THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

WAKE UP CALL

Bringing you the updated news from **RSM Indonesia**

QUARTER I – 2025

Welcome to issue 72 of Wake Up Call
RSM Indonesia newsletter covering topics on audit, tax and consulting.

IN THIS ISSUE:

40 YEARS OF EXCELLENCE & PARTNERSHIP
1985 – 2025
RSM INDONESIA

RSM INDONESIA ANNIVERSARY

CELEBRATING 40 YEARS OF THE AAJ SPIRIT AND THE RSM STRENGTH

4 March 1985 – 4 March 2025

This year marks a proud milestone in our journey – **RSM Indonesia's 40th anniversary**. From our beginnings as AAJ Associates in 1985 to becoming part of the global RSM network, our story has been one of transformation, resilience, and shared success.

Founded in 1985 as **AAJ Associates**, we've grow through decades of transformation to become part of the global **RSM** network. Along the way, we've remained true to our purpose: delivering quality, insight, and impact for our clients, our people, and our communities.

Our anniversary theme, **"RSM Indonesia: Celebrating 40 Years of AAJ Legacy — A National Pride with Global Strength"**, honors our Indonesian roots while reflecting our unwavering commitment to global excellence.

This legacy would not be possible without the people who shaped it:

To our clients: thank you for your trust, collaboration, and continued partnership. Your success drives everything we do.

To our people: your passion, integrity, and dedication have brought us here. This achievement belongs to you.

As we celebrate this milestone, we look ahead with optimism–committed to growing stronger, staying connected, and always delivering more.

Here's to the next chapter–together.

Leveraging Data Analytics for Operational Excellence of Smart Hospitals

MUHAMMAD HAVIZ, TECHNOLOGY CONSULTING PRACTICE

Big Data Analytics (BDA) is transforming the healthcare sector by driving efficiency, reducing operational costs, and improving patient outcomes. The integration of Artificial Intelligence (AI), Internet of Things (IoT), and predictive analytics allows hospitals to optimize decision-making, allocate resources effectively, and adopt a patient-centered approach. As healthcare systems become more data-driven, hospitals must embrace these technologies to stay competitive and ensure high-quality care.

Historically, hospital management relied on manual processes and fragmented data systems, leading to inefficiencies and increased costs. Today, smart hospitals use AI-powered analytics, IoT-enabled devices, and real-time data insights to streamline operations and improve patient care. BDA enables healthcare providers to shift from reactive treatment to proactive healthcare management, ensuring better patient experiences and financial stability.

Key Pillars of Data-Driven Smart Hospitals

AI-powered decision support systems are transforming clinical decision-making by enhancing accuracy and speed. Predictive analytics help forecast potential health complications, allowing for early intervention that can save lives. AI also plays a crucial role in automating administrative processes, optimizing scheduling, billing, and claims processing, thereby reducing the burden on hospital staff and improving efficiency.

The integration of IoT and connected medical devices further enhances hospital operations. Remote patient monitoring improves chronic disease management and enables early detection of health issues before they escalate. Smart beds and wearable devices contribute to patient safety by continuously tracking vital signs and alerting healthcare professionals in case of abnormalities. IoT-enabled medical device support seamless data exchange between healthcare providers, ensuring comprehensive and coordinated care.

Predictive analytics is a vital component of smart hospitals, enabling efficient hospital operations. By analyzing patient data, hospitals can reduce readmissions by identifying high-risk patients before complications arise. AI-driven inventory management optimizes supply chain efficiency, ensuring that critical medical supplies are available when needed. Workforce allocation also benefits from predictive analytics, allowing hospitals to deploy staff more effectively, reducing burnout, and maintaining high levels of patient care.

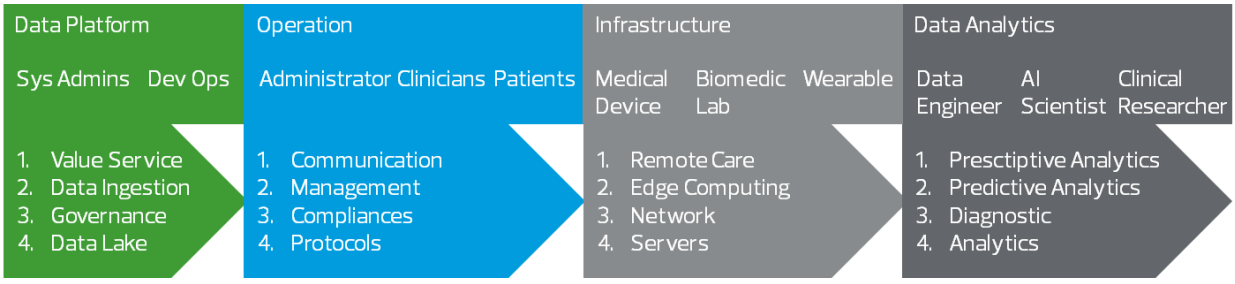


Figure 1: Cycle of Transformation of Data Driven Smart Hospital

Cybersecurity and data governance are critical considerations as hospitals become increasingly interconnected. Strengthening patient data security through advanced encryption and authentication protocols ensures compliance with regulatory frameworks such as HIPAA and GDPR. AI-powered cybersecurity systems enhance real-time threat detection and mitigation, protecting sensitive patient information from cyber threats and ensuring the integrity of healthcare operations.

Several hospitals worldwide have successfully implemented BDA to improve their operations and patient care. Paris hospitals, for instance, use AI-driven patient flow optimization to predict emergency department visits, reducing congestion and wait times. In Singapore, IoT-enabled smart wards leverage sensor technology to monitor patient movements, minimizing fall risks and enhancing real-time care. AI-based sepsis detection systems have significantly lowered mortality rates by enabling early intervention and improving treatment outcomes.

Challenges and Considerations

Despite the numerous benefits of BDA, hospitals face several challenges in adopting these technologies. The BDA is called big, at least in three aspects, there are the Volume of the data, Velocity of data streams, and Variety of all types of format. All of the above aspect if its not regulate carefully will introduce the organization into several challenges that stated in Figure 2. One of the most difficult is the integration.

