang ketat, Auditor IT memverifikasi akurasi, kerahasiaan dan keandalan data SCV. Kepatuhan ini tidak hanya menjaga standar hukum tetapi juga mengurangi risiko yang terkait dengan ketidakakuratan.

Selain itu, Pemeriksaan IT penting untuk menjaga integritas dan kerahasiaan data. Mengingat sifat yang sensitif dari data SCV yang mencakup informasi pelanggan dan rincian keuangan, mengevaluasi langkah-langkah kerahasiaan sepanjang siklus data. Ini juga memastikan integritas data dari pengumpulan hingga pelaporan, sejalan dengan tujuan LPS. Selain itu, Pemeriksaan IT memperkuat ketahanan operasional dengan memeriksa infrastruktur IT, kekuatan sistem dan keamanan. Pendekatan ini meminimalkan risiko, meningkatkan kepatuhan, dan menciptakan lingkungan aman yang sejalan dengan regulasi LPS.

Melalui evaluasi dan verifikasi yang teliti, Pemeriksaan IT meningkatkan kepatuhan, kerahasiaan, integritas, dan ketersediaan data SCV. Pada akhirnya meningkatkan ketahanan operasional dan berkontribusi pada strategi mitigasi risiko yang efektif bagi bank. Pengalaman pemegang CISA di SW Indonesia telah banyak membuktikan efektivitas Pemeriksaan IT tersebut.



Pemeriksaan IT Terhadap Bursa Kripto di Indonesia

Secara terminologi *cryptocurrency* (mata uang kripto) berasal dari dua kata, kriptografi dan mata uang. Dilansir dari Investopedia.com, mata uang kripto adalah mata uang digital berbasis kriptografi dalam sebuah jaringan yang terdistribusi di antara komputer dalam jumlah yang besar. Kriptografi merupakan sistem pengaman yang membuat mata uang kripto aman dari masalah pemalsuan dan penggunaan ganda *(double spending).*

Sebagian besar mata uang kripto dibangun dengan menggunakan teknologi *blockchain.* Teknologi *blockchain* memungkinkan berbagai entitas untuk menyimpan, mencatat, dan memverifikasi transaksi dalam sebuah buku kas besar *(ledger)* secara transparan dan aman dalam sistem yang terdesentralisasi tanpa adanya campur tangan pihak ketiga. Teknologi *blockchain* inilah yang menjadi dasar teknologi mata uang kripto terbesar, Bitcoin.

Bitcoin merupakan mata uang kripto generasi pertama yang menuai kesuksesan. Bitcoin lahir pada tahun 2009 tepat setahun setelah krisis keuangan global. Pada mulanya, banyak pihak yang skeptis dan menyangsikan kemampuan bitcoin untuk bertahan. Namun sampai saat ini, ketahanan jaringan bitcoin dinilai sangat baik dan tidak pernah sekalipun mengalami peretasan. Hal ini tidak terlepas dari jaringan bitcoin yang dibangun dari banyak *nodes.*

Nodes adalah jaringan komputer yang mengoperasikan jaringan bitcoin. Nodes saling terhubung dan berkomunikasi untuk membangun dan memperbarui blockchain database. Peretasan pada sebuah nodes tidak akan mengakibatkan gangguan pada keseluruhan jaringan dikarenakan nodes lain akan segera menyingkirkan nodes yang teretas dari keseluruhan jaringan.

Terlepas dari teknologi yang revolusioner, kelahiran mata uang kripto membawa disrupsi teknologi di bidang keuangan. Pertumbuhan penggunaan mata uang kripto dunia secara eksponensial menjadi peluang tumbuhnya berbagai bursa kripto. Pada akhir tahun 2022, FTX, bursa kripto terbesar ke-2 di dunia, mengalami kehancuran. Sam Bankman-Fried (SBF), pemilik bursa FTX yang digadang-gadang menjadi The Next Warren Buffet, kehilangan seluruh kekayaannya yang bernilai US$ 16 milyar dalam 24 jam.

FTX diduga melakukan penyalahgunaan dana nasabah. Melalui Alameda Research, anak perusahaan FTX, perusahaan mengalirkan dana nasabah yang digunakan untuk berbagai aktivitas seperti dana kampanye, dana sosial, dan *trading.* FTX melakukan praktik *fractional reserve* sehingga ketika ada penarikan dana dalam jumlah besar FTX tidak mampu mengembalikan dana nasabah.

