

# WAKE UP CALL

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

## QUARTER IV – 2023

Welcome to issue 67 of Wake Up Call – RSM Indonesia newsletter covering topics on audit, tax and consulting.

### IN THIS ISSUE:

- How Technology is Reshaping the Media and Entertainment Industry: Strategies for Success
- Overcoming Security Challenges in the Cloud
- Navigating the Change Landscape of Data Protecting in Indonesia
- Assurance on Greenhouse Gas Statement
- Our Activities

# How Technology is Reshaping the Media and Entertainment Industry: Strategies for Success

RESDY BENYAMIN, TECHNOLOGY CONSULTING PRACTICE

The entertainment industry has undergone significant transformations since the 20th century. Internet has revolutionized the way content is obtained and distributed, breaking the monopoly once held by large corporations. In order to thrive in today's landscape, businesses must leverage user data and implement robust measures to combat piracy.

The entertainment industry also failed to recognize the potential of digital music, resulting in the decline of compact discs (CD) and the rise of Apple Music, Pandora and Spotify. Companies like Netflix utilizing data analytics to personalize user experiences. The transformation of the entertainment business means big corporations no longer hold a monopoly.

## The Utilization of Big Data can Greatly Enhance a Company's Marketing Strategies

Shazam's success is due to its app-based model, allowing users to identify songs and generating valuable data. This data has given Shazam a competitive advantage and attracted music agents. In 2014, Shazam collaborated with Warner Music Group using its data. This shows that publishers improve marketing campaigns by using data-driven processes. These involve collecting and analyzing data to make informed decisions and tailor campaigns to specific audiences. By leveraging data, publishers gain insights into consumer behavior and preferences, optimizing campaigns and achieving marketing objectives.

## The Internet has Undeniably brought Numerous Advantages, but It has also Given Rise to the Problem of Piracy

The internet has revolutionized the way people access information and entertainment, but it has also facilitated illegal activities such as piracy. This has had a profound impact on the entertainment industry, which heavily relies on revenue generated from the sale of copyrighted content. Studies have shown that piracy has a detrimental effect on sales. To combat piracy, it is crucial for consumers to comprehend the consequences of their actions. In 2012, a French law was implemented that sent notices to pirates, and its effectiveness was analyzed. To prevent piracy from harming artists, producers, and consumers, it is essential to safeguard and share content fairly.

### Redefining Media and Entertainment in Digital Era



Media and entertainment need to adapt the changing power dynamics in the entertainment industry and also position themselves strategically to capitalize on new opportunities that technology brings to the sector. The strategic such as:

### **1. Digital Transformation Strategy**

Before developing a digital transformation strategy for the media and entertainment industry, the organization should assess the current technology landscape. They need to identify opportunities to leverage innovative technologies for content creation, distribution, and audience engagement.

### **2. Data Analytics and Insights**

Analyze audience behavior, preferences, and trends with data analytics solutions. The organization needs to predict market trends and demands.

### **3. Content Distribution Optimization**

The organization needs to assess the current technology landscape in media and entertainment before developing a digital transformation plan. They also need to identify opportunities to use innovative technologies for audience engagement.

### **4. Blockchain and Intellectual Property Management**

The use of blockchain technology for secure and transparent intellectual property management should be assessed. In addition, they need to explore the potential of non-fungible tokens (NFTs) for content monetization and ownership tracking.

### **5. Monetization Strategies**

Explore new revenue streams, such as crowdfunding, direct fan support, and innovative pricing models. If required, implement e-commerce solutions for selling merchandise, tickets, or exclusive content directly to fans.

### **6. Regulatory and Compliance Guidance**

Stay abreast of regulatory changes in the media and entertainment sectors by ensuring the business strategies and technologies comply with relevant laws and industry standards.

### **7. Training and Skill Development**

Design training programs for the business to upskill the workforce in emerging technologies and industry best practices. Through the initiative, the organization will have capability to ensure that the team is equipped to adapt to evolving technological trends.

### **8. Risk Management and Cybersecurity**

Evaluate and reduce cybersecurity risks in digital content distribution by safeguarding sensitive data and intellectual property. Check on regulatory compliance for data security as well.