Integration with legacy systems remains a key barrier, as outdated IT infrastructure makes seamless adoption of analytics difficult. The cost of implementing AI-driven systems is another challenge, requiring hospitals to justify the initial investment with measurable benefits. Workforce training and adaptation also play a crucial role in the successful implementation of BDA. Ensuring that hospital staff are adequately trained to use AI-powered tools and analytics platforms is essential for maximizing the potential of these technologies.

Figure 2: Challenges in Big Data Analytics

Call to Action

To fully leverage Big Data Analytics, hospitals must evaluate their existing data strategies, collaborate with technology partners, and foster a data-driven culture. A phased approach to implementing BDA will facilitate smoother integration and long-term sustainability. By developing clear strategies for data utilization, investing in scalable AI solutions, and prioritizing cybersecurity, hospitals can ensure a seamless transition toward becoming smart healthcare facilities.

The future of hospital management is driven by AI, IoT, and predictive analytics. Healthcare institutions that invest in data analytics will achieve superior efficiency, cost reduction, and improved patient care. Now is the time for hospital executives to embrace digital transformation and position their organizations at the forefront of smart healthcare innovation.

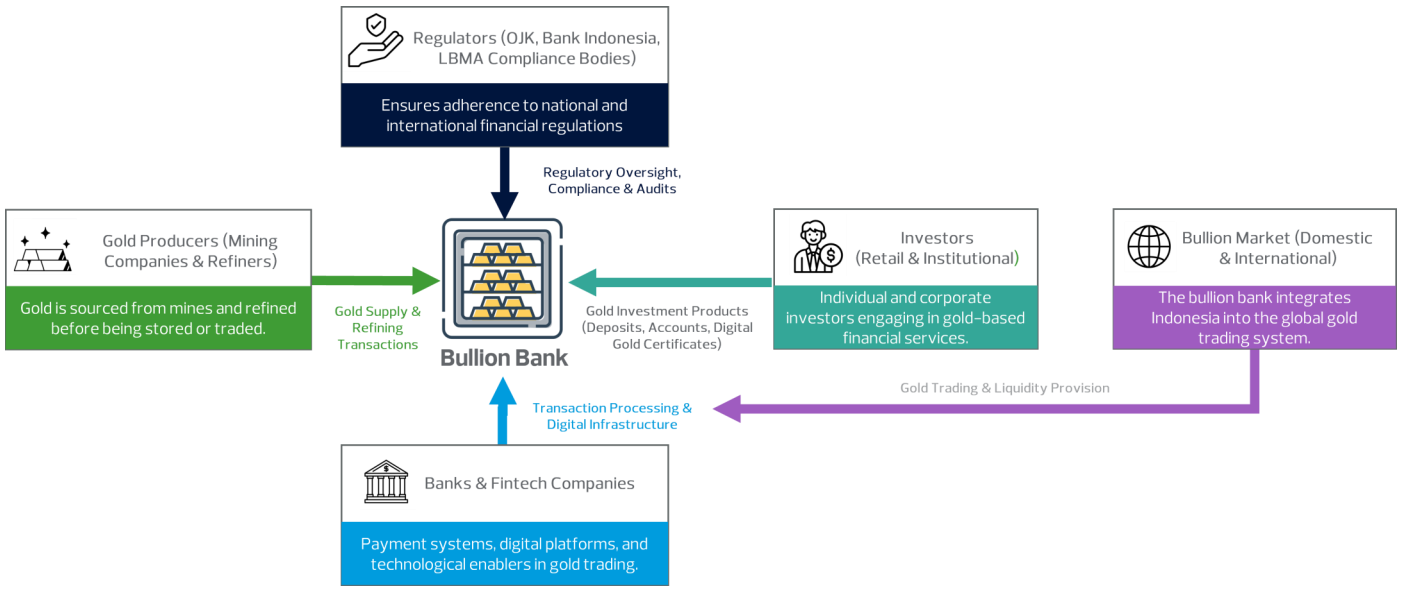
RSM can help hospitals navigate this transition by providing tailored data analytics solutions, advanced AI-driven decision support, and seamless integration with existing hospital systems. With expertise in predictive analytics, IoT implementation, and cybersecurity, RSM ensures that healthcare organizations maximize their return on investment while enhancing patient care. By partnering with RSM, hospitals can accelerate their journey towards becoming fully digital, data-driven institutions, ensuring long-term sustainability and competitive advantage in an evolving healthcare landscape.

For further information, please contact : **inquiry@rsm.id**

Building Indonesia's Bullion Bank: A Technology-Driven Approach to Gold Finance

RESDY BENYAMIN, TECHNOLOGY CONSULTING PRACTICE

Indonesia, as one of the world's largest gold producers, contributes approximately 4% of the global supply. However, inefficiencies in the domestic bullion trade continue to hinder its full potential. Dependence on international intermediaries, high transaction costs, and regulatory gaps limit the country's ability to fully capitalize on its bullion reserves. To address these challenges, the Indonesian government is exploring the establishment of a bullion bank to facilitate storage, trading, and financing activities. This initiative mirrors global trends, where bullion banking services enhance market efficiency, transparency, and accessibility in the precious metals sector.

