THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

QUARTER III – 2024

RSM

WAKE UP CALL

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

Welcome to issue 70 of Wake Up Call – RSM Indonesia newsletter covering topics on audit, tax and consulting.

IN THIS ISSUE:

Due Diligence: Unveiling Competitive Insights

SYAHRIZAL MUSA, CONSULTING PRACTICE

In the fast-paced world of business, staying ahead of the competition is paramount for sustained success. Companies constantly seek ways to innovate, improve, and overtake rivals.

One powerful tool in their arsenal is due diligence. While typically associated with mergers, acquisitions, or investments, due diligence also serves as a potent means for companies to glean valuable insights from their competitors.

UNDERSTANDING DUE DILIGENCE

Due diligence is a comprehensive investigation and analysis process conducted by companies before engaging in significant transactions, such as mergers, acquisitions, or investments. It involves scrutinizing various aspects of a target company's operations, finances, legal status, and overall viability.

However, beyond its traditional applications, due diligence can be effectively employed by companies to study their competitors.

WHY IS DUE DILIGENCE CRUCIAL AS A LEARNING TOOL?

- Deep Dive into Competitor Operations
  Conducting due diligence on competitors provides an unparalleled opportunity to gain a comprehensive understanding of their strategies, business models, market positioning, and operational processes. This insight goes beyond surface-level observations, offering a nuanced view of how competitors operate and compete in the market.
- Identifying Strengths and Weaknesses
  Through meticulous examination, companies can identify their competitors' strengths and weaknesses. Understanding what sets competitors apart and where they fall short enables companies to capitalize on their own strengths and exploit competitor weaknesses to gain a competitive edge.
- Anticipating Market Moves
  By closely scrutinizing competitors, companies can anticipate their next moves and strategic initiatives. Whether it's launching new products, entering new markets, or adjusting pricing strategies, insights gained through due diligence empower companies to proactively respond to market dynamics and competitor actions.
- Discovering Untapped Opportunities
  In the process of analyzing competitors, companies may uncover untapped market opportunities or areas where competitors are underperforming.
- Mitigating Risks
  Through due diligence, companies can identify and mitigate potential risks associated with engaging with competitors. Whether it's legal liabilities, financial instability, or reputational risks, thorough due diligence enables companies to make informed decisions and safeguard their interests.

STEPS TO CONDUCT DUE DILIGENCE ON COMPETITORS

- **Define Objectives**: determine what specific information you aim to uncover about your competitors.
- **Gather Intelligence**: collect data from various sources, including public filings, industry reports, news articles, social media, and networking events.
- **Analyze Findings**: analyze the gathered data to extract meaningful insights and patterns.
- **Benchmark Performance**: compare competitors' performance metrics against industry benchmarks and your own company's performance.
- **Develop Actionable Strategies**: based on the insights gained from due diligence, develop actionable strategies to enhance your competitive position.

- **Monitor Competitor Activity**: due diligence is an ongoing process. Continuously monitor competitors' activities, market trends, and industry developments to stay abreast of changes and adapt your strategies accordingly.

STRATEGIC DATA

In carrying out due diligence, usually acquiring parties will request strategic data that includes:

1. List of Customer Details, for the top 10 to 20 Customers that cover majority of customers for the last 3 to 5 years in the form of:
   a. Customer name, address, contact persons
   b. The area where each customer is served
   c. Types of goods/services provided to each customer
   d. Number of units and in Rupiah for goods/services provided to customer
2. List of Supplier Details, for the top 10 to 20 Suppliers for the last 3 to 5 years in the form of:
   a. Supplier name, address, contact person
   b. The region where each supplier is obtained
   c. Types of goods/services provided to each supplier
   d. Number of units and in Rupiah for goods/services provided to the supplier
3. Company Strategy, Processes, Policy, System and Procedures for:
   a. Purchasing
   b. Production
   c. Storage and warehousing
   d. Sales and marketing
   e. Human resources
   f. Recording/accounting
4. List of Key Personnel, consisting of
   a. Key personnel names
   b. Curriculum Vitae of key personnel
   c. Addresses and contact numbers
   d. Compensation and benefit given
5. Other relevant factor that are important

CONCLUSION

In conclusion, due diligence serves as a powerful tool for companies to learn from their competitors and gain a competitive advantage in the market.