Kejadian ini mendorong berbagai otoritas keuangan dunia untuk melakukan pengawasan terhadap bursa kripto. Bursa kripto terbesar di Indonesia, Indodax, telah melakukan verifikasi Penerapan Prosedur yang Disepakati Bersama (AUP) atas Proof of Reserve (PoR) dan Perhitungan Kecukupan Likuiditas Perusahaan. Langkah ini dilakukan untuk meningkatkan rasa aman bagi nasabah dalam melakukan transaksi.

Peraturan Bappebti No 4 Tahun 2023 telah memberikan sejumlah pengaturan kerangka kerja bagi bursa kripto. Dalam Peraturan Bappebti No 4 Tahun 2023 diatur bahwa Calon Pedagang Fisik Aset Kripto wajib menempatkan seluruh dana nasabah pada Lembaga Kliring Berjangka dalam rekening yang secara khusus dipergunakan untuk memfasilitasi penempatan dana dan penyelesaian transaksi Pasar Fisik Aset Kripto. Penyediaan fasilitas jual beli, sistem perdagangan online wajib diperiksa atau diaudit oleh lembaga independen yang memiliki kompetensi di bidang sistem informasi. Selain itu, Calon Pedagang Fisik Aset Kripto wajib melaporkan seluruh wallet yang dikelola sebelum melakukan pendaftaran sebagai Calon Pedagang Fisik Aset Kripto.

Untuk mendukung kegiatan operasional, Calon Pedagang Fisik Aset Kripto diwajibkan melampirkan kontrak kerja dengan pegawai yang memiliki sertifikat Certified Information System Security Professional (CISSP) dan Certified Information System Auditor (CISA) pada saat melakukan pendaftaran ke Bappebti. SW Indonesia terbiasa diminta untuk membantu Calon Pedagang Fisik Aset Kripto dalam rangka kepatuhan terhadap aturan dan kerangka kerja yang diberikan regulator.

Melalui UU PPSK No 4 Tahun 2023, peraturan mengenai kripto di Indonesia akan mengalami perubahan yang cukup signifikan dengan peralihan kewenangan pengawasan dari Bappebti ke OJK. Selanjutnya OJK akan melakukan pengawasan di sektor keuangan secara menyeluruh, mulai dari perbankan, pasar modal, dana pensiun, asuransi, tekfin, kripto, hingga koperasi. Transisi peralihan kewenangan pengawasan ini akan memerlukan waktu antara 6 bulan hingga 2 tahun. Dalam masa transisi ini diharapkan Calon Pedagang Fisik Aset Kripto mempersiapkan kepatuhan terhadap peraturan yang berlaku.

Pemerintah Indonesia sendiri telah meluncurkan bursa kripto pada 17 Juli 2023 sesuai dengan Keputusan Kepala Bappebti Nomor 01/BAPPEBTI/SP-BBAK/07/2023 yang bernama Commodity Future Exchange (CFX) yang berada di bawah PT Bursa Komoditi Nusantara. Pemerintah Indonesia melalui kementerian perdagangan berharap dengan adanya bursa kripto dalam negeri dapat meningkatkan jumlah transaksi kripto dan menciptakan ekosistem transaksi yang aman bagi nasabah. Pemeriksaan IT oleh pemegang CISA menjadi salah satu alternatif menciptakan rasa aman nasabah atau investor di bursa kripto.

SW INDONESIA

Catalyst for success

CONSULT WITH OUR EXPERIENCE TAX CONSULTANT

OUR SERVICES ARE THE ANSWER TO YOUR TAX CASES

Supports The Wider Financial Services Industry

Connect with us

SW Indonesia @shinewing.indonesia sw-indonesia.com

KAP Suharli, Sugiharto & Rekan | SW Tax Consulting | SW Business Advisory | SW Business Process Outsourcing

审计师层面的信息技术一般控制：程序及益处

随着信息系统（系统和软件）的发展和所使用硬件的技术进步，公司内部的信息技术（IT）环境已经发生了显著变化。此外，国际组织标准（美国反虚假财务报告委员会（COSO）、（国际信息系统审计协会）ISACA、国际标准化组织（ISO））关于信息安全框架的内容也发生了实质性变化。在这种情况下，了解信息技术一般控制（ITGC）（也称一般信息技术控制）变得至关重要。