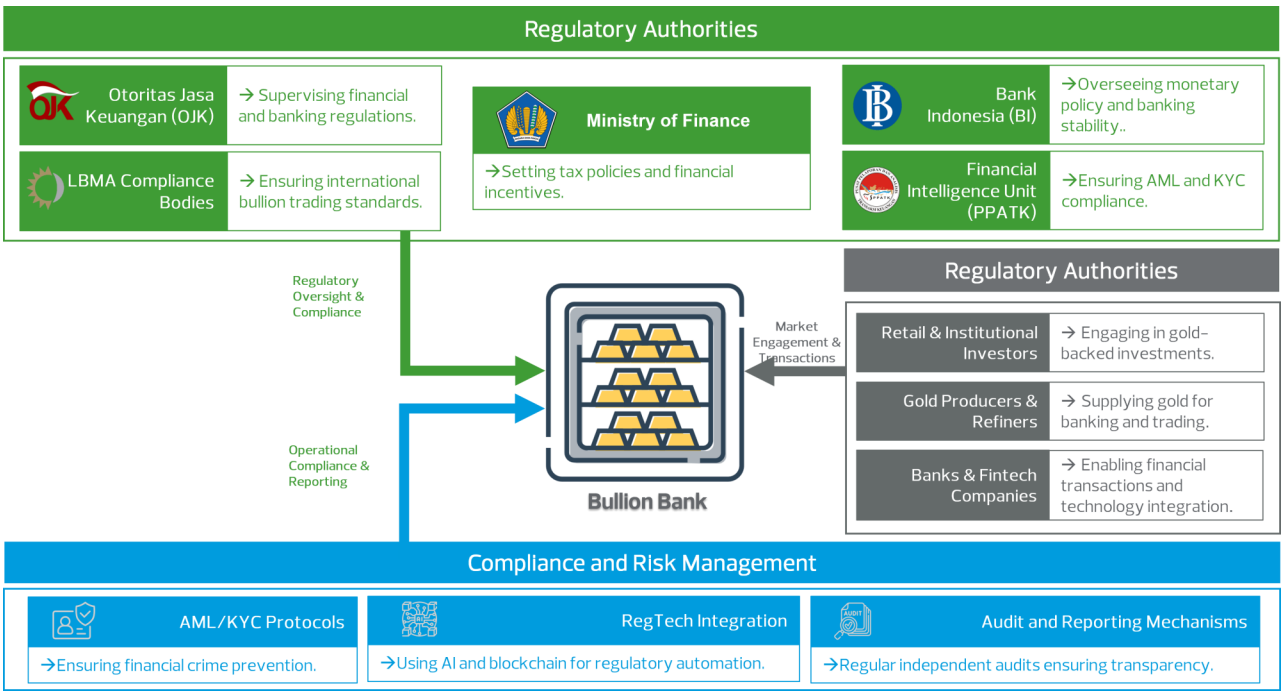


A bullion bank would create a structured domestic gold market, reducing reliance on foreign trading hubs while ensuring transactions comply with London Bullion Market Association (LBMA) standards. Enhanced liquidity and transparency would promote financial inclusion, allowing broader participation in gold markets. By certifying and processing bullion domestically, Indonesia could capture more value from its gold production, reducing raw exports and strengthening its global market position.

Regulatory Framework and Governance

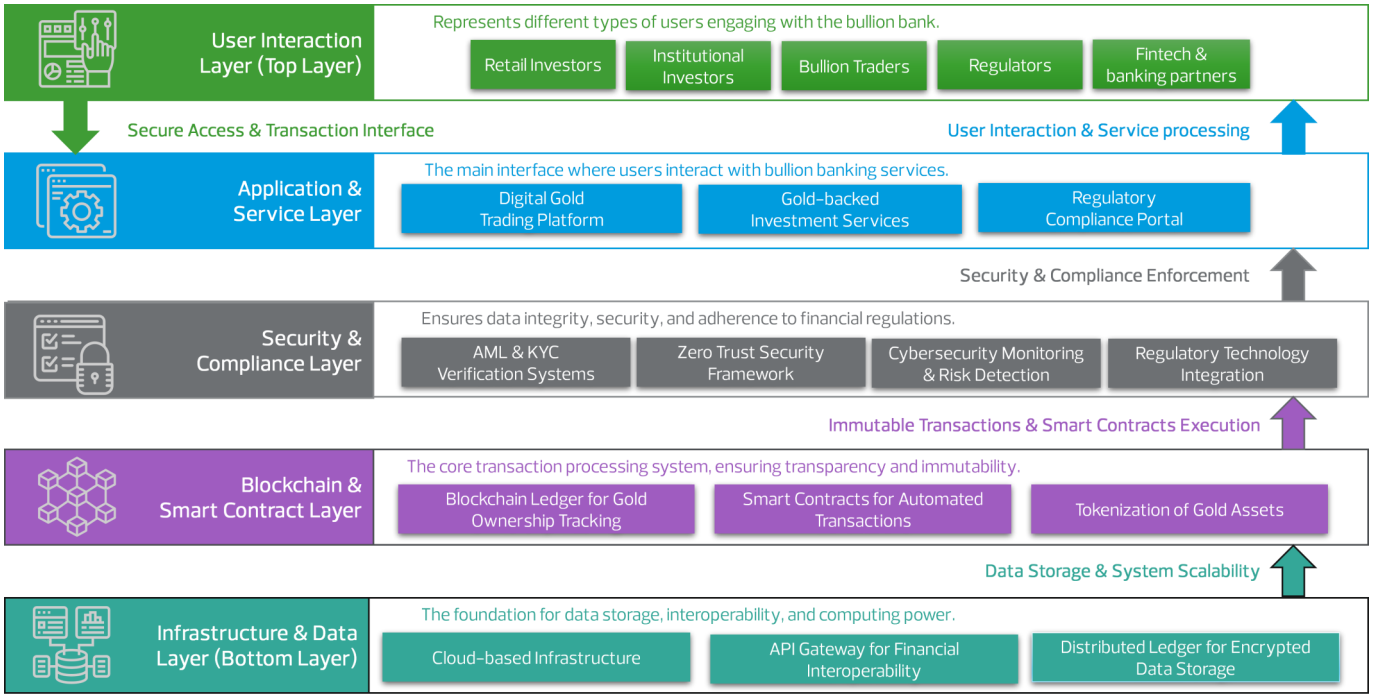
A well-defined regulatory framework is fundamental to ensuring the stability and security of a bullion bank. Supervision by Otoritas Jasa Keuangan (OJK) and Bank Indonesia (BI) would ensure investor protection and transaction integrity. Tax policies and investment incentives should be structured to attract capital while maintaining a fair and competitive market environment.

Adopting *LBMA Good Delivery standards* would enhance credibility, allowing Indonesia's bullion market to integrate with global financial systems. Additionally, *Regulatory Technology* (RegTech) could automate compliance monitoring, reducing risks related to fraud and financial crime. Independent audits would reinforce transparency, strengthening investor confidence in bullion banking operations.



Technology Adoption and Security Considerations

The success of a bullion bank hinges on cutting-edge technology integration. Blockchain technology would ensure transparency by maintaining immutable ownership records, mitigating risks of fraud and counterfeiting. Artificial intelligence (AI) and machine learning could strengthen risk management by detecting suspicious transactions in real time and ensuring adherence to anti-money laundering (AML) and know-your-customer (KYC) regulations.