By conducting thorough investigations, companies can uncover valuable insights, anticipate market moves, identify opportunities, and mitigate risks.

Incorporating due diligence into strategic decision-making processes enables companies to stay ahead of the curve, adapt to changing market conditions, and drive long-term success.

In today's hypercompetitive business environment, leveraging due diligence as a tool for competitive intelligence is not just advantageous – it's essential for survival and growth.

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

Preparing for Indonesia's New Data Protection Law: What your Business Needs to Know

ERIKMAN D PARDAMEAN, TECHNOLOGY RISK CONSULTING PRACTICE

As Indonesia prepares to fully enforce its Personal Data Protection Law (UU PDP) after 17 September 2024, businesses are facing a critical decision point. With the deadline rapidly approaching, organizations must either take proactive measures to ensure compliance or risk significant challenges once the law takes full effect. The clock is ticking, and organizations that delay may face substantial hurdles as they scramble to meet the new requirements.

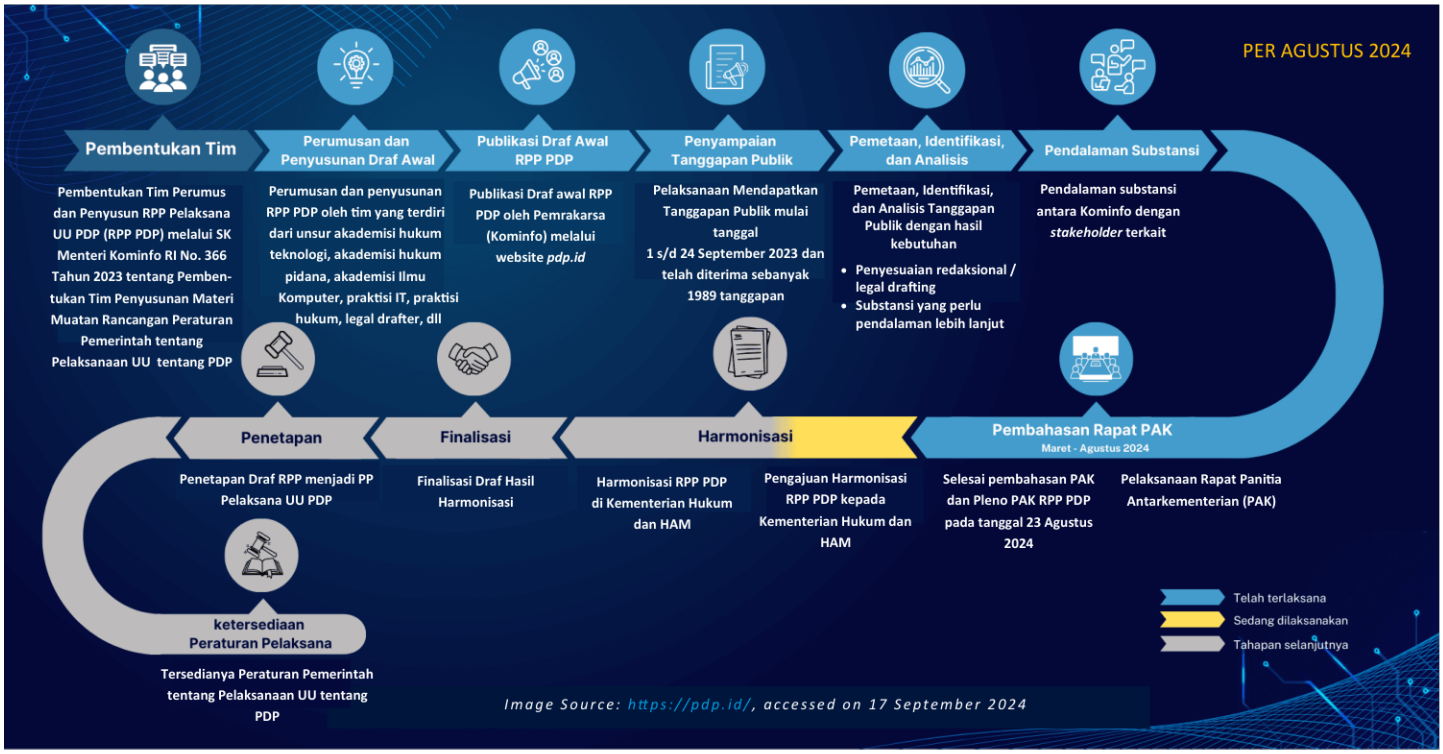
The UU PDP marks a significant shift in personal data management, aligning Indonesia's practices with global standards such as the EU's General Data Protection Regulation (GDPR). It aims to safeguard personal data and ensure that businesses handle it responsibly. However, despite the impending full implementation, several key issues remain unresolved, creating uncertainty for businesses on how to proceed.

