THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

QUARTER II – 2024

RSM

Ani

One of the
RSM team

WAKE UP CALL

Bringing you insights from **RSM Indonesia**

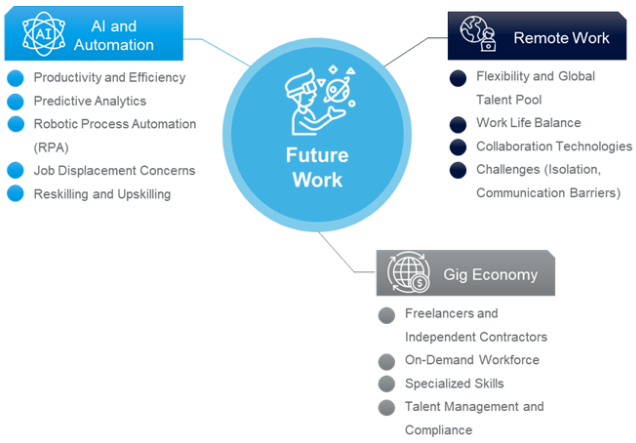
Welcome to issue 69 of Wake Up Call – RSM Indonesia newsletter covering topics on audit, tax and consulting.

IN THIS ISSUE:

The Future of Work: Embracing AI, Automation, and Remote Work for Business Transformation

RESDY BENYAMIN, TECHNOLOGY CONSULTING PRACTICE

The world of work is undergoing a significant shift, driven by the rapid advancements in artificial intelligence (AI), automation, and the widespread adoption of remote work. These transformative forces are not just changing the way we work; they are redefining the very nature of work itself. As traditional business models and practices become increasingly outdated, organizations must embrace these changes to stay competitive, attract top talent, and unlock new opportunities for growth. This article explores the profound impact of AI, automation, and remote work on businesses and the workforce and provides actionable strategies for navigating this new landscape with the guidance of technology consulting firms.



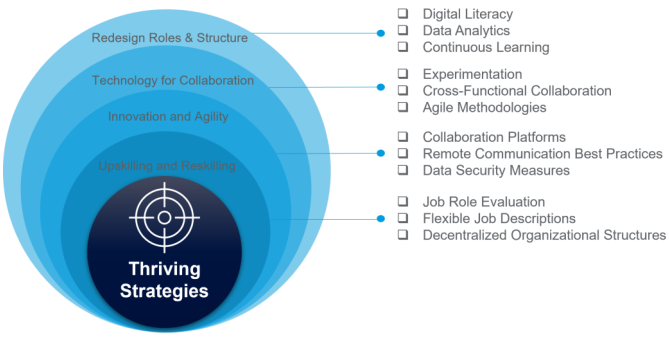
THE AI AND AUTOMATION REVOLUTION

The integration of AI and automation technologies is bringing about a new era of productivity and efficiency across industries. From manufacturing and logistics to healthcare and finance, these intelligent systems are automating repetitive tasks, optimizing processes, and enabling data-driven decision-making. AI-powered predictive analytics, for example, can anticipate equipment failures, optimize supply chains, and personalize customer experiences. Robotic process automation (RPA) is streamlining back-office operations, freeing human workers from mundane tasks and allowing them to focus on higher-value, strategic activities.

However, the rise of AI and automation also raises valid concerns about job displacement and the future of work. As machines become increasingly capable of performing tasks previously reserved for humans, some roles may become redundant. Yet, this disruption also presents unprecedented opportunities for the creation of new, high-skilled jobs that require uniquely human capabilities such as creativity, critical thinking, and emotional intelligence. To harness the full potential of AI and automation while mitigating the risks, businesses must prioritize reskilling and upskilling initiatives. By investing in comprehensive training programs that equip employees with the necessary competencies for the future of work, organizations can foster a resilient and adaptable workforce ready to thrive in the age of intelligent machines.

THE REMOTE WORK REVOLUTION

Remote work has gained traction, offering businesses and employees new flexibility. Remote work offers unparalleled flexibility, eliminates commute times, and enables access to a global talent pool. It has the potential to improve work-life balance, boost productivity, and reduce operational costs. However, remote work also presents unique challenges, such as feelings of isolation, communication barriers, and difficulties in maintaining work-life boundaries.