For further information, please contact:  
[inquiry@rsm.id](mailto:inquiry@rsm.id)

# Overcoming Security Challenges in the Cloud

*DIAN P RAHMASARI, TECHNOLOGY RISK CONSULTING PRACTICE*

In this massive digitalization era, infrastructure security has become inevitable for every organization. With the increasing adoption of cloud technology, companies must take account of higher priority in protecting critical IT infrastructure. Many organizations are starting to rely on the cloud as data storage, which also forces them to design a robust plan for recovery planning. Thus, Disaster Recovery Center (DRC) and Cloud Security are essential in maintaining business continuity and protecting the organization's information assets.

## Cloud Infrastructure Security: How Data Center and Disaster Recovery Center (DRC) Plays a Vital Role

The data center is the main foundation in information technology operations, while the Disaster Recovery Center (DRC) plays a vital role in dealing with disasters or severe disruptions. Protecting the Data Center from cyber-attacks, data theft, or system vulnerabilities is critical in maintaining operational and business continuity. In another way, DRC also plays a significant role in recovering after a disaster and ensuring organizations can run their operations as smoothly as they should.

## Cloud Security Trends: How to Well-Adapt

Cloud security trends continue to evolve along with technology development, the increasing complexity of cyber attacks, and the dynamics of business needs. These security trends include:

- **Multi-Layered Security (Defense-in-Depth):**  
An approach that "one layer of defense" is not enough, so it must be multiple layers to protect the infrastructure from various types of attacks, including a combination of data encryption, firewalls, threat detection, and integrated security tools.

- **Identity and Access Security**

It "guarantees" that only authorized individuals can access sensitive systems and data through double authentication, extreme user access management, and regular user activity monitoring.

- **AI and Machine Learning Security**

The use of artificial intelligence and machine learning to automatically detect and respond to security threats, including intelligent data analysis to identify attack patterns and proactive countermeasures.

- **Blockchain Security**

In the cloud context, blockchain helps secure transactions and provide proof of data immutability, reducing the risk of information manipulation or leakage.

- **Compliance and Regulation**

Security trends also include compliance with security standards and regulations, such as GDPR in Europe or HIPAA in the United States, as well as currently in Indonesia with the Personal Data Protection (PDP) Law No. 27/2022. Consequently, organizations must ensure their cloud infrastructure complies with the acceptable regulations.

## Security Operations Center in a Cloud Environment: Pathway to Reach a Comprehensive Protection

In a cloud environment, the presence of a Security Operations Center (SOC), Network Operations Center (NOC), and Threat Detection and Response Center is critical to ensure comprehensive protection of data and infrastructure.

They are responsible for continuous monitoring, early detection, and rapid response to security issues that may arise in the cloud ecosystem, keeping the organization compliant with applicable security standards and regulations.

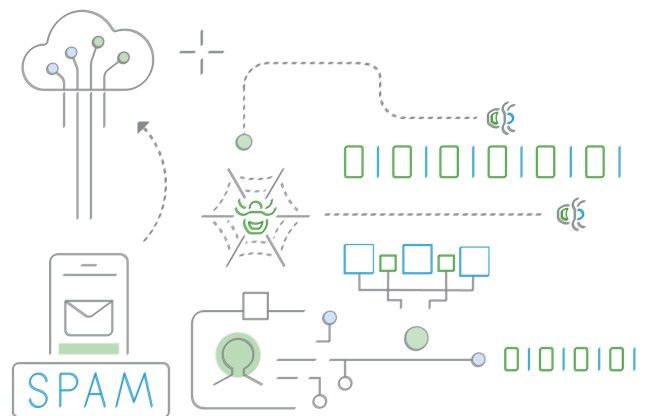
### Cloud Adoption, Nowadays: A Business Opportunity

Organization today is shifting to more cloud-connected business models. Migrating to the cloud is not just about data storage but also about applications, software development, data analysis, and artificial intelligence. Predictions for global corporate spending on cloud computing infrastructure is expected to reach US\$1 trillion by 2024, this number shows a growing need for the latest platforms and services, including artificial intelligence (AI) services.

It has been popular nowadays that cloud migration has enormously saved time and money and opened opportunities for innovation. While there are still a plethora of security and data protection issues, new cloud models such as hybrid cloud and federated cloud systems continue to develop to overcome these obstacles.