Non-compliance with the UU PDP carries serious consequences. Organizations face administrative fines of up to 2% of annual revenue, in addition to potential criminal penalties. This article outlines what businesses need to know and provides a clear guide on how to effectively prepare for the upcoming regulations.

CURRENT LANDSCAPE OF UU PDP IN INDONESIA

While the law is about to take full effect, there are still a few strategic issues that are yet to be finalized, adding to the complexity of compliance for businesses:

1. Pending Government Regulations (PP)
   One of the most significant hurdles is that the detailed Government Regulations (*Peraturan Pemerintah*, PP) accompanying the UU PDP are still in draft form. These regulations will cover important aspects like data processing activities, data disclosure, and penalties for violations. Without this clarity, businesses are left uncertain about the exact steps they need to take to comply fully with the law.



2. Absence of a Data Protection Supervisory Body
   The law calls for an independent supervisory authority, *Lembaga Pengawas Perlindungan Data Pribadi*, to oversee and enforce data protection regulations. According to Article 58, this body is expected to set data protection strategies and policies while also enforcing administrative sanctions. While it will ultimately report to the President, for now, it will coordinate with the Ministry of Communication and Information Technology (Kominfo). The absence of this supervisory authority makes businesses unsure of how enforcement will play out in practice.
3. Overlapping Regulations
   Indonesia has multiple existing data protection regulations that overlap with the UU PDP. This can cause confusion, particularly for companies in sectors with complex regulatory requirements. Clearer harmonization between these laws is needed to avoid compliance issues.

TOP CHALLENGES FOR BUSINESSES IMPLEMENTING UU PDP

As businesses prepare for the UU PDP, they are encountering several challenges. Below are the 3 most pressing:

Compliance Readiness

Many organizations, especially small and medium-sized enterprises (SMEs), are not fully prepared for the law's requirements. They need to upgrade their data protection systems, create privacy policies, and enhance cybersecurity measures. Delaying these preparations can lead to significant penalties and damage to reputation.

Appointing a Data Protection Officer (DPO)

The UU PDP requires organizations to appoint a Data Protection Officer (DPO) if they handle substantial amounts of personal data. Finding and training qualified DPOs is a challenge, particularly in technology and finance sectors. This shortage adds complexity to achieving compliance.

Enforcement and Penalties

One of the biggest concerns businesses have been the strict penalties outlined in the UU PDP. Media coverage has highlighted the severity of potential fines and criminal charges, making it a top worry for business leaders. The uncertainty surrounding how the law will be enforced also adds to the anxiety, as organizations are unsure of what operational changes are needed to avoid penalties.

