KPMG

Guidance on the new NIST Cybersecurity Framework (CSF) 2.0

NIST Cybersecurity Framework

The National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF") provides international guidance to organisations, including but not limited to industry sectors and government agencies. Following the previous release of NIST CSF 1.1 in 2018, NIST unveiled the revamped version 2.0 in February 2024.

NIST CSF 2.0 is a useful tool that helps organisations evaluate their current cybersecurity maturity status (ranging from Tier 1 Partial, Tier 2 Risk-informed, Tier 3 Repeatable, and Tier 4 Adaptive). It also provides guidance on the implementation of advanced processes and controls to achieve the target maturity level.

Source: NIST CSF 2.0

What are the major updates?

Addition of Cybersecurity Governance

NIST CSF 2.0 includes the new **Govern (GV)** function, which emphasises the organisation's cybersecurity risk management strategy, setting clear expectations and policy guidance. GV puts weight on embedding cybersecurity within the organisational context, delineating risk management strategy, roles, responsibilities, authorities, and management oversight. The updated CSF implementation also advocates integration of the NIST Privacy Framework within the broader practice of Enterprise Risk Management.

Supply Chain Risk Management

As part of the new GV function, emphasis is placed on **Cybersecurity Supply Chain Risk Management**. This aims to ensure the implementation of proper controls across suppliers, customers and other business partners.

The scope includes but is not limited to the establishment of a management programme, clarity on roles and responsibilities among each stakeholder, prioritisation of suppliers based on criticality, execution of due diligence before contracting, and the preparation of a supply chain incident response plan.

Guidance on CSF implementation

To help organisations implement the controls set out in NIST CSF 2.0, implementation guidance is provided with action-oriented examples.

NIST CSF 2.0 also introduces the **CSF Organisational Profile** as a tool for organisations to appraise their present cybersecurity maturity and chart a course towards the target maturity level.

Source: NIST CSF 2.0

Advantages of adopting NIST CSF 2.0

Adopting NIST CSF 2.0 can bring numerous benefits to your organisation, including aiding in the prioritisation of cybersecurity investment and strategic decisions, improving cyber resilience in response to potential incidents, and simplifying the translation of complex cybersecurity risks into an accessible management dashboard.

Prioritise cybersecurity investment:

NIST CSF 2.0 can help your organisation in identifying high-risk areas in the IT environment and guide the adoption of purposeful security measures.

Enhance cybersecurity resilience:

A systematic and comprehensive cybersecurity risk framework can enhance the robustness of cybersecurity controls, thereby improving its ability to withstand and respond to cyber events.

Translate complex cybersecurity risks:

NIST CSF 2.0 can serve as an instrument for your organisation to evaluate its cybersecurity maturity status, making it easier to benchmark against peers.

How KPMG can help

KPMG provides a range of services to help organisations evaluate their cybersecurity maturity status with reference to NIST CSF 2.0, and in advising on control implementations to enhance maturity levels, including:

01 **Cybersecurity maturity assessment:** A review of your organisation's current cybersecurity processes and controls within the **Govern, Identify, Protect, Detect, Respond and Recover** functions, and identification of any improvement opportunities.

Enhancement design recommendations: Advice on the design of enhancement processes and control mechanisms, based on the identified opportunities for improvement. 02

03 **Technology implementation assistance:** Collaborate with security solution vendors to help your organisation implement solutions that protect assets and advance overall cyber security maturity.

Cyber incident management services: Assist your organisation in (i) establishing, strengthening, and testing cyber incident management controls (such as cyber drill tests and developing incident response playbooks), (ii) performing on-demand incident management and cyber investigations, and (iii) providing post incident services (such as remediation support). 04

KPMG's experience in NIST CSF assessment

KPMG boasts a wealth of expertise in performing cybersecurity maturity assessments that adhere to the NIST CSF. The firm's experience spans across multiple industry sectors including aviation, education, insurance, consumer retail, hospitality, entertainment, internet infrastructure, securities, private equity and financial technology.

Contact us

Henry Shek
Partner, Cybersecurity
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Danny Hao
Partner, Cybersecurity
KPMG China
T: +8610 8508 5000
E: danny.hao@kpmg.com

Mohit Kumar
Director, Cybersecurity
KPMG China
T: +852 2685 7428
E: mohit.kumar@kpmg.com

kpmg.com/cn/socialmedia