

# Cyber Security Act 2024

## A new era for cybersecurity in Malaysia

The Cyber Security Act 2024 (the Act) has come into force on 26 August 2024. Together with four subsidiary regulations, the Act aims to strengthen Malaysia's cyber defences and enhance the country's resilience against emerging threats by putting the necessary measures in place.

A key concept introduced under the Act is the National Critical Information Infrastructure, or NCII. This refers to a computer or system that, if disrupted, would be detrimental to key national and government functions, public safety or public order of Malaysia.

The Act outlines roles and responsibilities of NCII Sector Leads and NCII Entities alongside licensing requirements for cybersecurity service providers.

### Key provisions

**NCII's obligations:** NCII entities must comply with specific cybersecurity measures, conduct risk assessments, audits and report incidents

**Licensing requirements:** Cybersecurity service providers must obtain service licences, with penalties for non-compliance

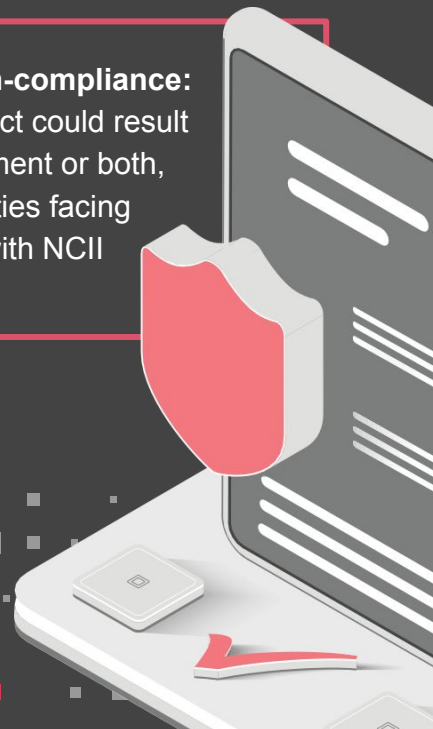
**Extraterritorial application:** The Act applies to offences affecting Malaysia's NCII, even if committed by foreign entities outside Malaysia

**National Cyber Security Committee:** The Act establishes the committee to oversee cybersecurity policies, chaired by the Prime Minister

**NACSA's role:** The National Cyber Security Agency (NACSA) is reinforced as the lead cybersecurity agency, empowered with regulatory and enforcement responsibilities

**Sector-specific governance:** Designated NCII Sector Leads must regulate entities in critical sectors

**Penalties for non-compliance:** Violations of the Act could result in fines, imprisonment or both, with stricter penalties facing non-compliance with NCII obligations



# Overview of the governance framework

## Cyber Security Act 2024

The Act is supplemented by four regulations which provide clarifications on the following areas.

### Period of risk assessment and audit

Obliges NCII Entities to conduct an annual risk assessment and an audit at least once every two years

### Incident notification

Obliges NCII Entities to report cybersecurity incidents to NACSA and NCII Sector Lead, and provide specific updates within stipulated time frames

### Compounding of offences

Lists six compoundable offences applicable to NCII Sector Lead, NCII Entities and/or cybersecurity service providers

### Licensing of service provider

Mandates all companies providing cybersecurity services to obtain valid licences with three exceptions.

## National Critical Information Infrastructure (NCII)

### National Cyber Security Committee

Oversee national cybersecurity policies

### Chief Executive of NACSA

Implements cybersecurity policies with authority to order enforcement and investigation

### NCII Sector Lead

Oversees each critical sector<sup>1</sup>, setting cybersecurity standards, establish code of practice, implementing NCSC's decisions and ensuring compliance

## Code of practice (COP)

### Implementation and providing information

Setting measures, standard of practice and providing information relating to NCII Entities

### NCII Entities' compliance flexibility

NCII Entities may propose alternative measures with approval from the NACSA Chief Executive if they offer equal or better protection, or establish measures based on internationally recognised standards or framework

### Cybersecurity risk assessments

NCII Entities are required to conduct cybersecurity risk assessments and audits

### Cybersecurity incident notification

NCII Entities must notify NACSA Chief Executive and NCII Sector Leads of any cybersecurity incidents

### NCII Entities

A government entity or person designated by Sector Lead to follow cyber security practices, conducting audits and reporting incidents

## Cybersecurity service provider

Anyone offering, advertising or representing themselves as a provider of cybersecurity services must be licensed unless involving systems outside Malaysia or related company (Holding, subsidiary, subsidiary of holding). The type of services that must be licensed includes:

- Managed security operation centre monitoring services:** monitoring another person's computer system for cyber threats and determining necessary responses
- Penetration testing:** Assessing cybersecurity vulnerabilities, simulating attack and recommending mitigation measures







Offence	Maximum penalty
Providing or advertising any cybersecurity services without a license	RM500,000 fine or 10 years' imprisonment, or both
Transferring or assigning license to any other person without approval	RM200,000 fine or 3 years' imprisonment or both
Breaching licensing conditions imposed on a cybersecurity provider	RM100,000 fine or 2 years' imprisonment or both
Failing to maintain records of cybersecurity services provided *	

\* compoundable offence

<sup>1</sup> The 11 NCII sectors are government, banking & finance, transportation, defence & national security, information, communication & digital, healthcare services, water, sewerage & waste management, energy, agriculture & plantation, trade, industry & economy, and science, technology & innovation

# Enforcement and penalties for NCII

Note: This list is non-exhaustive. There may be other offences detailed in the Act that are not included in this summary.

Obligation	Who	Offence	Maximum penalty (fine and/or years of imprisonment)
 <b>Compliance with code of practice</b>	NCII Sector Lead	Failing to prepare the code of practice	RM100,000
	NCII Entity	Failing to implement measures, standards and processes as specified in the code of practice	RM500,000 or 10 years or both
 <b>Provision of information</b>	NCII Entity	Failing to comply with NCII Sector Lead's request of information, or inform on new computer / system that qualifies as critical infrastructure *	RM100,000 or 2 years or both
	NCII Sector Lead	Failing to notify Chief Executive on any information received from NCII Entity on the above *	RM100,000
 <b>Cybersecurity risk assessment</b>	NCII Entity	Failing to conduct cybersecurity risk assessment *	RM200,000 or 3 years or both
		Failing to submit report to the Chief Executive within 30 days after cyber risk assessment *	
 <b>Audit</b>	NCII Entity	Failing to complete audit or submit an audit report by an auditor approved by the Chief Executive	RM200,000 or 3 years or both
		Failing to rectify audit report upon Chief Executive's request	RM100,000
 <b>Cybersecurity incident reporting</b>	NCII Entity	Failing to report a cybersecurity incident	RM500,000 or 10 years or both
 <b>Cybersecurity exercise</b>	NCII Entity	Failing to comply with the Chief Executive's directions on his intention to conduct a cybersecurity exercise *	RM100,000

\* compoundable offence

# Staying ahead

## Critical steps for Cyber Security Act 2024 compliance

### For NCII Organisations

The Act has significant implications for businesses designated as NCII. Compliance requires regular risk assessments, security measures and incident reporting which, in cases of non-compliance, may result in reputational and financial loss.



#### **Build a strategic compliance plan.**

Develop frameworks to meet regulatory requirements, ensuring readiness for any future legislative changes



**Ensure robust risk management processes.** Continuously assess and mitigate cybersecurity risks through proactive measures and regular audits



**Invest in and retain cybersecurity talent.** This helps to build a skilled workforce to address emerging threats and navigate the competitive demand for cybersecurity professionals



#### **Leverage technology and automation.**

Use advanced technologies and optimise processes to enhance threat detection, response and resilience



**Strengthen partnership and information sharing.** Foster collaboration across sectors to improve knowledge against threats and collective defense capabilities

### For other organisations

While they're not within the scope of the Act, non-NCII entities can prepare for potential regulatory expansion by staying informed about evolving cybersecurity regulations. Adopting practices in line with the Act can help enhance their security posture and demonstrate proactive compliance.



**Assess and align with the code of practice.** While not mandatory, aligning cybersecurity practices with the code of practice can strengthen defences and demonstrate proactive compliance



**Invest in cybersecurity talent.** Focus on attracting and retaining skilled cybersecurity professionals to address increasing demand.



**Improve threat detection and response.** Enhance capabilities and leverage advanced technologies to detect and respond to emerging threats



**Ensure data protection and privacy compliance.** Align cybersecurity measures with data protection laws to safeguard sensitive information

“

Cybersecurity isn't just the responsibility of IT or security teams; it's a collective duty across every level of an organisation.

The Cyber Security Act 2024 is a crucial and timely legislation that strengthens Malaysia's cyber defense capabilities, reinforcing our position in an increasingly digital and interconnected world.

Now is the time to reevaluate your cybersecurity strategies, ensure compliance with the new requirements, and invest in the necessary technologies and training to protect critical information infrastructure from evolving threats.

”



**Clarence Chan**

Digital Trust and  
Cybersecurity Leader,  
PwC Malaysia

+60 (12) 712 1285

[clarence.ck.chan@pwc.com](mailto:clarence.ck.chan@pwc.com)