To thrive in a remote work environment, organizations must invest in the right technologies, establish clear communication protocols, and cultivate a culture of trust and accountability. Collaboration platforms, video conferencing tools, and project management software are essential for seamless virtual teamwork and knowledge sharing. Leaders must prioritize regular check-ins with the teams, provide emotional support, and ensure that employees have access to the resources they need to maintain the well-being and productivity. By embracing remote work as a strategic opportunity rather than a temporary necessity, businesses can tap into new talent pools, enhance employee satisfaction, and build a more resilient and agile workforce.

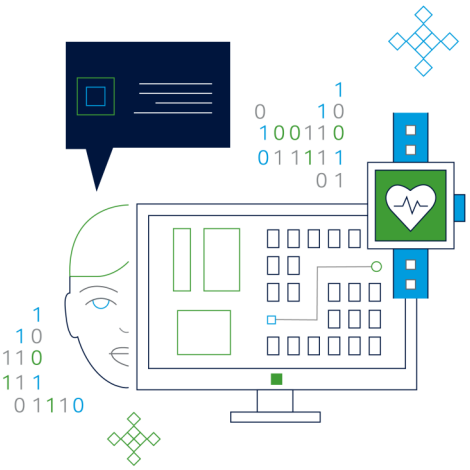
THE RISE OF THE GIG ECONOMY

Alongside the remote work revolution, the gig economy is experiencing significant growth. Freelancers, independent contractors, and project-based workers are becoming an integral part of the modern workforce, offering businesses flexibility, cost-effectiveness, and access to specialized skills. Platforms like Upwork, Freelancer, and Fiverr are connecting organizations with a global pool of talented professionals, enabling them to scale the workforce on-demand and adapt to changing market conditions.

To fully leverage the benefits of the gig economy, businesses must rethink the traditional hiring practices and talent management strategies. This involves developing streamlined onboarding processes, implementing robust project management tools, and ensuring compliance with labor regulations. By successfully integrating gig workers into the operations, your business can enhance agility, tap into niche expertise, and foster a more diverse and inclusive workforce.

Navigating the complexities of the future of work can be overwhelming for businesses. This is where technology consulting firms play a vital role.

The future of work is not a distant concept; it is already here. Businesses that embrace this reality and adapt accordingly will be the ones that thrive in the years to come. By leveraging the power of AI, automation, and remote work, your business can achieve success in an ever-evolving business landscape. The rewards for those who lead the way will be significant, and the impact on the world of work will be profound.



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

Strengthen Your Cyber Fort: Why IT Audits Lead the Charge

ERIKMAN D PARDAMEAN, TECHNOLOGY RISK CONSULTING PRACTICE

Imagine waking up to find hackers have breached your company's network due to outdated software and lax password policies. The fallout – customer data theft, public relations nightmares, and regulatory fines – could be catastrophic. In today's digital landscape, where cyber threats lurk around every corner, robust cybersecurity isn't just essential – it's a survival imperative. Yet, many organizations overlook a pivotal tool in their defense arsenal: the IT Audit.

WHY KICKSTART WITH IT AUDITS?

An IT Audit isn't just about checking boxes; it's your proactive shield against cyber threats. It's your way of identifying vulnerabilities and ensuring that your defenses are up to par. By conducting an IT Audit, you're shining a spotlight on potential weaknesses before they become entry points for malicious actors, thereby significantly bolstering your overall security posture.

EMBARK ON YOUR IT AUDIT JOURNEY: LET'S BEGIN!

Kickstart your IT audit journey with these actionable steps:

- **Evaluate your Current Systems:** Take stock of your IT infrastructure, from hardware to software and network configurations.
- **Set Clear Objectives:** Define what you want to achieve with your audit, ensuring you cover all necessary areas.
- **Pick your Audit Framework:** Choose a trusted framework like COBIT or ISO/IEC 27001 to guide your audit journey. Curate a multidisciplinary team comprising network engineers, system administrators, and cybersecurity analysts to facilitate comprehensive analysis and insight generation.
- **Build your Expert Team:** Assemble a squad of IT experts who know the ins and outs of both systems and cybersecurity.
- **Dive into the Audit:** Dive headfirst into your audit, meticulously reviewing controls, processes, and compliance.
- **Uncover Insights:** Analyze your findings to unearth vulnerabilities and identify areas ripe for improvement.
- **Take Action:** Implement recommendations swiftly, fortifying your defenses against potential threats.