### CONCLUSION

Cloud infrastructure and data protection are no longer an option, but imperative in today's digital era. Comprehensive protection, regulatory compliance strategy and optimal operations centers are crucial in maintaining continuity and overcoming security challenges in a cloud environment. The adoption of the cloud opens the door for businesses to make any transformation, making security infrastructure a priority in optimizing the potential of cloud technology.



For further information, please contact:  
[inquiry@rsm.id](mailto:inquiry@rsm.id)

## INDONESIA FACTS

### LURIK

Lurik (Javanese script) is a cloth with small striped motifs that has traditionally been the typical clothing of rural men among the Javanese ethnic group. Lurik, which is made from coarse cotton, is relatively cheap and affordable for the poor. Lurik is the basic material for making *surjan*.

In modern developments, lurik now has a touch of new colors, so that it can also be used as shirt material or as an aesthetic component of a vest or suit.



Source: Wikipedia

Photo: Wikipedia

# Navigating the Change Landscape of Data Protecting in Indonesia

**ERIKMAN PARDAMEAN**, TECHNOLOGY RISK CONSULTING PRACTICE

The Personal Data Protection (PDP) Law in Indonesia, officially Law Number 27 of 2022, came into effect on 17 October 2022, marking a pivotal moment in data protection legislation. While effective immediately, the PDP Law allows a two-year transition period for Personal Data Controllers, Processors, and other relevant entities to align their practices with the new legal framework.

## Understanding Personal Data: a Crucial Starting Point

One of the key foundations of the PDP Law is its definition of personal data, encompassing information that identifies or can identify an individual directly or indirectly, through electronic or non-electronic systems. Article 4 of the PDP Law delineates two categories: general personal data, including full name, gender, citizenship, religion, marital status, and specific personal data, such as health and biometric information.

Recognizing these distinctions allows organizations to prioritize data protection measures, including Privacy Impact Assessments (PIA/DPIA), Record of Processing Activity (ROPA), and Third-Party Risk Assessments.

## Empowering Personal Data Subjects: Rights and Entitlements

The PDP Law empowers individuals with various rights, outlined in Articles 5 to 15. Personal data subjects have the right to clear information about the identity, legal basis, purpose, and accountability of entities requesting their data. They can update, access, and obtain copies of their personal data, withdraw consent, object to automated decision-making, and right to claim compensation.

## Responsibilities of Personal Data Controllers

Articles 19 to 49 of the PDP Law outline the obligations of Personal Data Controllers, emphasizing the need for legal bases, transparent information disclosure, access provision, accuracy updates, and secure processing. Beyond these, controllers must promptly notify data subjects and authorities in case of data breaches, adding an extra layer of accountability to the data protection landscape.

## Data Breach Reporting and Sanctions

In the event of a data breach, the PDP Law mandates a swift report within 3 x 24 hours to affected data subjects and relevant authorities. The report must detail the breached data, the timing and nature of the breach, and the remedial actions taken, as per Article 46. Non-compliance with the PDP Law carries substantial penalties, including written warnings, financial sanctions, imprisonment up to 6 years, temporary activity suspension, and even the dissolution of corporations.

## Embracing Data Protection: a Collective Responsibility

Beyond legal and compliance departments, every individual within an organization plays a crucial role in achieving PDP Law compliance. The purpose of collecting and processing personal data must be well understood across the board. Compliance with the PDP Law is not just a legal requirement; it is a shared responsibility that demands a collective effort to protect the personal data of Indonesian citizens.

## Transition Period and Compliance Deadline

The PDP Law, effective since 17 October 2022, provides a two-year grace period for Personal Data Controllers, Processors, and related parties to adjust to its provisions, as stated in Article 74. However, it's crucial to note that serious violations of personal data protection may still lead to criminal charges before the completion of the two-year adjustment period.

## CONCLUSION

As the PDP Law reshapes Indonesia's data protection landscape, organizations must proactively adapt, ensuring not only legal compliance but also fostering a culture that prioritizes and safeguards personal data. Regardless of size or industry, every organization engaging with the personal data of Indonesian citizens must recognize the profound impact of the PDP Law and take decisive steps to adhere to its provisions.