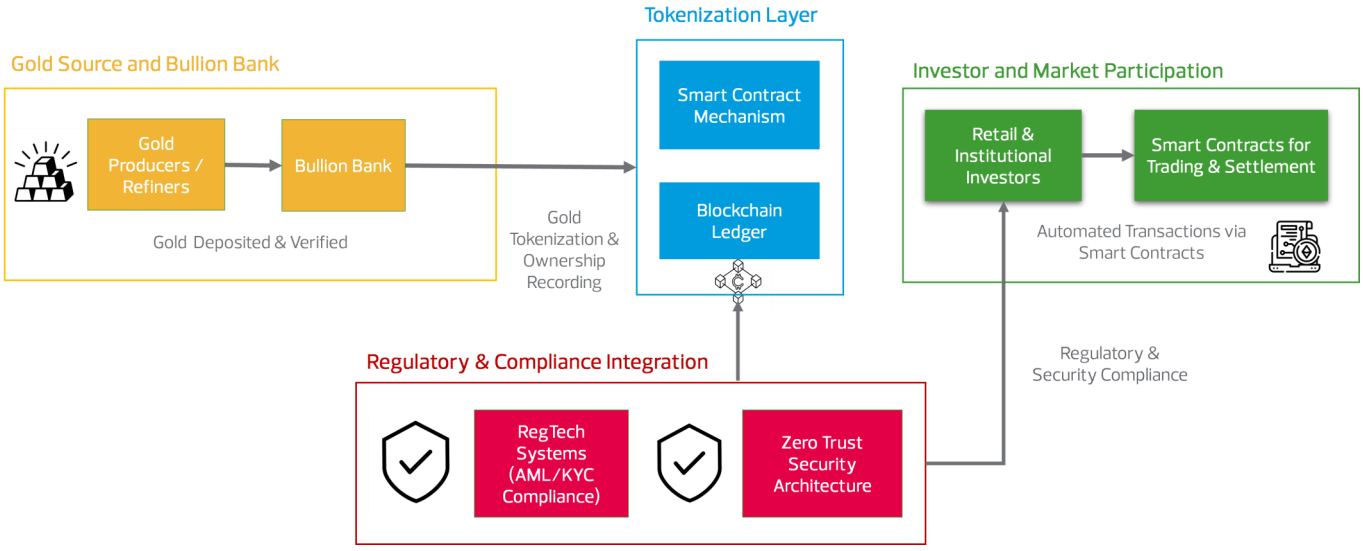


Given the high-value assets involved, cybersecurity must be a top priority. A Zero Trust Architecture would restrict system access to verified users, preventing unauthorized transactions. Distributed ledger technology would enable encrypted storage solutions, safeguarding customer information and bolstering trust in digital bullion transactions.

Technological Infrastructure and Digital Integration

A bullion bank's technological infrastructure must support advanced security, seamless transactions, and market accessibility. Digital platforms would facilitate real-time trading, secure storage, and bullion-linked financial transactions. Blockchain-based tokenization of gold assets would allow fractional ownership, broadening investor participation and enhancing liquidity.

Smart contracts would automate trade settlements, collateralized lending, and interest calculations on gold-backed financial products, improving efficiency and reducing operational risks. AI-driven analytics would enhance fraud detection, anomaly tracking, and regulatory compliance, ensuring secure and compliant transactions.



Cybersecurity must be a priority in digital bullion banking operations. The implementation of Zero Trust Architecture (ZTA) would enforce strict access controls, while distributed ledger technology would secure digital assets and protect against cyber threats.

Interoperability between banking institutions, fintech companies, and regulatory agencies will be critical for a well-functioning bullion banking ecosystem. An API-driven financial framework would facilitate seamless data sharing, compliance tracking, and transaction validation, reinforcing Indonesia's role as a competitive global bullion hub.

As financial technology evolves, adopting a cloud-based infrastructure would ensure scalability, cost-effectiveness, and enhanced disaster recovery capabilities. Cloud solutions would enable real-time market data access, supporting informed decision-making for investors, regulators, and financial institutions alike.

Short-Term (1-2 years):
Foundation & Regulatory Setup

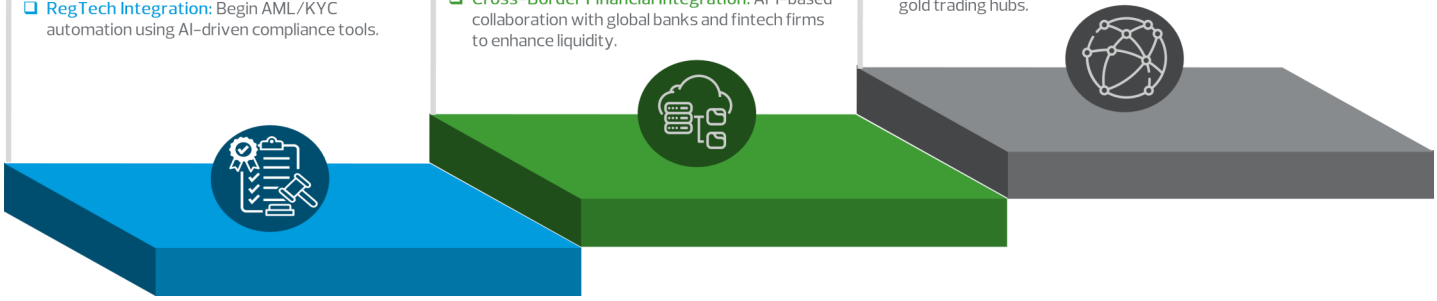
- ❑ Regulatory Framework Development: Establish legal and compliance structures with OJK, BI, and global regulators (LBMA).
- ❑ Licensing and Approval: Secure operational licensing for the bullion bank.
- ❑ Pilot Projects for Digital Gold Trading: Launch test platforms for tokenized gold transactions using blockchain.
- ❑ RegTech Integration: Begin AML/KYC automation using AI-driven compliance tools.