ALIGNING IT AUDITS WITH CYBERSECURITY STANDARDS FOR OPTIMAL DEFENSE

When it comes to IT Audit frameworks, integration with cybersecurity standards is key. Take COBIT, for instance – it dovetails seamlessly with the NIST Cybersecurity Framework, offering a holistic approach to IT controls and cybersecurity practices. Similarly, ISO/IEC 27001 provides a structured roadmap for safeguarding sensitive information, making it the perfect partner for IT Audit endeavors aimed at risk mitigation.

REAL-WORLD CASE STUDY: LEARNNG FROM MARRIOTT'S MISFORTUNE

Let's take a page from Marriott International's playbook. In 2018, the hospitality giant fell victim to a massive data breach, compromizing the personal information of millions. The breach stemmed from malware installed on the company's point-of-sale (POS) systems, allowing hackers to steal sensitive data, including passport numbers and credit card information.

Had Marriott conducted regular IT audits, they could have identified vulnerabilities in their POS systems, preventing the breach before it ever occurred. These IT

audits effort could have assessed the security posture of the POS systems, uncovered misconfigurations or outdated software, and recommended appropriate security patches or upgrades – saving Marriott from a PR nightmare.[1]

COMPLIANCE WITH INDONESIA'S TECHNOLOGY AUDIT REGULATIONS

In Indonesia, the imperative for technology audit compliance has significantly grown in the past 5 years, especially within tightly regulated sectors like banking, insurance, and financial services. The regulations are becoming more rigorous surrounding information technology management, including the mandatory implementation of technology audits. Bodies such as the Financial Services Authority and Bank Indonesia are at the forefront, racing to establish and enforce these regulations. There are undeniable needs for businesses to stay abreast of these developments. Let's stay ahead together as we navigate this evolving regulatory landscape!

[1]*Source: https://privacy.wiki/Mariott_Data_Breach*

CONCLUSION: THE SYNERGY OF IT AUDIT AND CYBERSECURITY

The synergy between IT audits and cybersecurity forms a robust defense against digital threats, ensuring longevity and compliance. As organizations rapidly adopt and replace technology, IT risks rise, necessitating agile and knowledgeable auditors. By prioritizing IT audits, organizations not only mitigate risks but also secure a brighter, safer future in an ever-evolving threat landscape.

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

NEWS FLASH

Congratulations to our Senior Partner,
ANGELA SIMATUPANG, has been elected to serve as President of the Institute of Internal Auditors Indonesia for a second term.

Unleashing the Power of Security Education, Training, and Awareness: a Path to Empowering the Community as 'Cyber Guardians'

DIAN P RAHMASARI, TECHNOLOGY RISK CONSULTING PRACTICE

A Glance of Cybersecurity Education, Training and Awareness: Let's We Recall Their Objectives

Securing information system assets is a pressing issue in today's digitally interconnected world. We are under constant surveillance in a digital age, with cybercriminals adapting to our environment. This situation has spurred our community to prioritize extensive security and awareness programs. These programs are not just a shield but tangible solutions to safeguard us from relentless cyber-attacks. Cybersecurity is no longer a mere technical practice but a necessity for sustainable goals. If we encapsulate it, it might sound like, 'If you want your business to thrive, you must also prioritize the security of your information assets. In this context, we are not just individuals but 'Cyber Guardians' responsible for protecting our digital world.

Humans are the Weakest Lines

Most experts, researchers, and ourselves agree that the weakest line of cyber is from the person we are as humans. It can be reflected in the most prominent cyber cases, such as hacking in financial institutions, retailers, and transportation, caused mainly by humans. We are not to say that humans are the primary weakest links" in attempts to secure information systems assets, but cases vary from the simplest thing, like:

- The use of unauthorized Wi-Fi or VPN that the employee uses
- Forget to update the version of the software
- Unaware of making a quick response plan based on the testing results, like vulnerability assessment and penetration testing.