For further information, please contact:  
[inquiry@rsm.id](mailto:inquiry@rsm.id)

## SEASON'S GREETING



# Assurance on Greenhouse Gas Statement

**BENNY ANDRIA**, AUDIT PRACTICE

Indonesian Standard on Assurance Engagements 3000 (SPA 3000 – Revised 2022) regarding assurance engagement other than audits or reviews of historical financial information will be effective starting from 1 January 2024. The implementation of SPA3000 to carry out assurance for greenhouse gas (GHG) statement is deemed inadequate because it does not specifically address an assurance technique for GHG. Therefore, the Public Accountant Professional Standards Board in Indonesia has adopted ISAE3410 as the Indonesian Standard of SPA3410 "Assurance Engagements for Greenhouse Gas Statement" as specific assurance standard. This new standard provide guidance for public accountants in providing either reasonable assurance or limited assurance regarding GHG that the statement is free of material misstatement—which result will enhance the reliability of the emission information being reported.

Public accountants are required to comply with SPA 3000 (Revised 2022) and SPA 3410 when performing an assurance engagement to report on an entity's GHG statement. Compliance with SPA 3000 requires compliance with the provisions of Code of Ethics for Public Accountants, including the Independence requirements. It also requires the engagement partner of this assurance engagement to be a member of a firm that applies Standard on Quality Control-1.

SPA3410 adopts a risk-based approach, where the public accountants should obtain understanding of the entity and its environment including its internal control, identify and assess the risk of material misstatements in GHG Statement, perform procedures to address the identified risks, and report in accordance with their findings.

SPA3410 requires that the assurance team consists of multidisciplinary team members which may include certain experts, including but not limited to information systems expert, and scientific and engineering expert. The team collectively is required to possess the necessary professional competencies to perform the assurance engagement, including assurance skills and GHG competencies: law and regulations, quantification, measurement methodologies, etc. This is in line with the nature of GHG Statement that is subject to uncertainty. There are two uncertainties, which are:

1. Scientific uncertainty, because of incomplete scientific knowledge about the measurement; and
2. Estimation uncertainty.

The GHG statement is a published report on the calculation of GHG emissions that is accounted for periodically. Types of GHG emissions include: Carbon Dioxide (CO<sub>2</sub>), Methane (CH<sub>4</sub>), Nitrous Oxide (N<sub>2</sub>O), Hydrofluorocarbons (HFCs), Perfluorocarbons (PFCS), Sulfur hexafluoride (SF<sub>6</sub>) and Chlorofluorocarbons (CFCs)<sup>1</sup>. This GHG emissions inventory is regulated by the government through Presidential Decree number 98/2021 to provide carbon economic value for achieving nationally determined contribution targets and controlling GHG emissions in national development. One of the relevant parties who have an obligation to carry out the GHG inventory is the business entity, as well as regional governments and the Minister. Meanwhile, the Central Bank is in the stage of developing "Kalkulator Bijak" to implement green financing.

<sup>1</sup>CFCs is currently not regulated in Presidential Decree number 98/2021



GHG inventory will report the amount of emissions produced by a particular entity. There are three scopes of emissions reported, namely Scope 1 is emissions directly produced by the entity. Scope 2 is emissions that are not directly produced by the entity, for example emissions from energy purchased and consumed by the entity. Scope 1 and Scope 2 are emissions that can be controlled directly by the entity. Meanwhile, Scope 3 is emissions that are outside the entity's control.

Apart from reporting emission sources, GHG inventory also reports sources of emission reduction, including the use of solar generators, wind generators, water generators, use of electric cars, purchase of carbon credits, green bonds and green donations. Other than carbon reduction, there is also carbon removal: whether geological (such as underground) or biological (such as planting trees).



For further information, please contact:  
[inquiry@rsm.id](mailto:inquiry@rsm.id)

## NEWSFLASH



Please be informed that our Surabaya office has been relocated to a new location effective 8 December 2023.

Our office address in Surabaya is as follow:

**Pakuwon Center**

Tunjungan Plaza 5, 11<sup>th</sup> floor, Unit 6

Jl. Embong Malang No. 1, Surabaya 60261

Tel: +62 31 35975222

Fax: +62 31 35979111

We look forward to serving your audit, tax and consulting needs from our new office.