Medium-Term (3-5 years):
Infrastructure & Expansion

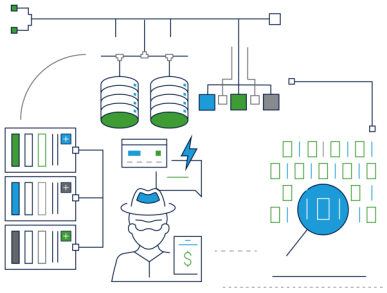
- ❑ Digital Trading Platform Development: Full-scale rollout of gold-backed digital investment products.
- ❑ Storage & Security Enhancements: Expansion of digital and physical bullion storage with cybersecurity reinforcements.
- ❑ Smart Contract Automation: Deploy smart contracts for trade settlement and collateralized lending.
- ❑ Cross-Border Financial Integration: API-based collaboration with global banks and fintech firms to enhance liquidity.

Long-Term (5+ years):
Global Integration & Market Leadership

- ❑ Full Integration with the Global Financial System: Position Indonesia as a bullion banking hub in Southeast Asia.
- ❑ Expansion of Tokenized Gold Products: Introduce fractional ownership and smart contract-based gold derivatives.
- ❑ Adoption of AI-driven Trading Strategies: Implement machine learning for real-time market predictions and automated gold portfolio management.
- ❑ Global Bullion Market Recognition: Secure stronger integration with LBMA and international gold trading hubs.



CONCLUSION



The establishment of a bullion bank in Indonesia represents a transformative opportunity to modernize the country's gold market, expand financial accessibility, and strengthen economic resilience. By leveraging blockchain, AI, and RegTech solutions, the bullion bank can offer a secure, transparent, and efficient ecosystem for gold transactions. These innovations would not only streamline domestic gold trading but also elevate Indonesia's position as a key player in the global bullion financial system.

To realize this vision, it is imperative that government and regulatory bodies implement clear, adaptive policies that foster responsible market participation while ensuring security and compliance with international standards. Strengthening interoperability between financial institutions, fintech players, and regulatory agencies will be crucial in creating a seamless and trusted bullion banking ecosystem. Furthermore, by embracing tokenization and smart contract automation, the system can offer innovative investment products that enhance liquidity and financial inclusion.

For further information, please contact : **inquiry@rsm.id**

NEWSFLASH

We are happy to announce that
our Technology Risk Consulting Partner,
ERIKMAN D PARDAMEAN,
has been elected to serve as
Secretary of ISACA Indonesia Chapter,
beginning in 2025 and ending in 2027.

Ministerial Decree SK-275: Strengthening Cybersecurity for Indonesia's SOEs

ERIKMAN D PARDAMEAN, TECHNOLOGY RISK CONSULTING PRACTICE

THE GROWING CYBERSECURITY THREAT TO STATE-OWNED ENTERPRISES

With rapid digital transformation, Indonesia's State-Owned Enterprises (SOEs) are increasingly vulnerable to cyber threats. Critical sectors like finance, energy, and telecommunications store vast amounts of sensitive data, making them prime targets for cyberattacks. The rise of ransomware, data breaches, and other cyber incidents highlights the need for a strong cybersecurity framework to protect national assets.

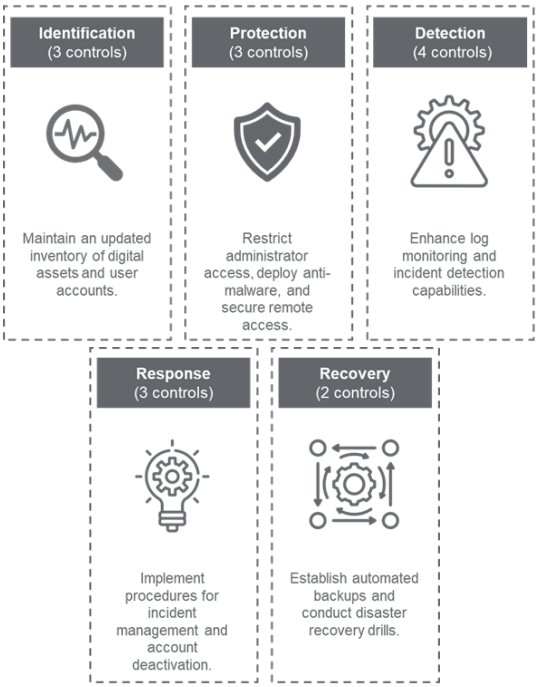
To address this, the Minister of SOEs has issued Decree SK-275/MBU/11/2024, mandating SOEs to implement cybersecurity measures that strengthen resilience and safeguard operations.

Key Directives of Ministerial Decree SK-275

The new regulation sets forth clear cybersecurity mandates for SOEs:

1. Implementation of 15 Essential Cybersecurity Controls

SOEs must integrate these controls across five key areas:



These controls ensure a layered defense against cyber threats and minimize operational disruptions.

2. Adoption of International Cybersecurity Standards

SOEs are encouraged to align security frameworks with internationally recognized standards, including:

- ISO 27001 (Information Security Management System)
- NIST Cybersecurity Framework (National Institute of Standards and Technology)
- CIS Controls (Center for Internet Security Best Practices)

Following these standards helps SOEs benchmark security maturity and apply best practices.

3. Risk Assessment for Non-Implemented Controls

If certain security measures cannot be immediately implemented, SOEs must conduct risk assessments covering:

- Risk Appetite: Define acceptable risk levels.
- Risk Treatment Plans: Outline mitigation, transfer, or acceptance strategies.
- Risk Mitigation: Implement countermeasures to reduce cyber threats.

This ensures security strategies align with each SOE's operational structure while maintaining compliance.

