Take5 for business

Volume 14 Issue 2 - 3 February 2025

Guidelines on information and network security for the communications and multimedia industry

The better the question.
The better the answer.
The better the world works

Shape the future with confidence

Building Malaysia's cyber resilience

In a landmark move, the Malaysian Communications and Multimedia Commission (MCMC) has released the Information and Network Security Guidelines (INSG) to elevate cybersecurity within the communications and multimedia sector.

The INSG is a proactive measure to improve Malaysia's internet by making it safer, protecting users and their privacy and countering against online threats. It is applicable for services providers under the Communications and Multimedia Act (CMA) 1998 and other industries as part of their cybersecurity measures.

Preparation to meet INSG safeguards will require significant effort from service providers, but it also presents an opportunity to safeguard Malaysia's overall digital ecosystem.

> "The INSG offers a robust framework, improving cybersecurity resilience and consumer protection, while avoiding additional regulation.
>
> This effort reflects a collective commitment from various sectors, contributing to a secure digital environment in Malaysia.

Jason Yuen
Malaysia Cybersecurity Leader; and Partner
Ernst & Young Consulting Sdn. Bhd.

Key highlights of the INSG

Best practices for improved capability and readiness in network and communication systems.

Security guidance and compliance requirements for resilient and sustainable network infrastructures.

Roles and accountabilities for board members, management and chief information security officers (CISOs).

Processes and technology solutions to address cyber threats and protect consumer interest.

Sources:

- *Information and Network Security Guidelines (INSG)*, MCMC, October 2024
- EY analysis

What are the accountabilities?

The INSG outlines strategic governance measures to effectively oversee and manage the evolving landscape of cyber threats. To ensure the highest level of oversight, organizations can consider the following roles and responsibilities:

Board members

- Review and approve a Technology and Cyber Risk Management Framework (TCRMF) and Cyber Resilience Framework (CRF) at least once every two years, to respond to significant technological or threat landscape changes.
- Retain ultimate responsibility for strategic oversight and policy approval on information and network security with adequate time given to manage cyber risks.
- Assign a person or a committee at the board level or a Board Audit Committee (BAC) with the responsibility to supervise the effectiveness of its risk management policy and its adaptability to evolving cybersecurity challenges.
- Approve the Technology and Cyber Risk Appetite (TCRA) and corresponding risk tolerance for technology-related events, aligning with the organization's risk appetite statement and the National Policy Objectives (NPO) stated in the CMA 1998.

Management

- Implement board-approved TCRMF and CRF into specific policies and procedures that are consistent with the approved risk appetite and risk tolerance supported by effective reporting and escalation procedures including periodical management reviews to discuss the TCRMF, CRF and cyber risk report.
- Establish a Technology Governance Committee (TGC) or its equivalent, with the role to provide guidance on the organization's technology plans, roadmaps, initiatives, investments and operations.
- Active involvement in continuous improvement of cybersecurity practices and periodically review, update and adapt the organization's cybersecurity strategies on new threats, emerging technologies and evolving business practices.

Chief information security officers (CISOs)

- Oversee the organization's security risk management and cyber resilience, reporting directly to the CEO or the board.
- Has end-to-end view of all cybersecurity systems, processes and governance in the organization and ensure the service provider's information assets and technologies are adequately protected.
- Maintain operational oversight of cybersecurity including developing audit frameworks and enforcing INSG compliance requirements.

Source: *Information and Network Security Guidelines (INSG)*, MCMC, October 2024

Risk and response: Crafting a risk management plan

The INSG is based on a risk-based approach and outlines the following requirements in crafting a cybersecurity risk management plan:

Technology and cyber risk management

- Establish a TCRMF as an integral part of the organization's Enterprise Risk Management (ERM).
- Develop a technology and cyber risk management policies and practices with specific provisions on assessment, evaluation and integration of emerging technologies.
- Make available an enterprise-wide cyber risk management approach that reflects the collective responsibility of business and technology lines.

Third-party provider management

- Ensure that the board and the management exercise effective oversight and address associated risks when engaging a third-party provider.
- Establish a comprehensive cybersecurity third-party risk management (CTPRM) function.
- Maintain and provide a list of third-party providers that have access to personal identifiable information (PII) data and its critical system to the Commission in a template as may be prescribed by the Commission from time to time.

