Cyber Assurance Advisory

Securing Your Future in the Digital World

Malaysia is accelerating its digital transformation, with Artificial Intelligence, automation, and data security at the forefront. The Digital Trust & Data Security Strategy 2026–2030, together with the Cyber Security Act (CSA) 2024 under the National Cyber Security Agency (NACSA), sets the stage for stronger protection, governance, and compliance across key sectors.

Requirements under CSA

Entities that fall under the National Critical Information Infrastructure (NCII) will be required to:

- Conduct a cyber security risk assessment at least once a year.
- Carry out an audit at least once in every two years, or at such higher frequency as may be directed by the Chief Executive of NACSA in any particular case.

Penalties for Non-Compliance:

Fine: Up to **RM500,000**
Imprisonment: Up to **10 years** Or both

National Cyber Security Baseline

6 core domains

- Governance
- Recover
- Identify
- Protect
- Detect
- Respond

Who the regulations apply to

The NCII sectors are as follows:

- Government
- Banking and Finance
- Transportation
- Defense and National Security
- Agriculture and Plantation
- Trade, Industry and Economy
- Science Technology and Innovation
- Information, Communication and Digital
- Healthcare Services
- Water, Sewerage and Waste Management
- Energy

We help

NCII Entities

Develop and implement a robust compliance plan

Design and implement practical frameworks for your organisation to meet regulatory obligations and strengthen cyber resilience

Leverage cyber security expertise

Deliver effective, scalable protection and expert-led advisory services to safeguard critical assets

Build tailored cyber risk controls

Incorporate cyber security risk management processes and controls tailored to your operations

Other Entities

Establish a strong cyber security foundation

Adopt baseline cyber security processes and benchmark against recognised standards to ensure consistent protection and compliance

Build cyber-ready capabilities

Enhance your organisation's competency and resilience, empowering teams to anticipate, respond to, and recover from cyber threats

Stay ahead with proactive governance

Integrate governance, risk management, and data protection into your business strategy, helping you move from reactive defence to proactive resilience

15 essential cyber security categories

- Cyber Security Policy & Objectives
- Organisational Development
- Cyber Security Assurance
- Resource Allocation and Optimisation
- Risk Management
- Operational Efficiency
- Data Security
- Contractual Management
- Physical Security
- System and Network Security
- Access Control
- Technical Vulnerability
- Cyber Security Event Management
- Cyber Security Incident Management
- Business Continuity Management

BDO Can Help You Stay Secure, Confident and Ready.

Navigating the CSA 2024 framework can be challenging. We help organisations strengthen their IT infrastructure in line with the National Cyber Security Baseline requirements.

We are here to guide you every step of the way, ensuring your organisation is well-prepared and compliant with the latest cyber security standards.

Get in touch with us to learn more about BDO's cyber assurance advisory practice:

Raymond Lim Khoon Seng
Executive Director, Technology Advisory
T: +603-2616 2805 | **E:** raymondlim@bdo.my

Mohamed Mansor Adhar bin Sabaruddin
Associate Director, Technology Advisory
T: +603-2616 7036 | **E:** mansoradhar@bdo.my