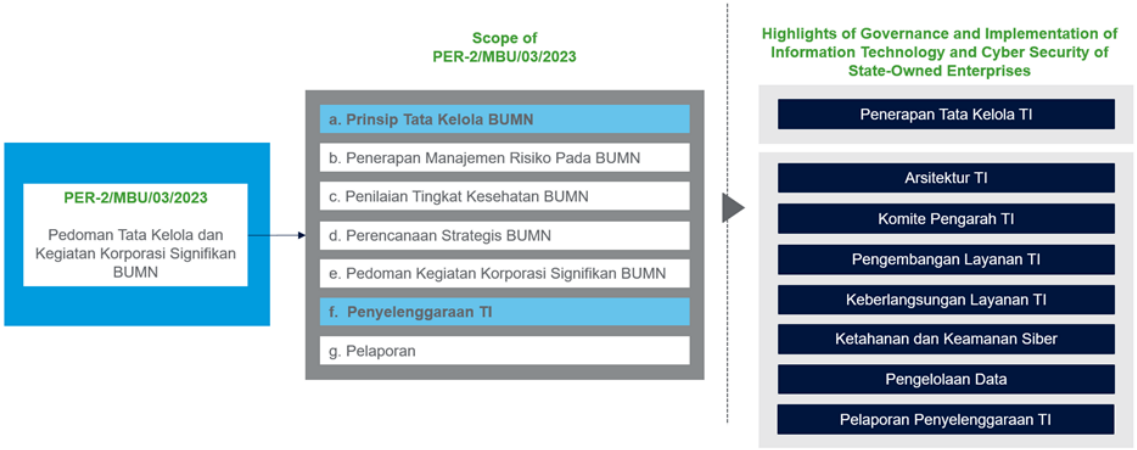
4. Strengthening Cyber Resilience Through Collaboration

The decree highlights:

- Cross-SOE Collaboration: Sharing threat intelligence and best practices.
- Annual Cybersecurity Reporting: Mandatory submission of security reports.
- Advanced Security Technologies: Encouraging tools like Security Information & Event Management (SIEM), Privileged Access Management (PAM), and Endpoint Detection & Response (EDR/XDR) solutions.

Integration with PER-2/MBU/03/2023: A Governance Perspective

Ministerial Decree PER-2/MBU/03/2023 establishes governance principles for SOEs, covering corporate governance, risk management, and IT governance. This regulation aims to ensure structured risk management, transparency, and regulatory compliance, particularly in IT governance, which directly aligns with SK-275's cybersecurity mandates.



Key alignments between PER-2/MBU/03/2023 and SK-275 include:

- Corporate Governance & Cybersecurity Integration: PER-2 mandates the establishment of governance structures, while SK-275 specifies how cybersecurity should be embedded into those structures.
- IT Risk Management: PER-2 emphasizes IT risk management as a critical corporate function, supporting SK-275's risk assessment requirement for cybersecurity controls.
- Compliance with International Standards: PER-2 sets broad IT governance policies, while SK-275 translates these into actionable controls aligned with ISO 27001 and NIST CSF.

By ensuring cybersecurity is embedded within broader corporate governance policies, these regulations collectively enhance SOEs' resilience against evolving cyber threats.

Implications for SOEs

While compliance requires investment, it also presents opportunities. Key takeaways include:

- Cybersecurity as a Business Priority: Not just a compliance requirement but a fundamental risk management function.
- Investment in Cybersecurity Talent & Infrastructure: Building a skilled workforce and modernizing security infrastructure.
- Leveraging AI & Automation: Enhancing detection, incident response, and risk management with cutting-edge technology.
- Compliance as a Competitive Advantage: SOEs that implement these measures will lead in cybersecurity governance and stakeholder confidence.

Conclusion: Enhancing Cyber Resilience to Meet Regulatory Expectations

Ministerial Decree SK-275 is a pivotal step in strengthening cybersecurity for SOEs. To achieve compliance and long-term resilience, organizations should focus on:

- Cyber Risk Assessments & Gap Analysis: Identifying vulnerabilities and ensuring alignment with regulations.
- Implementing Global Cybersecurity Standards: Strengthening security posture with ISO 27001 and NIST frameworks.
- Incident Response & Crisis Management: Establishing robust mechanisms for rapid threat detection and response.
- Security Governance & Compliance Advisory: Developing policies that support long-term resilience.
- Penetration Testing & Threat Intelligence: Simulating cyber threats to uncover vulnerabilities.
- Employee Training & Awareness Programs: Fostering a cybersecurity-conscious culture.

By adopting these approaches, SOEs can not only meet regulatory requirements and build a resilient cybersecurity framework that protects national assets and business continuity.

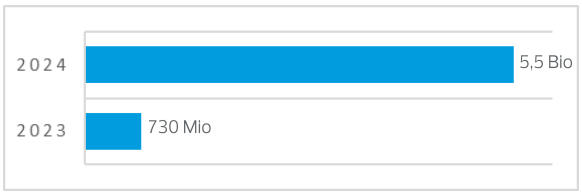
For further information,
please contact : **inquiry@rsm.id**

Why ISO/IEC 27701 is the Cornerstone of Effective Privacy Management

ERIKMAN D PARDAMEAN & SATRIO B PANDOWO, TECHNOLOGY RISK CONSULTING PRACTICE

With rising data breaches and stricter privacy laws, organizations can no longer ignore privacy.

Increase by **8 times** Compare to 2023



Graphic 1.0: Global Breached Accounts in 2024

Source: https://surfshark.com/research/study/data-breach-recap-2024

The surge in Personally Identifiable Information (PII) processing and evolving regulations like Indonesia's UU PDP (UU No. 27/2022), European's GDPR, and US-California's CCPA demand a proactive approach. ISO/IEC 27701:2019 extends security frameworks into robust Privacy Information Management Systems (PIMS), helping organizations ensure compliance, build trust, and mitigate risks in a data-driven world.

What is ISO/IEC 27701?

ISO/IEC 27701 is a critical extension of ISO/IEC 27001, enhancing its security-focused framework with privacy-specific controls. While ISO 27001 ensures data confidentiality, integrity, and availability (CIA principles), ISO 27701 builds upon this by incorporating privacy governance, making it ideal for organizations processing Personally Identifiable Information (PII). In the Indonesian context, ISO 27701 aligns closely with the Personal Data Protection (PDP) Law (UU No. 27/2022), providing a structured approach to compliance. Specifically, it helps businesses define roles as PII controllers or processors, establish lawful bases for data processing, implement data minimization and retention policies, and strengthen governance mechanisms (all key requirements under PDP Law).

The key clauses of ISO 27701 include:

- Clause 5: PIMS-specific requirements related to ISO 27001 – Expands upon the requirements of an Information Security Management System (ISMS) to incorporate privacy controls.
- Clause 6: PIMS-specific guidance related to ISO 27002 – Provides detailed privacy-related security controls.
- Clause 7: Additional guidance for Personally Identifiable Information (PII) controllers – Defines responsibilities for organizations acting as data controllers.
- Clause 8: Additional guidance for PII processors – Specifies privacy management requirements for organizations processing data on behalf of others.

