RDS ADVOCATES & SOLICITORS

In Business Collaboration:

AMT / ANDERSON MORI & TOMOTSUNE

The Risk Mitigation Code: Online Safety Is Now A Boardroom Issue

27 July 2026

For more information, please contact:

Datuk D P Naban
naban@rdslawpartners.com

Austen Emmanuel Pereira
austen@rdslawpartners.com

Bahari Yeow Tien Hong
bahari@rdslawpartners.com

Farah Shuhadah Razali
farah@rdslawpartners.com

Tan Sri Datuk Harmindar Singh Dhaliwal
harmindar@rdslawpartners.com

Kenny Lam Kian Yip
kenny@rdslawpartners.com

Lim Zhi Jian
jian@rdslawpartners.com

Michael Soo
michaelsoo@rdslawpartners.com

Rosli Dahlan
rosli@rdslawpartners.com

Steven Perian KC
speriankc@rdslawpartners.com

Vinayak Sri Ram
vinayak@rdslawpartners.com

The Risk Mitigation Code (RMC), issued by the Malaysian Communications and Multimedia Commission (MCMC) under the Online Safety Act 2025 (ONSA) came into force on 1 June 2026. While ONSA established the legal framework for regulating harmful online content, the RMC provides the operational blueprint for how licensed online platforms are expected to discharge those statutory obligations.

The significance of the RMC extends beyond regulatory compliance. It marks a broader shift in the governance of digital platforms. Matters that were previously determined largely by platform policy including user verification, advertiser due diligence, content moderation, algorithm design and internal oversight have now become subject to enforceable regulatory standards.

For businesses operating online platforms, advertising on digital services or protecting valuable brands online, the RMC represents a development that warrants immediate attention.

From Principles To Enforceable Standards

The RMC now gives practical effect to those statutory obligations. It applies to licensed service providers under the Communications and Multimedia Act 1998 (CMA), including providers of social media services, internet messaging services and online content platforms.

Importantly, the deeming provision under Section 46A of the CMA continues to play a significant role. Internet messaging and social media services with eight million or more users in Malaysia are automatically treated as licensed operators without any formal licensing application.

This ensures that many of the world's largest digital platforms fall squarely within Malaysia's regulatory framework.

The RMC therefore represents more than implementation guidance. It establishes the benchmark against which platform governance is likely to be measured by regulators, business partners and, potentially, the courts.

Why The RMC Matters

Historically, many aspects of online safety were left to the discretion of platform operators.

Policies governing anonymous accounts, advertiser verification, recommendation algorithms and content moderation were largely commercial decisions shaped by individual platform policies and community standards.

The RMC fundamentally changes that position. These areas are now subject to regulatory oversight.

The implications extend well beyond interactions with MCMC. Compliance with the RMC is likely to become increasingly relevant in commercial contracting, advertising relationships, corporate governance, regulatory investigations, mergers and acquisitions involving technology businesses, and disputes concerning online fraud or harmful content.

In that sense, the RMC should not be viewed merely as a compliance document. It is becoming part of the governance architecture of Malaysia's digital economy.

Six Pillars Of The Risk Mitigation Code

The RMC is built around six core obligations that collectively require platforms to adopt a proactive and risk-based approach to online safety.

1. Risk Assessment Becomes an Ongoing Governance Function

Platforms must conduct "suitable and sufficient" assessments of harmful content risks. This extends beyond identifying unlawful content. The assessment must consider service design, user demographics, behavioural trends and heightened-risk situations such as elections, public emergencies and national crises.

Where children may access the service, separate child-specific assessments conducted by individuals with appropriate expertise are required.

Importantly, these assessments are not one-off exercises. They must be documented, reviewed annually and updated whenever material changes occur.

The emphasis is therefore on continuous governance rather than periodic compliance.

2. Anonymous Content Is No Longer the Default

The RMC requires platforms to ensure that content is communicated only by registered users.

While anonymous browsing may remain possible depending on the platform, anonymous participation is no longer regarded as an acceptable default for user-generated content.

This reflects a broader international trend towards greater user accountability as a means of reducing scams, abuse and other harmful online behaviour.

3. Advertiser Verification Raises The Compliance Bar

One of the most commercially significant changes concerns paid advertising. Platforms may only publish advertisements for goods or services where advertisers have first been verified against government-issued identification documents.

For individuals, this includes MyKad, passports and work permits. For organisations, verification extends to certificates of incorporation and other official registration documents.

Where Malaysian government records are unavailable, equivalent documents issued by competent foreign authorities may be accepted.

Although the legal obligation rests with the platform, the practical burden will inevitably fall upon advertisers.

Businesses should therefore expect enhanced onboarding procedures before advertising campaigns can be launched.

For multinational organisations operating across several jurisdictions, advertiser verification is likely to become a routine compliance requirement within digital marketing operations.

4. AI-Generated Content Comes Under Regulatory Scrutiny

The RMC directly addresses one of the fastest-evolving areas of digital regulation: synthetic media.

Platforms must ensure that AI-generated or manipulated images, audio and video that closely resemble real persons, places, objects or events and are likely to appear authentic are clearly distinguishable through prominent labels or other appropriate markings.

Where content creators or advertisers disclose the use of AI-generated material, platforms must also provide accessible mechanisms to facilitate that disclosure.
The implications extend beyond platform operators.

Businesses increasingly using generative AI for advertising campaigns, digital influencers, promotional videos and customer engagement should anticipate greater scrutiny over transparency and disclosure.