ESSENTIAL STRATEGIES FOR IMMEDIATE ACTION

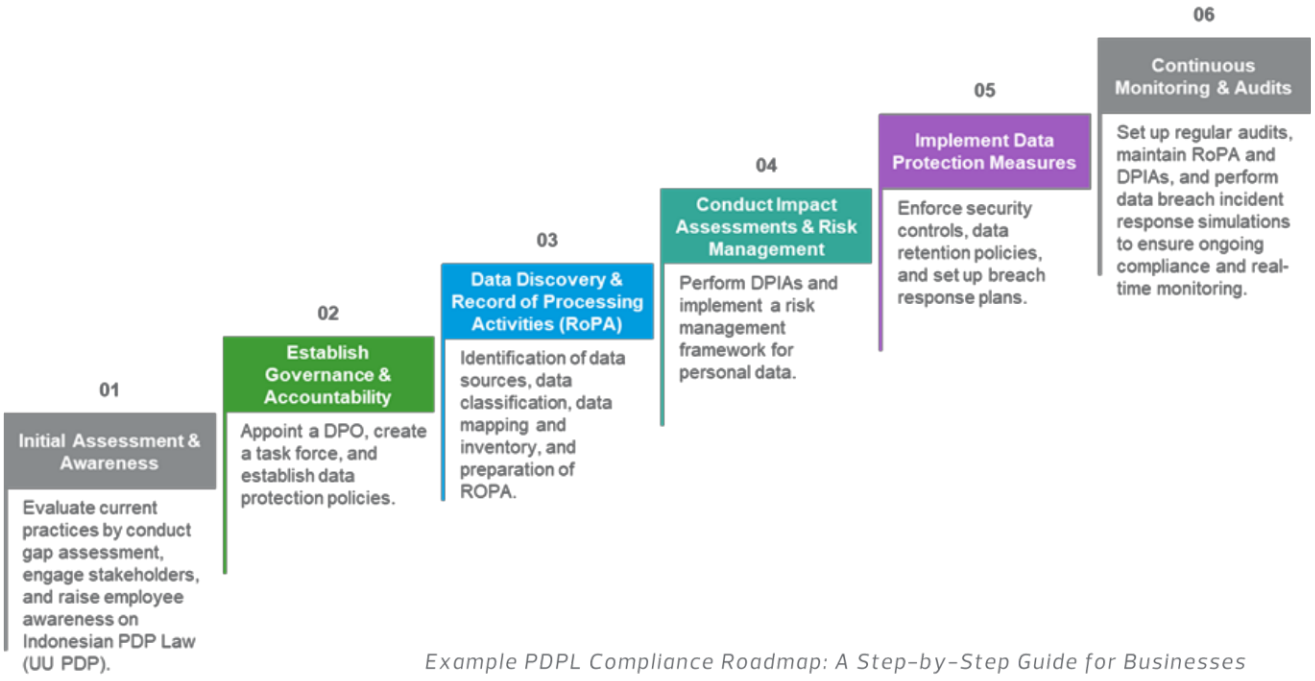
With the full implementation date approaching, businesses cannot afford to wait. Here are some quick-win strategies that can help companies kick-start their compliance journey:

Conduct a Readiness or Gap Assessment

The first step is to assess your organization's current data protection practices and identify any gaps in compliance with the UU PDP. This includes reviewing your data collection, processing, and storage practices, as well as evaluating your privacy policies and security measures.

Develop a Compliance Roadmap

Once gaps are identified, develop a phased roadmap to address them. This should include updating internal processes, securing personal data, and ensuring that data protection measures are integrated into your business operations.



Example PDPL Compliance Roadmap: A Step-by-Step Guide for Businesses

Appoint or Train a Data Protection Officer (DPO)

If your business is required to appoint a DPO, start the recruitment process now. Alternatively, you can train an existing employee who has a solid understanding of data protection laws and can take on the role of DPO with the right guidance.

Vendor Management and Third-Party Audits

Review your contracts with vendors and partners to ensure they are aligned with the UU PDP. Conduct third-party audits to confirm that they are also complying with data protection laws. This can help minimize risks associated with non-compliant partners.

CONCLUSION: ACT NOW TO STAY AHEAD

Despite the uncertainties, it's crucial for businesses to start preparing for the UU PDP now. The best approach is to conduct a readiness assessment to identify any gaps in your current data protection practices. From there, develop a phased compliance strategy to address these gaps and ensure you are ready when the law takes full effect.

Taking early action not only helps avoid last-minute compliance issues but also builds trust with your customers by demonstrating a commitment to protecting their personal data. The UU PDP presents an opportunity to enhance your data management practices and strengthen your business's reputation.

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

Inside the NSA Data Leak and CrowdStrike's Misstep: Strengthening your Third-Party Risk Management

SATRIO BAYU PANDOWO, TECHNOLOGY RISK CONSULTING PRACTICE

The global internet community has recently been rocked by startling news of the CrowdStrike epic fail and the National Security Agency (NSA) data leak. Numerous businesses globally have experienced significant disruptions to their Windows workstations due to a flawed update released by cybersecurity firm CrowdStrike on Friday afternoon 19 July 2024 *(source: Faulty CrowdStrike Update Crashes Windows Systems, Impacting Businesses Worldwide (thehackernews.com) – 19 July 2024).*

The core issue was a faulty sensor configuration update within CrowdStrike's Falcon platform. This update, intended to enhance security, inadvertently triggered a logic error on millions of Windows systems. This error resulted in system crashes and the infamous Blue Screen of Death (BSOD), severely disrupting operations across various industries.