Why ISO/IEC 27701 is Important?

The consequences of neglecting privacy are severe. Beyond hefty fines (up to 4% of global turnover under GDPR), organizations face reputational damage, loss of customer trust, and operational disruptions. ISO/IEC 27701 offers a roadmap to avoid these pitfalls by:

- Legal Compliance: Stringent global data protection laws, such as GDPR and CCPA, impose strict requirements on how personal data should be handled. Non-compliance can lead to hefty fines and legal actions.
- Consumer Trust: Customers are increasingly aware of their privacy rights and expect organizations to safeguard their personal data.
- Risk Mitigation: A strong privacy framework helps organizations prevent data breaches, cyberattacks, and unauthorized access to sensitive information.
- Competitive Advantage: Companies that prioritize data privacy gain a competitive edge, as compliance with international standards enhances credibility and business reputation.

Strategy to Implement ISO 27701

To successfully implement ISO 27701, we recommend organizations to follow these key steps:

1. Assess Current Privacy Practices: Conduct a gap analysis to compare existing privacy policies with ISO 27701 requirements.

2. Integrate with ISMS: Extend the existing ISO 27001 framework to incorporate privacy controls outlined in ISO 27701.

3. Define Privacy Objectives and Policies: Establish clear privacy policies and objectives aligned with business goals and regulatory requirements.

4. Implement Privacy Controls: Deploy required technical and organizational controls to safeguard personal data.

5. Train Employees: Conduct privacy awareness training for staff to ensure compliance with privacy management policies.

6. Conduct Risk and Opportunity Assessments: Apply an information security risk assessment process to identify risks associated with confidentiality, integrity, and availability of PII.

7. Define Roles and Responsibilities: Clearly document whether the organization acts as a PII controller, processor, or both.

8. Ensure Compliance with External and Internal Regulations: Address applicable legal, contractual, and regulatory requirements within privacy policies and operational processes.

9. Strengthen Data Governance and Accountability: Appoint a responsible officer to oversee privacy compliance and ensure governance frameworks are effectively implemented.

10. Implement Continuous Monitoring and Improvement: Regularly review and update privacy policies, conduct internal audits, and address non-conformities.

Additional Control Objectives for Data Controller and Data Processor

- Ensure processing is lawful, with a valid legal basis and legitimate purposes.
- Provide data subjects with necessary information and fulfill related obligations.
- Limit data collection, processing, and retention to what is necessary.
- Document and ensure compliance when sharing, transferring, or disclosing personal data.
- Identify & classify personal data (aligned with PDP Law requirements for PII controllers and processors).
- Establish lawful processing mechanisms (ensuring legal bases for data collection, processing, and retention).
- Enhance governance & accountability (defining roles like DPO and implementing privacy-centric risk assessments).
- Ensure data subject rights management (facilitating rights such as access, rectification, and erasure as mandated by PDP Law).
- Strengthen third-party data processing controls (ensuring vendor contracts comply with PDP Law's processor obligations).

CONCLUSION

With Indonesia's Personal Data Protection Law (UU No. 27/2022) now in full effect post-September 17, 2024, organizations must ensure compliance to avoid regulatory penalties, reputational risks, and operational disruptions.

ISO/IEC 27701 provides a structured framework to align with the PDP Law by helping organizations:

By adopting ISO 27701 alongside ISO 27001, organizations in Indonesia can proactively address compliance risks, avoid regulatory penalties, and build consumer trust in an increasingly data-driven landscape.

For further information, please contact : **inquiry@rsm.id**

TP Document Under Scrutiny: The Urgency of Prompt Benchmarking to Maintain Ex-Ante Principles

T QIVI HADY DAHOLI & RINDHASWARI LARETNA S, TAX PRACTICE

In the era of increased global tax scrutiny, Transfer Pricing (TP) compliance is no merely a discretionary best practice – it is obligatory. Regulators are tightening their grip all around the world, including Indonesia. With an increase in tax audits and adjustments, businesses operating in the country must recognize that outdated documentation methods can results in serious financial and legal implications.

What is the key issue? The strict use of the ex-ante principle in transfer pricing documentation.

Understanding the Ex-ante Principle

The ex-ante principle requires that transfer pricing documents be based on data available at the time of the transaction, ensuring that pricing decisions consistent with the arm's length principle before transactions occur. The OECD Transfer Pricing Guidelines 2022 (OECD TPG) define two approaches to time in data collection:

- Ex-ante (Arm's Length Price-Setting Approach) requires taxpayers to document conformity with the arm's length principle before undertaking intra-group transactions using data available at the time.
- Ex-Post (Arm's Length Outcome-Testing Approach): After the fiscal year closes, some taxpayers evaluate the actual outcomes of controlled transactions to ensure they follow the arm's length principle.

Indonesia strongly supports the ex-ante principle, as outlined in the Ministry of Finance Regulation No. 213/ 2016 (PMK-213) and strengthened by Ministry of Finance Regulation No. 172/ /2023 (PMK-172). Article 4 (1.b) of PMK-172 expressly stipulates that transfer pricing documentation must be developed using information available at the time related-party transactions occur. Failure to comply enables the Director General of Taxes (DGT) to reassess income and deductions, resulting significant tax adjustments under Article 36.5 of PMK-172. Non-compliance with the application of the ex-ante principle will result in loopholes and can serve as an "entry point" for tax adjustments. It is no longer a trivial oversight; it is a clear request for tax adjustments.

The Dangerous Gap in Compliance

It is known that many companies and transfer pricing practices collect comparable data after the fiscal year ends, which the DGT believes contradict the ex-ante principle. As a result there has been an alarming surge in transfer pricing disputes, with the ex-ante principle, which requires taxpayers to establish and document arm's length pricing before executing related-party transactions being major focus for tax auditors.

In recent years, there have been numerous cases of companies undergoing tax audits of affiliated transactions and experiencing adjustments due to the use of this ex-ante principle. Tax auditors are increasingly scrutinizing the timing of data collection and benchmarking and requesting evidence from taxpayers to support it.