# OUR ACTIVITIES

## ●●● RSM World Day

On 7 December 2023 we celebrated RSM World Day, a global celebration of network's vision and values. This year's theme was Knowledge is Power and at the same date RSM firm from 120 countries shared the same spirit.

Prior the event, our people through RSM Indonesia Mengajar program were volunteering to teach 'marginal kids' (kids that on the street and vulnerable to be on the street) at Yayasan Sahabat Anak.

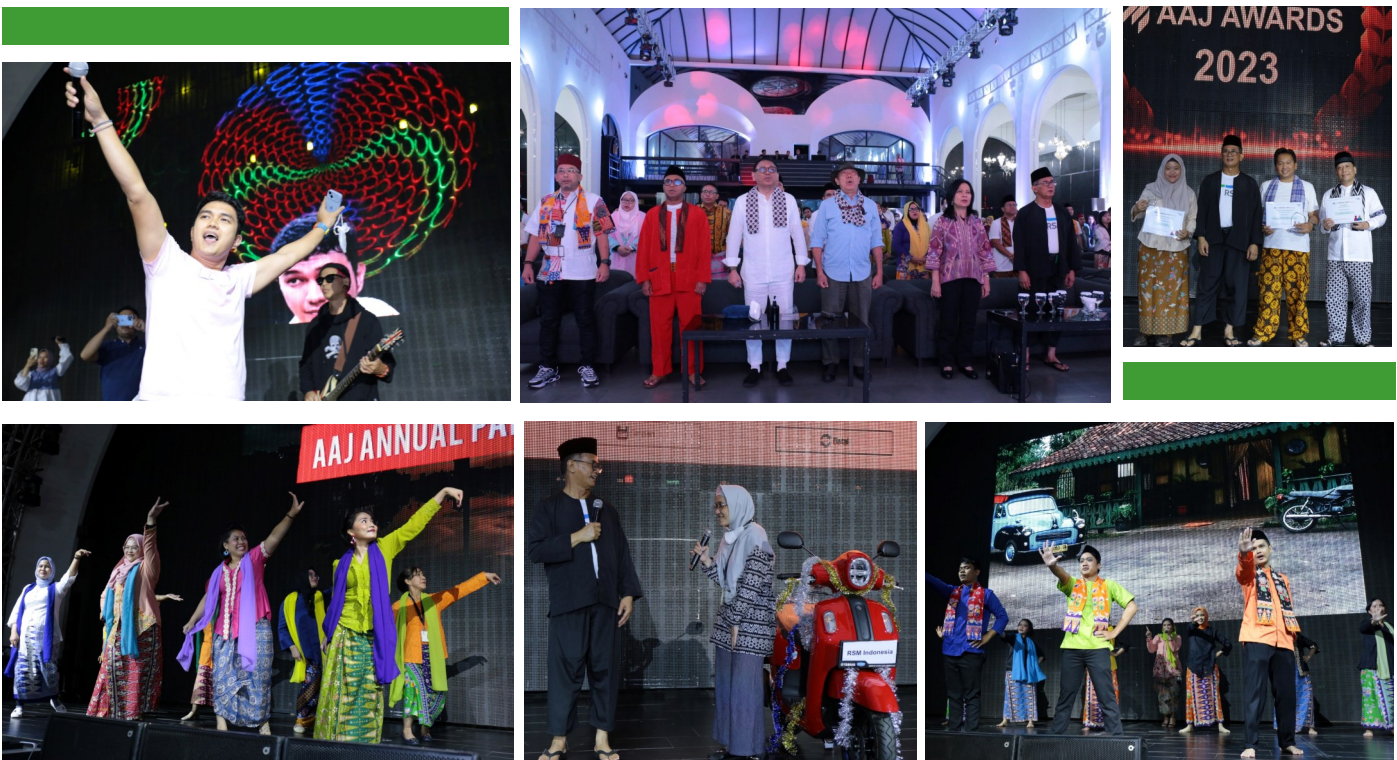


## ●●● AAJ Annual Party

We finally able to held an in-person annual party again this year. The RSM Indonesia's AAJ Annual Party was held with a specific theme of "Halo-Halo Jakarta" as a celebration of our capital city, the Betawi culture and Jakarta as a melting pot of Indonesia.