As synthetic media becomes increasingly sophisticated, organisations should review their internal approval processes to ensure AI-generated marketing materials comply not only with evolving platform requirements but also with regulatory expectations.

5. Recommendation Algorithms Become a Regulatory Concern

Perhaps one of the most significant developments is that regulatory attention now extends beyond content itself to the architecture through which content is delivered.

Platforms must regularly evaluate and adjust recommendation systems and algorithms to reduce users' exposure to harmful content. This reflects an important policy position adopted by MCMC.

Regulators are no longer concerned solely with whether harmful content exists on a platform. They are equally concerned with whether platform design unintentionally amplifies or promotes such content.

This places algorithmic governance alongside content moderation as a central regulatory issue.

6. Online Safety Is Now a Boardroom Responsibility

Perhaps the most significant feature of the RMC is its governance dimension.
Platforms must establish an internal assurance function responsible for monitoring the effectiveness of risk mitigation measures, with regular reporting to the audit committee or governing body.

This represents a clear shift away from treating online safety as solely the responsibility of trust and safety teams or operational personnel. Boards should increasingly expect regular reporting on matters such as:

- harmful content trends;
- effectiveness of moderation systems;
- algorithmic risks;
- advertiser verification;
- AI-generated content;
- regulatory complaints; and
- implementation of mitigation measures.

Online safety is becoming another component of enterprise risk management, sitting alongside cyber security, privacy and ESG.

Flexibility Within The Regulatory Framework

Notably, the RMC does not prescribe a single compliance model. Platforms may implement alternative measures in place of those specifically described in the Code, provided they can demonstrate to MCMC that the alternatives better achieve the intended risk mitigation objectives.

This principles-based approach allows innovation while preserving regulatory accountability.

Harmful Content: The Regulatory Priority

The RMC applies to the categories of harmful content listed in the First Schedule to ONSA, including:

- child sexual abuse material;
- financial fraud;
- obscene and indecent content;
- harassment;
- terrorism and violent extremism;
- content encouraging child self-harm;
- content promoting hostility or public ill-will; and
- dangerous drugs.

Among these, child sexual abuse material and financial fraud receive particular regulatory attention as priority harmful content, attracting heightened obligations and more urgent response expectations.

Beyond Financial Penalties: The Broader Consequences Of Non-Compliance

The maximum statutory penalty of RM10 million understandably attracts attention. However, financial penalties are unlikely to represent the greatest commercial risk.

Regulatory investigations may expose weaknesses in governance, moderation systems and internal controls, potentially affecting corporate reputation, advertiser confidence and stakeholder trust.

Where harmful content results in consumer losses or reputational damage, deficiencies identified during regulatory investigations may also become relevant in civil litigation, contractual disputes and shareholder scrutiny.

For many businesses, the reputational consequences of regulatory intervention may ultimately prove more significant than the financial penalty itself.

What Businesses Should Do Now?

Although the RMC is directed primarily at Licensed Service Providers, its practical impact extends much further.

- Advertisers - Businesses relying on paid digital advertising should prepare for enhanced verification procedures and review internal onboarding processes with platform providers.

- Brand Owners - Companies whose brands are targeted by scams, impersonation or fraudulent advertising should consider incorporating the RMC into their broader brand protection strategies. The regulatory framework now provides additional avenues through which rights holders may seek platform intervention.

- Businesses Using AI - Marketing teams should review internal governance surrounding AI-generated content, influencer campaigns and synthetic media to ensure appropriate transparency and disclosure before publication.

- Platform Operators - Operators within the licensing regime should undertake a comprehensive gap analysis against the RMC, reviewing governance structures, moderation policies, algorithmic oversight, documentation processes and board reporting mechanisms.

Part Of A Global Regulatory Trend

Malaysia is not regulating online safety in isolation. The RMC reflects developments seen internationally, including the United Kingdom's Online Safety Act 2023, Australia's Online Safety Act 2021 and the European Union's Digital Services Act.

The common direction is unmistakable.

Governments are increasingly regulating not merely harmful content itself, but the governance systems, algorithms and corporate decision-making processes that influence how such content is created, amplified and managed.
Malaysia has now joined that global movement.

Conclusion

The Online Safety Act 2025 established the legal framework. The Risk Mitigation Code brings that framework into operation.

Together, they represent a significant evolution in Malaysia's regulation of digital services. Online safety is no longer a matter of platform discretion or corporate policy. It is becoming an integral component of regulatory compliance, corporate governance and enterprise risk management.

Businesses that approach the RMC solely as another compliance exercise risk overlooking its broader commercial significance. Those that integrate online safety into governance frameworks, marketing practices, technology design and enterprise risk management will not only be better positioned to comply with Malaysian law but will also strengthen trust with regulators, users, investors and commercial partners in an increasingly regulated digital economy.

KUALA LUMPUR	PENANG	JOHOR BAHRU
Level 16, Menara 1 Dutamas No. 1, Jalan Dutamas 1, Solaris Dutamas, 50480 Kuala Lumpur T: +603 6209 5400 F: +603 6209 5411 enquiry@rdslawpartners.com	Suite S-21E & F21st Floor, Menara Northam, No. 55, Jalan Sultan Ahmad Shah, 10050 Penang T: +604 370 1122 F: +604 370 5678 generalpg@rdslawpartners.com	8-35, Menara Delima Satu, Jalan Forest City 1, Pulau Satu, 81550 Gelang Patah, Johor Bahru T: +607 585 6414 F: +607 509 7614 generaljb@rdslawpartners.com