Even with regular security assessment programs, many organizations resist evolving cyber threats. This phenomenon raises a crucial question: how effective are the security programs implemented in organizations in securing their information systems assets?

Expert's and Researcher's view: Way in Elaborate Security Assessment, Training and Education Program

Some acceptable answers have been patterned from this question. Researchers have made observations by referring to experts from developed countries. The observation shows that security Assessment, Training, and Education programs could be elevated to extensive-practical programs that can be implemented through extensive collaboration between IT consultancies services, educational institutions, businesses, and government. This collaborative effort is crucial in our collective mission to enhance cybersecurity.

1. Designing a security awareness program based on audience classification can be planned. For example, the security training program for top-level management differs from the staff or newcomer level. Whereas the top-level management needs more conference seminars, the staff levels need fresh training, such as more quizzes and games.
2. Motivate employees to engage in security awareness. For example, businesses can reward employees who actively engage in security awareness. This cannot be limited to the IT department staff but also to any employee from any department. As a result, the employee will feel eager to participate in security awareness activities to get promotions, recognition, etc. Additionally, it requires the extensive roles of the IT division to collaborate with another department.
3. Communicate in a Sustainable Way. The example can be done through regular security assessments conducted internally or externally, like vulnerability

and penetration testing. Then, all of the findings must be monitored, evaluated, and remediated. In addition, having an external auditor, an independent and objective professional who collaborates with the IT departments, is also an excellent practice for supporting sustainability. These auditors can provide a fresh perspective on the organization's security measures and identify potential vulnerabilities or improvement areas. Their involvement can significantly enhance the effectiveness of the organization's cybersecurity efforts.

How does Indonesia's position compare to other Southeast Asian (SEA) countries?

Based on data from the National Cyber Security Index (NCSI) in 2023, globally, Indonesia is ranked 49th out of 176 countries. Meanwhile, in the country with the best cybersecurity in the Association of Southeast Asian Nations (ASEAN) group, Indonesia is in the top five categories with a score of 63.64, after Malaysia, Singapore, Thailand, and the Philippines. Malaysia scored the highest in the Association of Southeast Asian Nations (ASEAN) group, with a score of 79.22, followed by Singapore, which scored 71.43.

CONCLUSION

Security education and awareness programs are not just necessary but a primary objective of maintaining business sustainability. When security is in place, it raises business and economic value and, respectively, a country's trust. Preparing security awareness requires extensive collaboration between the government, IT experts, IT consultancies, and businesses. The benefits of such awareness are limited to protection, the enhancement of business and economic value, and the fostering of the country's trust.

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

OUR NEW PARTNER

Rosita Uli Sinaga has joined RSM Indonesia as a Senior Partner for Consulting Practice. She has 30 years of experience in public accounting firm.

Employment Matters! – Part 1

NICHOLAS GRAHAM, BUSINESS SERVICES PRACTICE

EMPLOYEES ARE A CRITICAL DRIVER FOR SUCCESS

This is the first of a multi-part article that highlights some employment/HR matters that managers should be aware of to avoid mistakes that might jeopardize the relationship with employees and/or create risk.

Basic obligations

Although the Manpower Law permits oral arrangements, the Law states in principle that employment arrangements should be written. These should be in Indonesian language and, in the case of agreements for fixed term employment, the Indonesian version shall prevail if the agreement is bilingual.

Only offers for permanent employment can provide for a probation period, and this period cannot exceed 3 months.

If there are 10 or more employees then the employer is required to create Company Regulations (*Peraturan Perusahaan*) unless there is a collective labour agreement ("CLA"). The Company Regulations summarize key aspects of the employment relationship and must cover the rights and obligations of the employer and employee, working conditions/ requirements, discipline and rules of conduct, and the validity period of the Company Regulations (not more than 2 years). The Company Regulations must be developed after considering input from the employees, cannot contradict any laws/regulations, are submitted to the Ministry of Manpower for approval, and copies of the approved Company Regulations should be available to the employees.