IT环境的重大和持续变化会导致访问风险增加，并对财务报告产生影响。财务数据（财务报告的来源）存储在数据库等系统中，其功能是确保数据的访问和处理。授予/获得的用户访问权限会影响数据保护，包括以下Shiva密码身份验证协议(SPAP 315, A64)：

a. **身份验证控制：**确保访问IT环境内应用程序或其他方面的用户拥有适当的凭证。
b. **授权控制：**允许用户根据其工作职责和适当的职责分工访问所需信息。
c. **对配置、撤销和修改访问权限的控制：**授权新用户和更改现有用户访问权限，包括解约（辞职）后取消用户访问权限。
d. **特权访问权限控制：**允许具有管理员（超级管理员）访问权限或具有高级或特殊访问权限的用户进行系统或应用程序的管理。
e. **用户访问审查控制：**重新认证或评估用户访问的持续授权。
f. **安全配置控制：**大多数技术都有关键配置的设置，有助于限制访问，防止潜在数据丢失以及防止在需要时无法访问数据。
g. **物理访问控制：**对数据中心、硬件或其他IT资产的物理访问。

按照国际审计与鉴证准则理事会（IAASB）在《国际审计准则第315号》（ISA 315）（2019年修订版）中的规定，审计师必须通过建议的ITGC框架来了解客户的IT环境，并重点关注数据安全。审计师将评估风险，并运用专业判断来确定IT环境中的风险因素以及减轻风险的适当控制措施。。

ITGC是什么?

ITGC包括为了确保数据保密性、完整性和可用性，某一组织管理（控制）IT系统运行所使用的政策和程序。ITGC涵盖IT的方方面面，包括软件实施、用户账户创建和数据管理。

ITGC可分为以下几个大类，包括：

1 **一般IT管理控制，包括IT系统管理和监督、**长期IT战略规划和IT风险评估。一般IT管理控制还包括IT安全控制。
2. **访问控制，**包括防止未授权访问和数据操纵的各种方法。访问控制还包括用户身份验证、数据加密、账户锁定和审计跟踪。
3. **系统发展生命周期（SDLC）控制，**包括系统开发、测试、实施和维护。系统发展生命周期控制还包括文档、审批、变更跟踪和绩效评估。
4. **程序变更控制，**包括管理程序和系统配置变更。程序变更控制还包括影响分析、回归测试、职责分离和活动日志记录。
5. **物理硬件和数据中心安全控制，**包括物理环境（硬件）受到外部和内部威胁（包括损坏、电力中断和自然灾害）时采取的安全措施。数据中心物理安全控制包括门锁和窗锁、警报和闭路监控（CCTV）系统、烟雾和火灾探测系统以及空调系统。
6. **备份和系统/数据恢复控制，**包括数据的定期复制和备份（备份和恢复），以便在数据丢失或损坏时能够迅速恢复。备份和系统/数据恢复控制还包括备份时间安排、备份介质的安全存储、例行恢复测试和灾难恢复计划（DRP）。
7. **计算机运行控制，**包括IT系统的高效和有效运行。计算机运行控制还包括系统性能监测、技术问题解决、容量和可用性管理以及事故报告（帮助台）。

ITGC为何重要?

ITGC的重要性在于：其能帮助公司确保业务流程和财务报告中所使用信息系统的有效性和合规性。ITGC不仅可以提高信息系统所产生数据、程序和输出结果的安全性和完整性，还能防止未授权访问、数据泄露和运行中断。另外，ITGC还可以降低错误、操纵或滥用信息技术的风险，以防对公司的业绩和声誉造成负面影响。有效的ITGC可以提高财务报告的可靠性和准确性，并有助于降低舞弊风险。ITGC要求满足适用的审计标准和法规。

ITGC审查的执行方、执行时间及益处

理想状态下，应由独立的外部机构定期进行ITGC审查或评估，至少每年一次（建议在一般审计之前进行）或根据公司面临的风险情况按需开展。因为ITGC审查和评估于公司有益，所以必须开展且由独立的外部机构进行，益处包括：

a. 在利益相关方、监管机构、审计师和客户之间就公司所用信息系统的质量和合规性建立信任和信誉。
b. 从具有IT审计能力和经验的外部机构获得客观、专业的意见和建议。
c. 识别ITGC实施过程中的薄弱环节、风险和改进机会，并建议采取适当的纠正和预防措施。
d. 符合适用的审计准则和规定，如SOX合规性要求公司定期评估ITGC的有效性。

外部独立机构开展ITGC评估的方式

计划

现场工作

报告和建议

独立机构通常会选择信永中和的数字化转型和网络信任服务对其客户进行ITGC评估，原因如下：

1. 深厚的专业知识有助于我们了解控制系统和风险的复杂性。
2. 相关性和最新知识确保我们的服务符合最新的国际技术和审计准则。
3. 由ITGC成功实施的数据和事实构成的结果具有可衡量性，提供可衡量的结果将是我们服务的一部分，能够产生实际影响。
4. 在改进层面提供支持，不仅注重ITGC评估，还注重对客户控制系统的改进和强化措施提供建议。