On the other story, the recent online exposure of 1.4GB of NSA data *(source: cyberpress.org By Balaji – 8 July 2024)*, containing Personal Identifiable Information (PII) such as full name, phone numbers and email addresses, sent shockwaves through the cyber-security world. The NSA is a United States government agency responsible for global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes.

Threat actors claim that the data was allegedly obtained from Acuity Inc data breach., a company that works closely with the United States government and its allies. But here's the chilling truth: this breach isn't just a headline – it's a wake-up call for every organization that relies on third-party vendors. And chances are, that's you.

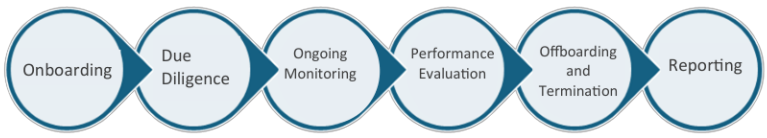


Figure 1.0: Third-Party Risk Management

THE HIDDEN THREAT LURKING IN YOUR SUPPLY CHAIN

Think of your business as a fortress. You've got strong walls, vigilant guards, and top-notch security systems. But what about the back door? The one your trusted partners use. That's where the danger lies – in the intricate web of third-party relationships that keep your business running.

The CrowdStrike fail story and the NSA leak proves that even the most secure organizations are vulnerable when their partners aren't. A single weak link, a lax security practice, a compromised employee at a vendor – any of these can become the Achilles' heel of your entire operation.

On the CrowdStrike story, as IT teams scrambled to restore services, cybercriminals exploited the chaos, distributing malware disguised as fixes or updates. Remcos RAT, a notorious remote access trojan, was among the malicious payloads spread during the crisis.

This added another layer of complexity and risk to an already dire situation. On the other situations, it could be many scenarios affected your business as IT Third-Party risk shown on figure 1.1.

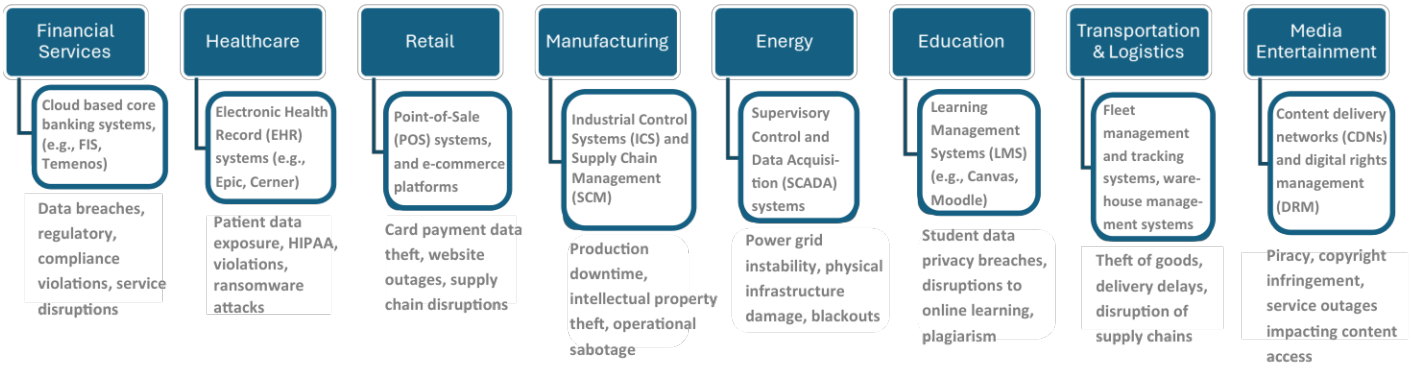


Figure 1.1: Example IT Third-Party Risk Within Industries

PICTURE THIS: YOUR BUSINESS OPERATION SUDDENLY STOPPED AND YOUR DATA EXPOSED

Imagine your business operations suddenly stopped and your customer data splashed across the dark web. Businesses, hospitals, schools, and government agencies across the world were impacted as critical systems went offline. Financial records, personal details, confidential information – all up for grabs by cybercriminals. It's a nightmare scenario, but it's happening every day. And if you're not actively managing your third-party risk, you're practically rolling out the red carpet for hackers.