Salaries can be paid on a daily, weekly or monthly basis. For monthly salaries, employees are entitled to receive their salary no later than the end of the month or such earlier date as is stated in the employment agreement, Company Regulation or CLA (relevant agreements). Therefore, it is best if relevant agreements state that payment will occur no later than the end of the month unless you wish to commit to an earlier payment. Late payment of salary is subject to a fine and an employee can apply for termination with compensation if salary is paid late for 3 or more consecutive months.

The employer must also provide a payslip (*Bukti Pembayaran Upah*) that provides sufficient information regarding the components of the pay. This should be provided at the time the salary is paid.

All employees are required to be registered for the BPJS Ketenagakerjaan and BPJS Kesehatan programs. The exception are daily workers or fixed term contract employees (PKWT) engaged for less than 3 months, who are only required to be registered for the JKK (accident at work) and JKM (death benefit) components of BPJS Ketenagakerjaan. The employer should make the necessary employer contributions, deduct the employee contributions and pay all contributions to BPJS.

In addition to BPJS, no later than 20 May 2027, employers are required to register for the *Tabungan Perumahan Rakyat*/Tapera (People's Housing Savings) program. Similar to BPJS, Tapera requires both employer and employee contributions.

We recommend that the relevant agreements clearly state that employee contributions will be borne by the employee and deducted from the salary to be paid to them.

Employee entitlements

Employees in Indonesia have certain basic entitlements that may differ from other countries, such as:

- THR, that is paid no later than 1 week before the employee's major religious holiday (this should not be confused with a "13th-month" bonus as exists in some countries).
- Minimum annual leave of 12 days per year for those employees working a 5-day working week.
- Sick leave is generally unlimited and on full pay for up to four months. The relevant agreements can stipulate reasonable documentation to support the leave.
- Various paid leave, including hospitalization/death of direct family, circumcision or baptism of children, marriage (self or of children), maternity & paternity leave, menstruation (period leave) and pilgrimage leave.
- Overtime.

The employer is entitled to create rules regarding when annual leave becomes due and how it should be taken. Employers can stipulate that the leave must be taken within 12 months of that anniversary (use-or-lose) or that it can be accumulated.

Most employees are entitled to overtime if required to work more than 8 hours per day (assuming a 5-day work week) or to work on weekends/public holidays. The exception are employees in "certain positions/roles", such as those with responsibilities as thinkers, planners, executors, and/or controllers. Those roles that are not entitled to overtime are expected to receive higher salaries and should be identified in the relevant agreements. The overtime payable is determined using specific multipliers for overtime-hours-to-payroll-hours depending on the hours worked and whether these occurred.

Implications arising from the taxation of Benefits in Kind (BIK)

BIK can be in the form of the provision of goods other than money ("natura", such as food and drink) or the provision of facilities or services (*kenikmatan*, such as the use of a car).

Following the enactment of Law No. 7 on the Harmonization of Tax Regulations, commencing the later of 1 January 2022 or commencement of the employer's 2022 Tax Year, all BIK are an income tax object for the employee, unless otherwise regulated.

Accordingly, employers are required to record BIK as income earned by employees and withhold tax from that income under Article 21.

All things equal, it is likely that employers will need to gross up the tax on BIK so that the employee does not suffer a reduction to their take-home pay as a consequence of the BIK being included as a component of their income. This should be documented in the relevant agreements.

The BIK must then be disclosed in the pay slip.

Foreign management of HR matters

Expatriates are not permitted to be employed in positions that manage personnel matters. This is also understood to mean that personnel matters should not be managed by foreign employees at the Group/overseas level.

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

INDONESIA **FACTS**

SERUNE KALEE – traditional musical instruments

Acehnese horn with a clarinet-like structure. Serune Kalee is usually played as the main instrument in a traditional music performance in Aceh, accompanied by geundrang, rapai, and a number of other traditional instruments. To this day, Serune Kalee is still alive and well in the Acehnese community, and plays a major role in Acehnese social rites such as the *intat linto baro* ceremony, opening ceremonial events, welcoming honored guests, and celebrating holidays.

The instrument is made from an alloy of wood, brass and copper. It is classified as an aerophone, or an instrument that has a sound source from blowing air in the cavity. In fact, Serune Kalee comes from 2 words, namely (serune) which refers to a traditional Acehnese instrument, and (kalee) which is the name of a village in Laweung, Pidie Regency. So in simple terms, Serune Kalee can be interpreted as a serunai/flute from the Kalee area. It is very likely that the naming is associated with the appearance or place of manufacture of the serunai/flute.