银行业的信息技术一般控制审计：程序及益处

随着数字化时代的不断发展，信息技术（IT）已成为包括银行业在内的许多行业的运营支柱。从基本交易到复杂的数据分析，现代银行均依靠强大可靠的IT系统来支持其运营。因此，银行必须对其IT基础设施采取强有力的控制措施，而信息技术一般控制（ITGC）在其中发挥着重要作用。ITGC是使银行有信心可靠驾驭数字环境的力量支柱。

ITGC是指设计用于确保IT系统和数据的完整性、可靠性和安全性的一套程序和政策，包括访问控制、变更控制、运行控制和系统开发管理等诸多方面。

ITGC对银行业的重要性

银行业是一个受严厉的法律法规高度监管的行业，对安全性和准确性的要求很高。同时，银行业也是网络攻击的目标，因此IT安全是头等大事。随着电子交易的持续增长，网络安全威胁日益凸显。客户数据或财务信息泄露或被盗可能会损害银行声誉，造成重大经济损失。

此外，银行业要求运行效率以期能够迅速准确地开展交易。银行如不具备有效的信息技术一般控制，可能遭遇交易流程受阻、报告出错甚至经济损失等问题。

ITGC由几个关键组成部分构成，银行机构需要了解这些组成部分，才能安全高效地开展业务：

- 访问控制：确保只有经过授权的人员才能访问系统和数据，包括身份认证、授权和审计追踪。
- 变更控制：监控系统和应用程序的变更，确保所有更改在实施前都经过测试和批准。
- 运行控制：确保日常业务顺利开展，包括数据备份、灾难恢复和日常维护。
- 系统开发管理：监控新系统或现有系统更新的开发、测试和实施过程。

ITGC在银行业的实施

ITGC在银行业的实施过程包括一系列严谨有序的步骤：

- **访问控制**：银行必须确保客户数据和金融交易等敏感信息只能由授权方访问，可以通过实施多因素身份认证、访问控制政策、入侵检测系统以及日志和监控机制来实现。访问日志和系统监控也可用于检测可疑活动。
- **变更控制**：IT系统中的每项变更均应在实施前进行记录、测试和批准，以防止发生错误导致运行中断或造成安全漏洞。
- **运行控制**：包括备份和恢复政策、硬件维护、系统性能监控和灾难恢复程序，以确保运行连续性。
- **系统开发管理**：监控从初始系统开发到发布的整个过程，确保深入分析所有代码和基础设施的潜在风险。应严格管理需求分析、设计和测试等流程，以确保质量和安全性。

银行业ITGC审计的常见问题及改进建议

ITGC审计通常发现的常见问题包括：

- **访问控制存在薄弱环节**：许多银行在系统和数据访问控制层面存在薄弱环节。授予的访问权限可能与个人岗位不符，导致潜在安全风险。为减少这种风险，银行需要完善访问控制政策及其实施措施，并为员工提供关于信息安全重要性的培训。
- **缺乏变更控制**：一些银行没有完全采用变更控制原则，因此导致了错误或中断。对系统进行更改后未进行充分的测试，从而增加了出现漏洞的风险。为此，银行需要实施变更跟踪体系，并在每次实施变更前召开审查会议。所有变更都应记录在案，在受控环境中进行测试，并在应用前先获得批准。
- **维护不足或疏于日常维护**：过时或维护不善的IT基础设施很容易受到攻击。此外，定期维护往往被忽视，导致了潜在的运行故障。因此，银行需要安排日常维护并定期升级系统。
- **备份和恢复失败**：有时，银行缺乏适当的灾难恢复程序。许多银行虽然有此类方案，但可能长时间没有对其进行测试或更新。为此，银行需要制定全面的灾难恢复方案，并定期测试以确保其有效性。

银行业的这些ITGC问题可能与利息计算、贷款处理、交易记录等核心交易功能有关。因ITGC不足而导致的一些进一步的问题可能包括：

- **利息计算不准确**：银行系统的逻辑或配置可能存在错误，导致客户账户的利息计算不准确。
- **贷款处理中的错误**：系统可能无法正确处理贷款申请，或者在贷款审批自动化方面存在缺陷，导致授信不符合标准。
- **交易授权不当**：交易在执行前可能不需要适当的授权或验证，从而增加了出错或滥用的风险。
- **未能遵守数据隐私政策**：系统可能不符合数据隐私政策，这可能会对银行声誉造成负面影响或导致巨额罚款。
- **交易错误**：交易处理过程中可能会出现错误，如重复转账或交易与客户指示不符。