SEEING INSIDE THE BLACK BOX: TECHNICAL MONITORING

But how can you truly know what's happening behind the scenes at your third-party vendors?

Rigorous Testing: Implement a comprehensive and multi-layered testing strategy that includes extensive simulations and real-world scenarios to catch potential logic errors before updates are released.

Phased Rollouts: Instead of pushing updates to all systems simultaneously, adopt a phased approach. Start with a small, controlled group and gradually expand the rollout, closely monitoring for any anomalies.

Rollback Mechanisms: Ensure the ability to quickly revert to a previous, stable version of the software if a critical issue is detected in a new update.

Vulnerability Scanning: Regularly scan your vendors' systems for known vulnerabilities using tools like Nessus, Qualys, or OpenVAS. This can reveal outdated software, misconfigurations, or other weaknesses that hackers could exploit.

Penetration Testing: Go a step further by simulating real-world attacks to test the resilience of your vendors' security controls. Ethical hackers can uncover vulnerabilities that automated scans might miss.

Security Configurations Assessment and Attack Surface Management: Platforms such as CIS Benchmark, BitSight, SecurityScorecard, and Wazuh continuously assess your vendors' security posture based on publicly available data like leaked credentials, malware infections, or outdated software. They provide an easy-to-understand rating that reflects their overall security hygiene.

Cloud Security Posture Management (CSPM): If your vendors operate in the cloud, CSPM tools (e.g., Wiz, Orca Security) can monitor their cloud configurations for misconfigurations, compliance violations, and potential security gaps.

TAKE CONTROL: DON'T BE THE NEXT VICTIM

Don't wait for disaster to strike. Take proactive steps to safeguard your business from the inside out:

Comprehensive Due Diligence: Before onboarding any third party, conduct thorough risk assessments. Scrutinize their security practices, data handling procedures, incident response capabilities, and compliance with relevant regulations (e.g., UU No 27 Tahun 2022 tentang Pelindungan Data Pribadi, PBI No 4 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber Bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia, or other related regulation such as GDPR, and CCPA). Don't just rely on self-reported information; verify their claims through independent audits or security questionnaires.

Continuous Monitoring: Third-party risk isn't a "set it and forget it" proposition. The threat landscape is constantly evolving, and so are the risks posed by your vendors. Implement ongoing monitoring to track changes in their security posture, identify emerging vulnerabilities, and ensure they maintain compliance with your contractual requirements.

Clear Contractual Agreements: Establish clear and comprehensive contracts with your third parties that explicitly outline their security obligations, data protection responsibilities, and breach notification procedures. Include provisions for regular audits and the right to terminate the relationship if they fail to meet their security commitments.

Incident Response Planning: Develop and test incident response plans that specifically address third-party breaches. Ensure you have clear communication channels with your vendors and a well-defined process for coordinating response efforts in the event of an incident.

Leverage Industry Standards: Utilize established frameworks like NIST Cybersecurity Framework, ISO 27001/27002, or Shared Assessments SIG to guide your third-party risk management program. These provide best practices and standardized approaches for identifying, assessing, and mitigating third-party risks.

THE TIME TO ACT IS NOW

The NSA data leak is a stark reminder that no one is immune to cyber threats. Don't become another statistic. Take charge of your third-party risk management today and protect your business from tomorrow's headlines. Remember, cybersecurity isn't just about technology – it's about vigilance, preparedness, and a commitment to safeguarding your most valuable assets.

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

INDONESIA **FACTS**

GESOK-GESOK – traditional musical instruments

This is a traditional musical instrument from South Sulawesi with strings known as Gesok-gesok. This instrument is made of wood and animal skin. Gesok-gesok is a traditional musical instrument that is played by strumming. This instrument is shaped like a heart equipped with a stick and only has two strings. Gesok-gesok is generally played to accompany poems that contain advice about past history.

Source: Indeksmedia.id

Employment Matters! – Part 2

NICHOLAS GRAHAM, BUSINESS SERVICES PRACTICE

This is the final part of a multi-part article that first appeared in our Quarter II Wake Up Call highlighting some employment/HR matters that managers should be aware of to avoid mistakes that might jeopardize the relationship with employees and/or create risk of disputes.