For better understanding, we provide a simulation for 2025 Transfer Pricing Documentation. If comparable and benchmarking are collected in 2026 or later, the DGT is likely to consider it as non-compliance with ex-ante principles, increasing the risk of exposure to tax adjustments and l subsequent penalties. As a result, the company will face higher tax adjustment from the DGT, as well as longer and more expensive disputes with tax authorities.

Immediate Action: Ex-ante Data Collection and Operational Transfer Pricing

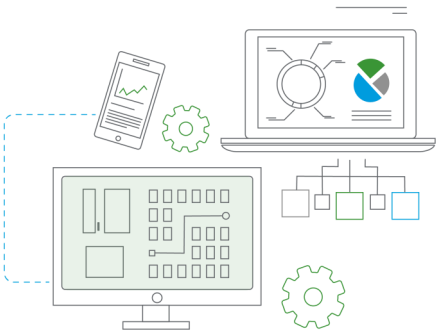
A fundamental part of the ex-ante principle is the utilization of reliable and timely data for comparable data collection and benchmarking. To remains ahead of regulatory scrutiny and avoid costly tax adjustments, companies must radically change their approach to data collection and benchmarking. For example, for 2025 Transfer Pricing Documentation, comparable data collection and benchmarking must be conducted at the beginning of 2025 or throughout the year, prior to any related party transactions. This ensures full compliance with ex-ante principles requirements. Thus, business should implement operational transfer pricing, which monitors affiliated transactions on a regular basis, in order to reduce and mitigate the risk of non-arm's length results in the previous year.

Furthermore, taxpayers who rely on external consultants for transfer pricing documents must secure engagement letters well in advance. The date of the engagement letter from the service contract becomes important because it can be used as supporting evidence, together with the date of data collection, for taxpayer's ex-ante application.

CONCLUSION

To summarize, timely implementation of benchmarking is paramount to ensuring conformity with ex-ante principles, safeguarding taxpayers against potential disputes and penalties. It is strongly recommended that taxpayers adopt this practice and conduct data collection and benchmarking before engaging in related party transactions.

The message is clear: plan ahead of time, document everything in real-time, and safeguard your business. The era of reactive transfer pricing has ended—adapt or pay the price.



For further information,
please contact : **inquiry@rsm.id**

OUR ACTIVITIES

RSM GLOBAL FINANCIAL RESULT

Earlier this year, RSM proudly announced the worldwide revenues of US$ 10 billion for the year ending December 2024, which is a year-on-year growth of 6%.

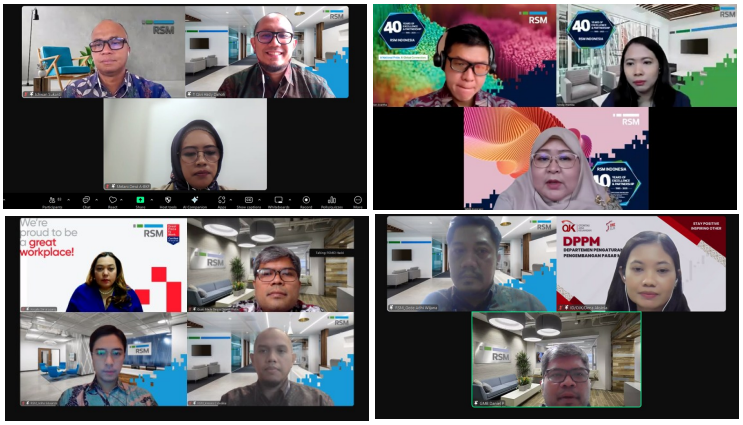
This reflects the combined efforts, collaboration and unwavering commitment of every single member of our RSM team worldwide.

RSM INDONESIA WEBINAR

During the first quarter, we successfully held several webinars to share some of the latest issue that impact business and industry.

In these webinars, our Tax Team covered about global minimum tax, corporate and individual income tax return, whilst our Governance Risk Control Consulting team covered about POJK No. 15/2024 and ESG and sustainability.

Our previous webinars can also be watched on our YouTube channel. Stay tuned for our next webinar!



INDONESIA FACTS

RUJAK CINGUR – traditional food

Rujak is a salad dish of Javanese origin, commonly found in Indonesia. Rujak cingur is a variant of rujak originates from Surabaya. This speciality rujak from East Java has a "meaty" taste. It contains slices of cooked buffalo or cow lips, *bangkuang*, unripe mango, pineapple, cucumber, *kangkung*, *lontong* (rice cake), tofu and tempeh, all served in a black sauce made from petis (black fermented prawn paste, related to *terasi*) and crushed peanuts. It is topped with a sprinkle of fried shallots and *kerupuk* (Indonesian prawn crackers).

OUR PUBLICATION

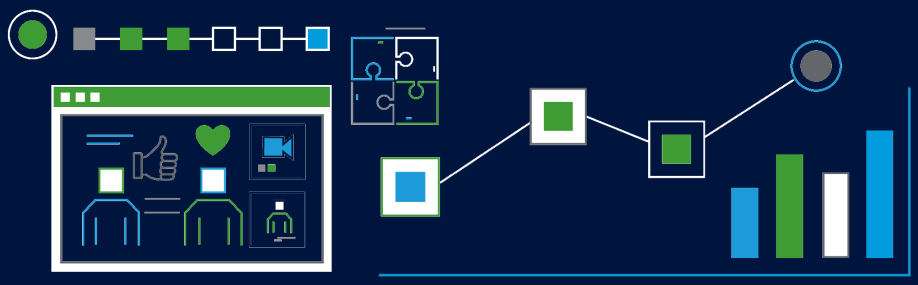
We issued 3 Client Alert publications during 1st quarter of 2025. Click **here** to read more.

- Implementation of 12% VAT Rate
- Implementation of Global Minimum Tax in Indonesia
- Waiving Administrative Penalties related to the Implementation of Coretax

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

Thank you for reading



@ID_RSM RSM ID RSM Indonesia RSM Indonesia @rsm_indonesia

Contact us at newsletter@rsm.id to subscribe or unsubscribe from our quarterly newsletter.
For general queries, contact us at inquiry@rsm.id

RSM INDONESIA

Plaza ASIA Level 10
Jalan Jendral Sudirman Kav. 59
Jakarta 12190 Indonesia

www.rsm.id