Source: Kulturnesian

RSM **PUBLICATION**

Sustainable finance and banking in 2024: A climate risk integration approach

In recent years, the discourse around environmental, social, and governance (ESG) factors has gained significant momentum within the financial services industry. Organizations are under increasing pressure to incorporate climate-related risks and opportunities into their operations and reporting practices.

Click **here** to read more.

OUR **ACTIVITIES**

RSM INDONESIA GOES TO CAMPUS

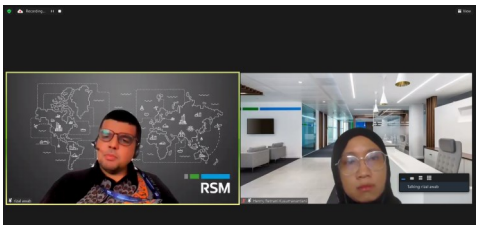
On 2nd quarter of this year, we participated in Career Days events at FEB Universitas Indonesia, Depok and Universitas Gadjah Mada, Yogyakarta. More than 200 students joined the events. This is one of our commitment to seek potential talents in reputable universities and empowering them to thrive with RSM Indonesia.

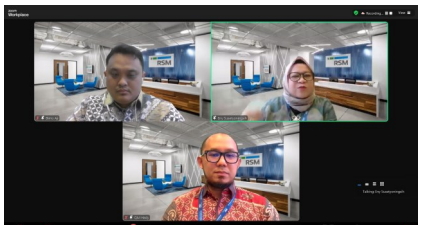
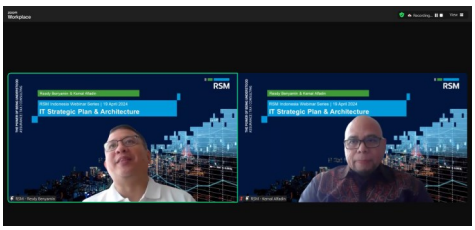
See you at our next Career Days event!

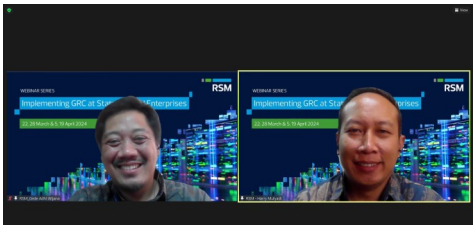

RSM INDONESIA WEBINAR

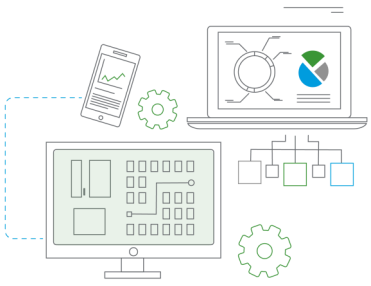
We successfully conducted several tax and consulting webinars during the 2nd quarter of this year. More than 100 participants attended each webinar and delivered by our Senior Manager and Partners. The webinars covered updates on tax and GRC Implementation for State-Owned Enterprises.

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



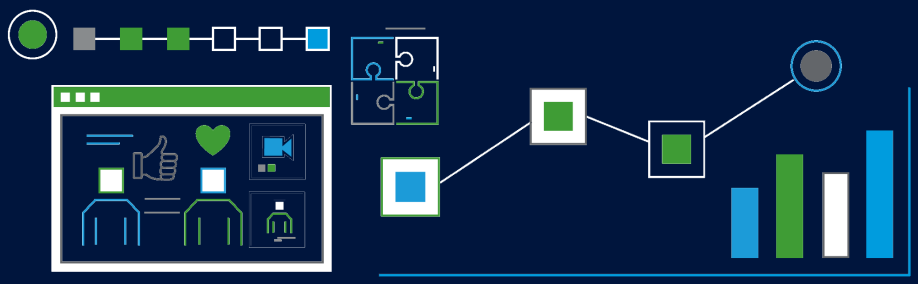




THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

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