Cuti Bersama – Mandatory, Free Leave or Ignore?

Cuti Bersama (CB) or collective leave applies to government employees, who are required to take leave on certain specified days linked to public holidays. These CB are deducted from the employee's annual leave entitlement.

The CB dates are not required to be followed by the private sector and therefore it is the private sector employer's decision whether it wishes to follow the CB or not. Frequently banks and institutions linked to the financial markets will follow these because the supporting government institutions (e.g. Bank Indonesia) are closed.

Private sector employers can decide whether to ignore the CB, offer a free/office holiday or require that some CB are followed (mandatory leave with deduction from the employee's leave balance). The employer should document the policy in the relevant agreements.

Long Service Leave

Since the enactment of the 2003 Manpower Law, employers are not required to offer long service leave. However, if they did offer long service leave, then certain minimum requirements were stipulated.

The 2020 Job Creation Law has removed these minimum requirements, leaving these to be regulated by ministerial regulation. That regulation states that any provisions regarding long service leave shall be determined by the employer and documented in the relevant agreements. Therefore, at present, it is the employer's discretion whether it will offer long service leave and on what basis. However, any existing long service leave will need to follow the existing agreed terms.

Updated maternity & paternity benefits – Law 4 on Maternal & Child Welfare during the first 1000 days of life

Law No. 4 on Maternal & Child Welfare during the first 1000 days of life (Law No. 4) was signed by the President on 2 July 2024, with immediate effect.

Although Law No. 4 is subject to the issue of implementing regulations that must be issued within 2 years of 2 July 2024, there are several requirements that employers should be aware of.

Mothers are entitled to maternity leave of:

- A minimum of the first 3 months; and
- Up to an additional 3 months if there are special conditions (such as the mother experiencing health problems, complications after childbirth or miscarriage; or health problems or complications experienced by the newborn child). A doctor's certificate is required as evidence for an additional leave.

The salary entitlement during this period is:

- Full salary for the first 3 months;
- Full salary for the fourth month;
- 75% of the salary for the fifth and sixth months.

The base 3-month paid leave entitlement is consistent with the existing law and regulations, however, the additional leave and related salary for leave exceeding 3 months is new.

If the expected mother suffers a miscarriage then she is entitled to 1.5 months paid leave or the period specified in a certificate from a doctor, obstetrician or gynecologist, or a midwife.

This is also consistent with the existing law and regulations. However, it appears there might also be an entitlement for up to 6 months if this is supported by a doctor's certificate. This view is based on the stipulation that the "special conditions" referred to above also include a miscarriage. It is hope this will be clarified when the implementing regulations are issued. Assuming our view is correct then the salary due would also follow the above entitlement to full salary for the first four month and then 75% of salary for the fifth and sixth months.

A provision that is likely to create some concern for employers is the obligation for employers to support mothers by providing:

- Space for lactation
- Daycare

As suggested in the elucidation to Law No.4, this obligation might be limited to workplaces where is there are sources of danger. It is hoped the relevant implementing regulation will be promptly issued to clarify employer's obligations for these matters.

Failure to provide these facilities will result in guidance and/or administrative sanctions in accordance with applicable laws and regulations. This might be stipulated in the implementing regulations.

Compared to the current entitlement for 2 days leave in the event of the birth of his baby or a miscarriage, Law No. 4 provides the husband with:

- 2 days paid leave in the event of the birth of a baby that can be extended for up to 3 days additional paid leave or as agreed, or
- 2 days paid leave in the event of a miscarriage.

Further the husband should be "sufficient time" (*waktu yang cukup*) to accompany his wife and/or the child if:

- The wife has health problems, health disorders, and/or post-childbirth complications or miscarriage;
- The child is born with health problems, health disorders, and/or complications;
- The wife who gave birth passed away; and/or
- The newborn Child passed away.

The meaning of "sufficient time" and any limitations are not stipulated in Law No. 4 and might be explained in the implementing regulations.

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

RSM **PUBLICATION**

Healthcare is the prime target for cybercriminals. Cyber-attacks on healthcare have severe consequences. Beyond financial loss, patient safety, privacy, and service delivery are compromised

Click **here** to read more.