在应对这些情况时，管理层的积极参与至关重要。管理层必须支持IT团队，了解相关风险，分配必要的资源，以降低相关风险，并向整个组织传达合规和控制的重要性。管理层的认知和投入将有助于确保风险缓解的成功和可持续。通过识别和缓解ITGC问题，辅以管理层的积极支持，银行可以强化其IT基础设施，提高客户信任度，并确保运营的平稳和安全。

ITGC是维护银行业安全性、完善性和运营效率的关键因素。通过有效实施和维护ITGC，银行可以降低安全风险，增强客户信任，确保运营顺畅。对ITGC进行定期评估可以让银行找出需要改进之处。管理层要对审计结果采取后续行动，提出改进建议和举措。

此外，印度尼西亚金融服务监管局(OJK)也出台了关于商业银行实施信息技术的第11/POJK.03/2022号POJK银行业法规（特别是第55条第（2）款），该法规要求银行至少每三年一次利用独立的外部服务对信息技术实施情况的内部审计职能进行重新评估。信永中和印尼所可以为印度尼西亚银行业公司提供专业服务，拥有多年经验。我们不断拓展自身能力，可以为银行业客户在ITGC审计服务、对信息技术实施情况的内部审计职能的重新评估、网络安全等服务方面提供支持。

银行业公司的IT审查：印度尼西亚存款保险公司法

银行所处的行业规章制度繁多，业务流程涉及复杂的信息技术(IT)。信息技术是开展银行业务活动、改善客户体验和提高运营效率的基础。信息技术和数字技术的变革给维护安全、遵守法规和管理风险带来了挑战。银行业的IT审查至关重要，并受到印度尼西亚存款保险公司(IDIC，或称LPS)法规的监管。

储蓄保险和LPS的重要作用

在金融安全领域，存款保险机构目前在建立信任和维护经济稳定方面发挥着非常重要的作用。LPS在印度尼西亚是指印度尼西亚存款保险公司。LPS是根据关于存款保险公司的2004年第24号法律（《印度尼西亚存款保险公司法》）成立的机构，2009年第7号法律对该法规进行了修订。自2005年9月22日颁布以来，《印度尼西亚存款保险公司法》的实施标志着上届政府在1998至2005年间担保政策的重大转变。

这一政策最初给人们带来了信心，但也给公共财政带来了负担，并引起了人们的担忧，导致该政策最终终止。LPS的出现是为了确保存款保险的保护作用、维持对银行业的信任及管理风险。

LPS的真正影响是从一般担保向有限担保的转变。《印度尼西亚存款保险公司法》第11条规定，客户在银行每笔存款的最高担保额为1亿印尼盾。这符合在72个国家践行的国际惯例，包括经济发达的国家。向有限担保的过渡可以平衡存款人的信心，降低系统性风险，增强银行系统抵御市场波动的能力。

Bryant Junevan, *bryant.mulia@shinewing.id*

LPS的职能和权限

LPS具有特定的职能和权限，旨在保障存款人的利益，并帮助维护银行系统的稳定。LPS的主要作用是保证客户存款安全，同时维护银行系统的整体稳定。LPS负责制定存款保险政策，执行保险程序，并制定银行系统稳定政策。此外，LPS的权限还涉及确定保险费和开展存款保险宣传活动等多个方面。

SCV报告：PLPS 2019年第5号

在银行监管领域，2019年第5号LPS法规（PLPS）具有重要地位，特别是与第3条和第10条有关。该法规解决了基于客户的存款担保数据报告的迫切问题，即为单一客户视图（SCV）。

第3条

(1) 银行必须拥有并维护：
   1）原始数据；
   2）每个客户的 SCV 详细数据；
   3）每个客户的 SCV 数据；以及
   4）每个银行的 SCV 数据汇总
(2) 银行应根据银行业法律法规的规定，对第（1）段所述数据的正确性负责。

第10条

(1) 银行内部审查必须对第3条第（1）段所述数据的质量以及用于处理和保存数据的系统的可靠性进行审查。
(2) 第（1）段所述的审查必须至少每1（一）年进行一次。
(3) 除了银行内部审查外，第（1）段所述的系统可靠性审查还必须由独立的外部方根据法律法规进行，至少每三（3）年进行一次。