We always start with our National Anthem "Indonesia Raya", continued by speech from our Chief Executive Partner, Amir Abadi Jusuf. There were group performances, door prizes & grand prize drawing, and award to our people. We also invited the famous Aldi Taher to perform as guest star.

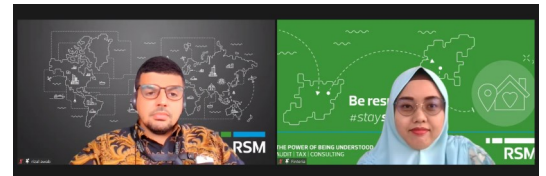
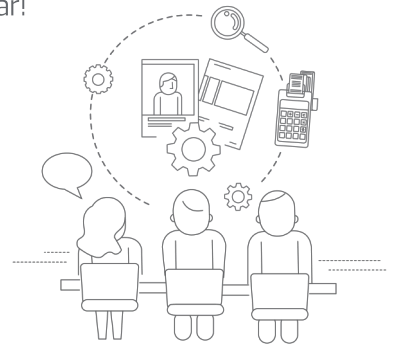
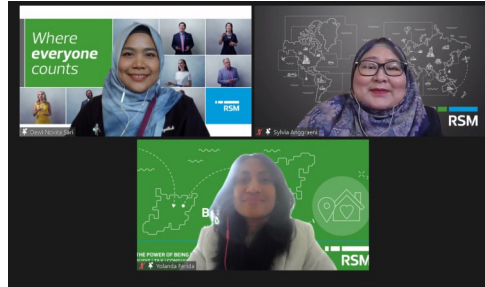
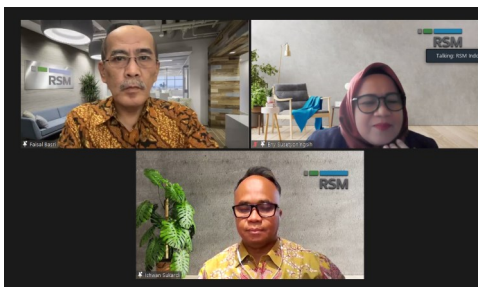
This activity is part of our tradition to appreciate our people and to creates a strong bond of RSM Indonesia people.



# OUR ACTIVITIES

## RSM Indonesia Webinar

We successfully conducted several webinars during the last quarter of this year. The webinars were delivered by our Partners. We also invited Bapak Faisal Basri as a speaker in our tax webinar to share about key and projected trends of the economy and taxation in 2024. More than 100 participants attended each webinar. See you next year on our next event and happy new year!



## RSM Indonesia become a Signatory to the Women's Empowerment Principles



We have now become a signatory to the Women's Empowerment Principle's of the United Nations Global Compact. We believe that equality and diversity makes our organization stronger and more sustainable.

Click [here](#) to view our profile.

# Thank you for reading



@ID\_RSM



RSM ID



RSM Indonesia



RSM Indonesia



@rsm\_indonesia

## RSM Indonesia

Plaza ASIA Level 10  
Jl. Jend. Sudirman Kav. 59  
Jakarta 12190 Indonesia

[www.rsm.id](http://www.rsm.id)

Opinions expressed in these articles are the personal view of RSM Indonesia and are not intended as specific business advice. It might contain extracted information from publicly disclosed information. Though this publication was prepared in cautiousness, no warranty is provided for the information it contains and no liability is accepted for any statement or opinion presented. Readers of this material are recommended to seek professional advice before making any business decisions.

Contact us at [newsletter@rsm.id](mailto:newsletter@rsm.id) to [subscribe](#) or [unsubscribe](#) from our quarterly newsletter.

For general queries, contact us at [inquiry@rsm.id](mailto:inquiry@rsm.id)

RSM is represented in Indonesia by Amir Abadi Jusuf, Aryanto, Mawar & Rekan; PT RSM Indonesia Konsultan; PT RSM Indonesia Mitradaya; PT RSM Indonesia Mitradana. RSM's Indonesian member firms work closely together within Indonesia. Each firm is a separate and independent legal entity and a member of the RSM network and trades as RSM. The RSM network is not itself a separate legal entity in any jurisdiction.