Technology audit

- Establish a specialized internal technology audit function with a dedicated team, authority and resources.
- Ensure technology audits are dynamically aligned with the TCRMF and CRF objectives.
- Ensure the technology audits are designed to proactively identify vulnerabilities and assess the resiliency of the service provider's capability and capacity in managing cyber threats and recovering from cyber attacks.

Security assessment and audit

Conduct security assessments and audits that include:

- Penetration testing
- Compromise and compliance assessments
- Data center resilience
- Network risk assessment
- Cryptography audit
- Patch and end-of-line (EOL) assessment
- Assess control audit
- Cloud security assessment
- Third-party risk assessment
- Privacy impact assessment
- Information Security Management System (ISMS) audits

Collaborative intelligence and information exchange

Actively engage in sharing and exchanging information with the Commission and within the industry on a collaborative approach with the following considerations:

- Commission interaction
- Industry collaboration
- Threat intelligence exchange

Internal awareness competency building

Conduct cybersecurity and consumer or customer awareness and training programs at least annually that are tailored to specific roles and risks, reflecting the following:

- Phishing awareness
- Password hygiene
- Social engineering defense
- Data protection
- Incident reporting protocols

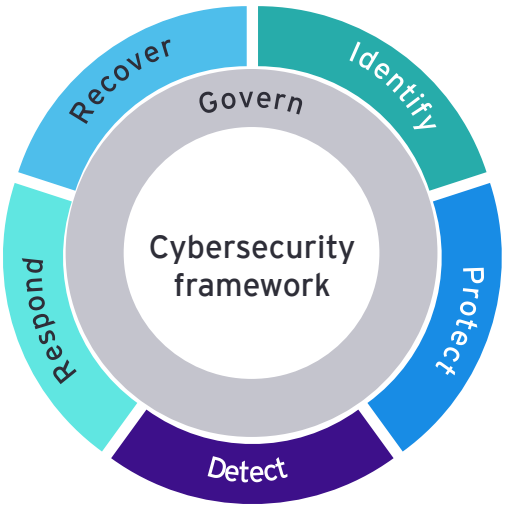
Source: *Information and Network Security Guidelines (INSG)*, MCMC, October 2024

Designing safeguards for infrastructure

To build a resilient information and network security infrastructure, companies can develop a Cyber Resilience Framework (CRF) supported by infrastructure requirements as follows:

What does the CRF do?

- Provide clear governance in managing cyber risks and resilience.
- Ensure the appropriate operational resiliency measures against extreme but plausible from internal or external.
- Provide the required capability of Identify, Protect, Detect, Response and Recover (IPDRR) Critical Systems and Data hosted on-premises or by third-party providers.



Infrastructure requirements

Network

- Establish Network Oversight Functions to review, design and deliver a resilient network infrastructure.
- Ensure that network services supporting its critical systems are designed and implemented to achieve data security, confidentiality, integrity and availability.

Data center

- Dedicate spaces to host critical systems in the production data center.
- Dedicate physical space that is secured from unauthorized access and is not located in disaster-prone area.
- No Single Point of Failure (SPOF) in the design and connectivity for critical components of the production data center.

Cloud services management

- Ensure that data management practices within cloud services adhere to data protection laws and regulations.
- Ensure that data is stored and processed in geographic locations that comply with legal and regulatory requirements.
- Implement data encryption in use, at rest, and in transit to protect sensitive and personal information.

Cryptography

- Adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random key generation.
- Adoption of secure processes in managing cryptographic key lifecycles.
- Periodic review, at least once in every two years, of existing cryptographic standards and algorithms.