- **原始数据**
  由印度尼西亚银行、Otoritas Jasa Keuangan（OJK）和LPS（通过综合报告门户网站报告客户信息）提供的原始数据作为编制SCV的基础。数据每月提交一次。
- **每个客户的SCV数据**
  至少包含根据LPS担保计划总额分类的存款总额的数据。该数据每年提交一次，截至当年年底。
- **每个客户的SCV详细数据**
  a. 拥有储蓄、贷款或相当于存款或贷款的资产；以及
  b. 根据相关客户存款的LPS担保计划条款分类的存款价值。
- **数据汇总**
  每家银行SCV数据汇总是最常用的数据，用于按照每名客户SCV数据类别计算客户数量和存款。该数据每月提交一次，截至当月月底。

这一监管框架揭示了商业银行报告以客户为基础的存款保险数据的复杂性和相关责任。该法规向我们介绍了不同的客户类别，即第1类、第2类和第3类。这些类别决定了客户存款数据的管理方式。第1类包括银行仔细记录的数据且其不会对银行稳定构成风险的客户。相比之下，第2类客户的数据未被银行记录，他们可能会造成不健康的银行环境。第3类包括前两类以外的客户。

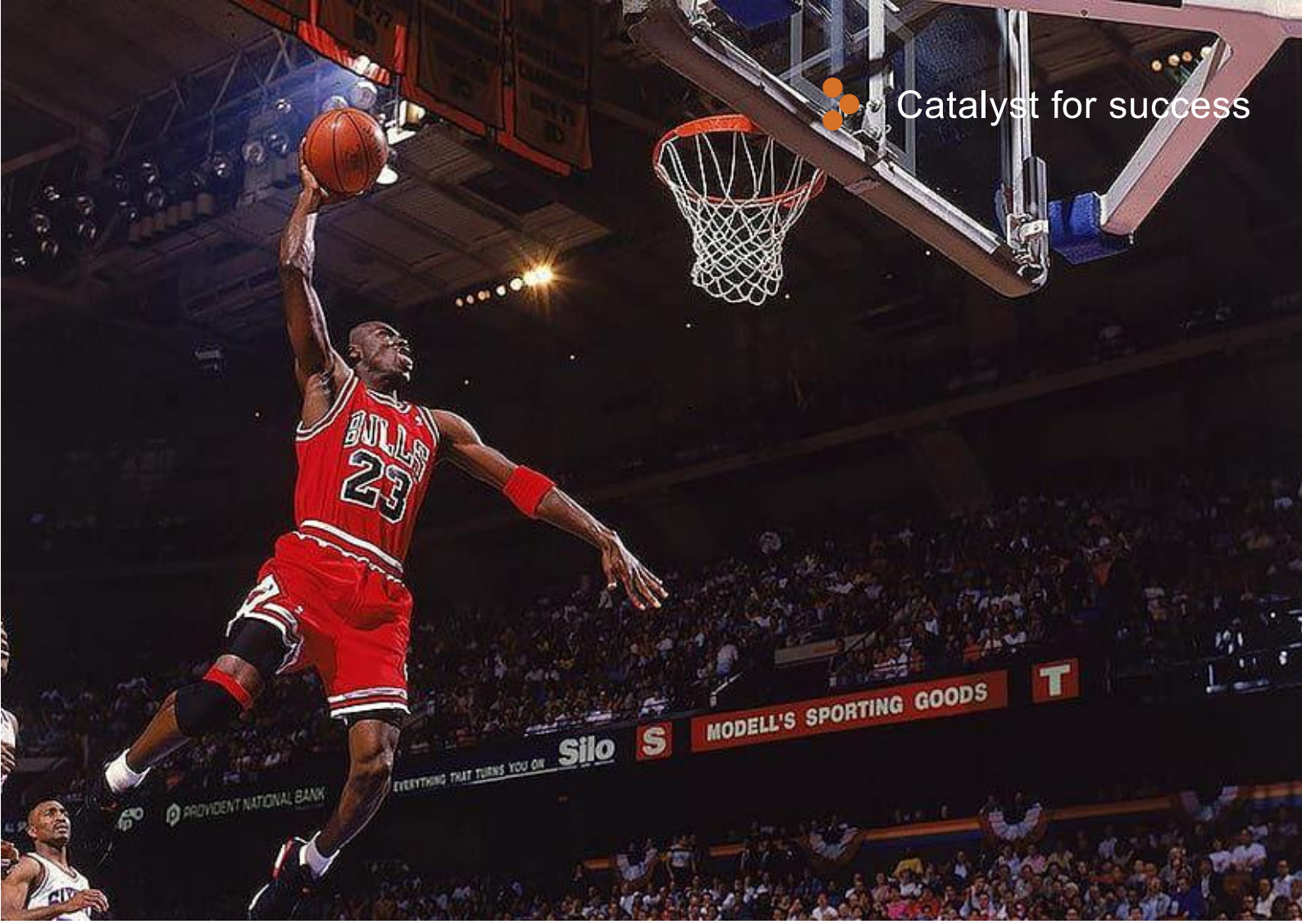
该框架的关键组成部分之一是单一客户视图（SCV）概念，即客户与银行财务关系的综合视图。SCV数据和数据处理系统的可靠性在银行的IT审查中，尤其是在确保遵守LPS法规方面，显得尤为重要。LPS法规（PLPS）2019 年第5号等法规强调了准确报告SCV数据和数据处理系统完整性的重要性。