OUR **ACTIVITIES**

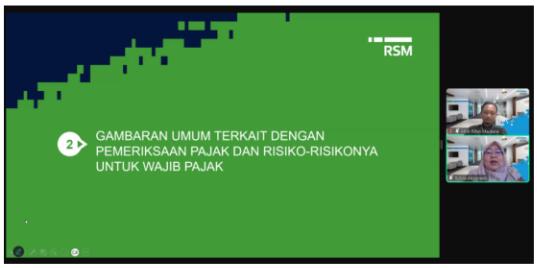
RSM INDONESIA HAS BEEN CERTIFIED AS **GREAT PLACE TO WORK** FOR THE 2ND CONSECUTIVE YEAR

We are proud to share that we have been Certified™ by Great Place To Work® for the second year in a row for period September 2024 – September 2025.

None of it would be possible without our team's contribution for the growth and positive environment in RSM Indonesia.

View our result at Great Place to Work website **here**.

RSM INDONESIA WEBINAR



We held 2 webinars on tax throughout Q3 2024 with total attendees of those webinars sum up to 150 participants.

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

RSM INDONESIA AT ACIIA REGIONAL CONFERENCE 2024

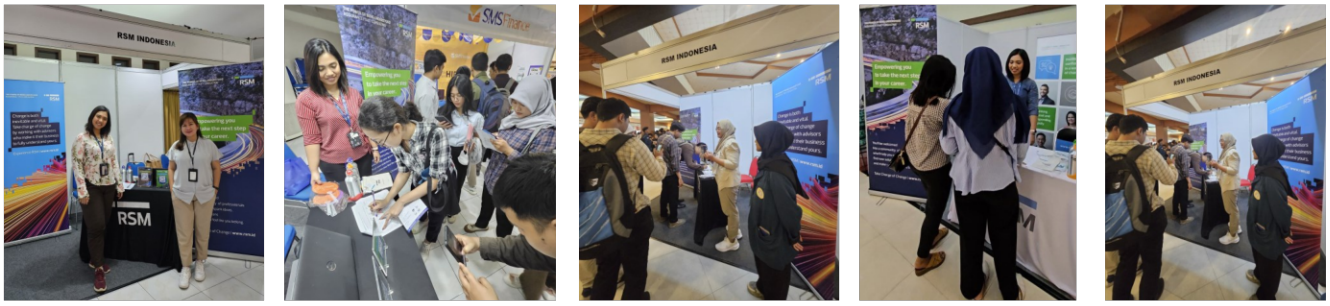
On 28–29 August 2024, we participated in Asian Confederation of Institutes of Internal Auditors (ACIIA) Regional Conference in Bali. Over 750 professionals from 19 countries attended this event. At this event, we connected with GRC professionals and catch up with them on latest issues related to governance, risk management, internal audit, and technology.

OUR **ACTIVITIES**

CELEBRATE INDEPENDENCE DAY AT RSM INDONESIA

We celebrated the 79th Independence Day of Indonesia in our office. Began with flag ceremony and followed by traditional games competition. All staffs, whether they are participating in these games or supporting from the sidelines, are having fun.

RSM INDONESIA GOES TO CAMPUS

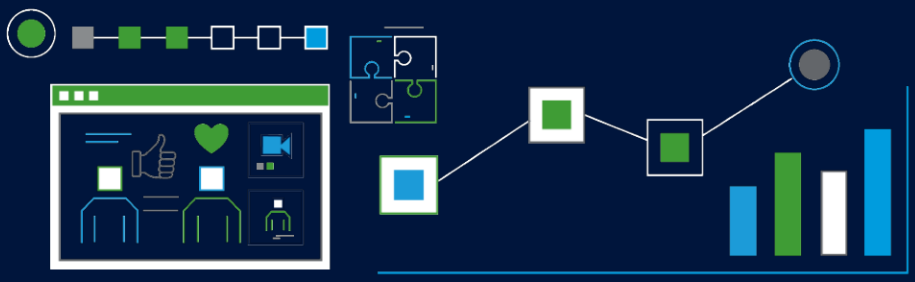


On 3rdquarter of this year, we participated in campus events at Universitas Diponogoro Semarang, Universitas Bina Nusantara Jakarta, Universitas Telkom Bandung, and Universitas Airlangga Surabaya. More than 100 students joined the events. This is one of our commitment to gather the brightest talents from reputable universities who wants to elevate their career with RSM Indonesia. See you at our next campus event!

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