Source: *Information and Network Security Guidelines (INSG)*, MCMC, October 2024

Building information and network security

INSG focuses on supporting organizations to develop robust information and network security. To protect the integrity of computer networks, organizations can develop the following components:

Components	Considerations
System development and acquisition	Ensure any changes to the source code of critical systems are subject to adequate reviews.
Security patching and end-of-life (EOL) system management	Ensure all critical vulnerabilities corrective measures and critical systems on EOL are reported to the board and management periodically for immediate rectification.
Identity management and access control	Implement an appropriate access controls policy for the identification, authentication and authorization of users and address both logical and physical technology access controls equal with the level of risk exposure of unauthorized access to systems.
Credential monitoring and protection	Establish monitoring processes to detect the exposure or theft of credentials on the dark web or other sources.
Data security and protection	Ensure data is protected and implement technical means to protect data.
Data storage	Ensure data stored is encrypted and protected by an adequate backup schedule, perform periodic testing and ensure data can be restored from backups.
Data disposal	Implement a clear data sanitization procedure to ensure the data is irretrievably destroyed from systems and devices.
Cybersecurity operations	Establish clear responsibilities for cybersecurity operations and implement appropriate mitigating measures that correspond to the cyber kill chain or threat actor management equivalent.
Security operations center	Establish clear responsibilities for cybersecurity operations and implement appropriate mitigating measures that correspond to the phases of cyber kill chain or threat actor management equivalent.
Incident response and recovery	Implement proactive measures to mitigate the impact of incidents on network and information system security, ensuring service continuity.

Source: *Information and Network Security Guidelines (INSG)*, MCMC, October 2024

Compliance and reporting requirements

To mitigate the prevalence of cybersecurity incidents in Malaysia, the INSG provides for the following compliance and reporting requirements:

Reporting and notification to the Commission

Reporting obligations

- Immediately notify the Commission in writing, within 90 minutes upon the occurrence of any cybersecurity incident in respect of the service provider network, facilities, services, application, data, computer or computer system and provide a full report of the incident within seven business days.
- Report external audits outcomes within five business days. This includes periodic and on-demand reports generated by external auditors, ensuring that the Commission is continually informed of the service provider's compliance status and updated on any critical cybersecurity issues.

Periodic and on-demand reporting submission

- A service provider shall submit reports to the Commission on matters specified under INSG as required by the Commission.
- The Commission may conduct audit on service provider and/or request reports from service provider on compliance to INSG implementation.

Prevention of commission of offenses and investigation assistance

Retention and preservation of logs, information and data for investigation purpose

- Retain sufficient and relevant logs, information and data for investigations and forensic purposes, for at least one year, with an emphasis on capturing interactions involving servers or network equipment that relates to confidential repositories.
- Preserve the data specified in the notice for the period and in the manner outlined in the notice, ensuring that data integrity and availability are maintained for forensic analysis.

Prevention of commission of offenses

- Take measures to prevent network or application from being used or exploited for any offense under Malaysian laws.
- Ensure that the technology deployed in their network facilities is up-to-date and capable of preventing the commission or attempted commission of an offense under any Malaysian law.
- Block access to any harmful and illegal content upon receiving a notice from the Commission within the prescribed timeframe.
- Immediately preserve subscriber information and transaction records and terminate the telephone numbers used to commit an offense under Malaysian laws upon receiving notice from the Commission.

Source: *Information and Network Security Guidelines (INSG)*, MCMC, October 2024

Next steps

New technologies and innovations in various industries and sectors require businesses, regardless of their size, to step up their cybersecurity actions.

Key actions to consider:

1. Review the INSG requirements and develop a strategy and action plan to address gaps and areas of concern.
2. Assess current governance within your organization, including requirements at the board, senior management and operational levels.
3. Identify improvements in technology infrastructure and controls.
4. Determine the sufficiency of skills and resources for implementation and operationalization.
5. Consider the need for independent review and assurance.

Source: EY analysis

Contacts

Dato' Abdul Rauf Rashid
Malaysia Managing Partner,
Ernst & Young PLT

abdul-rauf.rashid@my.ey.com

Jason Yuen
Malaysia Cybersecurity Leader; and
Partner,
Ernst & Young Consulting Sdn. Bhd.

jason.yuen@my.ey.com

Shankar Kanabiran
Malaysia Deputy Consulting Leader; and
Partner,
Ernst & Young Consulting Sdn. Bhd.

shankar.kanabiran@my.ey.com

Jaco Benadie
EY ASEAN Cybersecurity Energy Leader
and OT Cybersecurity Competency Lead
Ernst & Young Consulting Sdn. Bhd.

jaco.benadie@my.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

APAC no. 07010935

ED None

ey.com