IT审查的作用

有效的IT审查对于实现这些目标至关重要。IT审查在确保银行业遵守LPS法规，特别是 SCV数据报告方面起着至关重要的作用。通过严格审查和评估操作，IT审查员可验证SCV数据的准确性、保密性和可靠性。这种合规性不仅能维护法律标准，还能降低与不准确性相关的风险。

此外，IT审查对于维护数据完整性和保密性至关重要。由于SCV数据的敏感性，其包括客户信息和财务细节，因此审查要评估数据整个周期的保密措施。IT审查还能确保从收集到报告的数据完整性，与LPS目标保持一致。此外，IT审查还通过审查IT基础设施、系统稳健性和安全性来增强运营韧性。这种方法最大限度地降低了风险，提高了合规性，并营造了一个符合LPS法规的安全环境。

通过严格的评估和验证，IT审查提高了SCV数据的合规性、保密性、完整性和可用性。最终提高运营韧性，并为银行制定有效的风险缓解策略做出贡献。印度尼西亚西南部CISA持有人的经验证明了IT审查的有效性。



印度尼西亚加密货币交易所信息技术审查

从术语上讲，加密货币一词起源于加密技术和货币这两个词。据Investopedia网站报道，加密货币是一种基于大规模计算机间分布式网络加密技术的数字货币。加密技术是一个安全体系，它可以避免加密货币的伪造和重复消费问题。

大多数加密货币都是利用区块链技术构建的。区块链技术允许各类实体在无第三方参与的情况下，于去中心化系统中透明且安全地存储、记录和验证分类账中的交易。这种区块链技术是最大的加密货币比特币的基础。

比特币是取得成功的第一代加密货币。它诞生于2009年，恰好是全球金融危机之后的一年。起初，很多人怀疑，甚至质疑过比特币的生存能力。然而，时至今日，比特币网络的恢复能力仍被视为出色，且从未被黑客入侵过。部分原因是比特币网络建立在许多节点上。

节点是运行比特币网络的计算机网络。节点相互连接并进行通信，以建立和更新区块链数据库。由于其他节点会迅速将被入侵的节点从整个网络中删除，因此，黑客入侵一个节点不会破坏整个网络。

尽管这项技术是革命性的，但加密货币的出现给金融行业带来了技术上的颠覆。全球加密货币使用量呈指数级增长，这使得各种加密货币交易所涌现。2022年底，全球第二大加密货币交易所FTX崩盘。被吹捧为“下一个沃伦·巴菲特”的FTX交易所老板山姆·班克曼-弗里德（Sam Bankman-Fried，简称SBF），在24小时内失去了他160亿美元的全部身家。

FTX涉嫌滥用客户资金。该公司通过其子公司Alameda Research将客户资金挪用于竞选资金、社会基金、交易等各种活动。鉴于FTX实行部分准备金制度，因此当出现大额提款时，FTX无法返还客户资金。

这一事件促使全球各金融官方机构对加密货币交易所进行监管。印度尼西亚最大的加密货币交易所Indodax已经执行对储备证明（PoR）和流动性资产充足率核算进行联合商定程序（AUP）验证。采取这一措施是为了增强客户在进行交易时的信心。

印度尼西亚商品期货交易监管机构（Bappebti）2023年第4号法规为加密货币交易所提供了框架。该法规明确要求，潜在实体加密资产交易商必须将所有客户资金存入期货清算机构的账户，该账户专门用于方便资金的存储和实体加密资产市场交易的结算。买卖设施和在线交易系统的准备金必须经过具有信息系统专业知识的独立机构进行审查或审计。此外，潜在实体加密资产交易商在注册之前，所有管理的钱包必须进行报告。

为支持经营活动，潜在实体加密资产交易商在印度尼西亚商品期货交易监管机构注册时，必须提供与持有注册信息系统安全师 (CISSP) 和注册信息系统审计师 (CISA) 证书的员工签订的雇佣合同。信永中和印度尼西亚所经常应邀协助潜在实体加密资产交易商遵守监管机构颁布的法规和框架。

根据2023年关于加密货币的第4号法规，印度尼西亚的加密货币法规将发生重大变化，监管机构将从印度尼西亚商品期货交易监管机构过渡为印尼金融服务监管局（OJK）。随后，印尼金融服务监管局将监管整个金融行业，包括银行业、资本市场、养老基金、保险业、金融科技、加密货币和合作社。过渡监督机构预计需要6个月到2年的时间。过渡期内，潜在实体加密资产交易商应针对适用法规做好合规准备。

根据01/BAPPEBTI/SP-BBAK/07/2023号印度尼西亚商品期货交易监管机构总部决议，印度尼西亚政府自身于2023年7月17日创办了一家加密货币交易所，取名为商品期货交易所（CFX），原名为PT Bursa Komoditi Nusantara。印度尼西亚政府希望通过贸易部，国内加密货币交易所能够提升加密货币交易量，并为客户创建一个安全的交易生态系统。信息技术审查由注册信息系统审计师持有者进行，这已成为加密货币交易所为客户或投资者创造安全感的替代方案之一。

SCAN BARCODE

Life at SW INDONESIA

TERUS MELAJU UNTUK INDONESIA MAJU

SW INDONESIA

FUN MATCH

PING PONG

11 August

DIRGAHAYU REPUBLIK INDONESIA

SW AGUSTUSAN

SW INDONESIA

TERUS MELAJU UNTUK INDONESIA MAJU

DIRGAHAYU REPUBLIK INDONESIA

SW AGUSTUSAN

FUN GAMES SW TANGERANG.

11 August

Catalyst for success

SW INDONESIA

TERUS MELAJU UNTUK INDONESIA MAJU

DIRGAHAYU REPUBLIK INDONESIA

SW AGUSTUSAN

FUN GAMES SW JAKARTA

11 August

Catalyst for success

SW INDONESIA

TERUS MELAJU UNTUK INDONESIA MAJU

DIRGAHAYU REPUBLIK INDONESIA

SW AGUSTUSAN

FUN GAMES SW SURABAYA

11 August

Catalyst for success

TERUS MELAJU UNTUK INDONESIA MAJU

SW INDONESIA

FUN MATCH

BADMINTON

12 August

DIRGAHAYU REPUBLIK INDONESIA

SW AGUSTUSAN

TERUS MELAJU UNTUK INDONESIA MAJU

SW INDONESIA

FUN MATCH

FUTSAL

12 August

DIRGAHAYU REPUBLIK INDONESIA

SW AGUSTUSAN

TERUS MELAJU UNTUK INDONESIA MAJU

SW INDONESIA

FUN MATCH FUTSAL

12 August

DIRGAHAYU REPUBLIK INDONESIA

SW AGUSTUSAN

SW

Catalyst for success

Asia-Pacific Business Hub

Even in uncertain times, you can rely on our market knowledge to help you take the lead.

Supporting the wider financial services industry

- Audit and other assurance
- Tax and custom consulting
- Deal and business advisory
- Digital transformation and cybertrust
- Licensing and legal counsel

www.sw-indonesia.com

TANGERANG	Unity Building 3rd Floor Jl. Boulevard Gading Serpong M5/21 15810	T. (+6221) 22220200
JAKARTA	UOB Plaza 34th Floor Jl. MH Thamrin Kav.8-10, Jakarta Pusat 10230	T. (+6221) 29932172
SURABAYA	Spazio Building 5th Floor Jl. Mayjen Yono Suwoyo Kav.3, Surabaya 60226	T. (+6231) 99141222
BALI	Benoa Square 2nd Floor Jl. Bypass Ngurah Rai No. 21A, Kuta, Bali 80361	T. (+62361) 200 3298

APPROVED EMPLOYER ACCA
Trainee Development - Platinum

ICAEW AUTHORISED TRAINING EMPLOYER

CPA AUSTRALIA

RECOGNISED EMPLOYER PARTNER