Assessment Frameworks

SecurityGate.io
INFO@SECURITYGATE.IO

22+
Industry frameworks available

3,000+
Cyber security control questions

+Module Builder
Bring, Create & Customize standard frameworks

Australian Energy Sector Cyber Security Framework (AESCSF)

The AESCSF module is derived directly from the May 2021 Framework Core. The framework has been developed and tailored to the Australian energy sector to enable Participants to assess, evaluate, prioritize, and improve their cyber security capability and maturity.

REVISION DATE July 2022
ASSESSMENT TYPE Maturity
QUESTIONS 282
COMPLEXITY LEVEL
INDUSTRIES Energy

Cybersecurity Capability Maturity Model (C2M2)

C2M2 focuses on the implementation and management of cybersecurity practices associated with information, information technology (IT), and operations technology (OT) assets and the environments in which the organizations operate. ISO 27001/2.

REVISION DATE June 2022
ASSESSMENT TYPE Maturity
QUESTIONS 356
COMPLEXITY LEVEL
INDUSTRIES Energy

Critical Infrastructure Maturity Model (CIMM)

REVISION DATE February 2020
ASSESSMENT TYPE Maturity
QUESTIONS 17
COMPLEXITY LEVEL
INDUSTRIES All critical infrastructures

Cybersecurity Maturity Model Certification (CMMC)

The CMMC assessment is derived directly from CMMC documentation to evaluate handling of CUI for a Defense Industrial Base contractor. It consists of 171 practices that are mapped across five levels.

REVISION DATE June 2023
ASSESSMENT TYPE Maturity
QUESTIONS 110
COMPLEXITY LEVEL
INDUSTRIES All sectors supporting the DoD

NIST SP 800-171 (DFARS NIST SP 800-171)

DFARS assesses data safeguarding standards required for all Department of Defense (DOD) contractors.

REVISION DATE April 2018
ASSESSMENT TYPE Compliance
QUESTIONS 110
COMPLEXITY LEVEL
INDUSTRIES All sectors supporting the DoD

General Data Protection Regulation (GDPR)

The GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

REVISION DATE August 2021
ASSESSMENT TYPE Compliance
QUESTIONS 365
COMPLEXITY LEVEL
INDUSTRIES Organizations anywhere, so long as they target or collect data related to people in the European Union (EU).

Maritime Cyber Assessment

Maritime cyber compliance assessment for selected vessel/entity.

REVISION DATE 2020
ASSESSMENT TYPE Compliance
QUESTIONS 354
COMPLEXITY LEVEL
INDUSTRIES Energy, Transportation

Cyber Assessment Framework (NCSC CAF)

The CAF (v3.1) is aimed at helping an organization achieve and demonstrate an appropriate level of cyber resilience to certain specified essential functions performed by that organization.

REVISION DATE April 2022
ASSESSMENT TYPE N/A
QUESTIONS 39
COMPLEXITY LEVEL
INDUSTRIES Organizations within the UK Critical National Infrastructure (CNI) » Organizations subject to Network and Information Systems (NIS) Regulations » Organizations managing cyber-related risks to public safety

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

The NERC CIP Module is derived directly from the NERC CIP standards and concerns the reliability and security of the Bulk Electric System of North America.

REVISION DATE February 2023
ASSESSMENT TYPE N/A
QUESTIONS 135
COMPLEXITY LEVEL
INDUSTRIES Electricity Subsector

Cybersecurity Framework (NIST CSF) - Compliance

The NIST CSF consists of three main components: the framework core, implementation tiers, and profiles for reducing cyber risks to critical infrastructure.

REVISION DATE April 2022
ASSESSMENT TYPE Compliance
QUESTIONS 108
COMPLEXITY LEVEL
INDUSTRIES All critical infrastructure sectors

Cybersecurity Framework (NIST CSF) - CMMI Maturity

The NIST CSF - CMMI maturity module implemented the ISACA's CMMI approach to provide organizations with a staged path for cybersecurity improvement.

REVISION DATE April 2022
ASSESSMENT TYPE Maturity
QUESTIONS 108
COMPLEXITY LEVEL
INDUSTRIES All critical infrastructure sectors

NIST SP 800-53 Rev.5

The NIST SP 800-53 Rev.5 provides a catalog of security and privacy controls for information systems and organizations to protect organizations from a diverse set of threats and risks.

REVISION DATE December 2022
ASSESSMENT TYPE Compliance
QUESTIONS 298
COMPLEXITY LEVEL
INDUSTRIES All critical infrastructure sectors

Assessment Frameworks CONT.

NIST SP 800-82 Section 6.2

This module evaluates performance against the SP 800-53 control families and implementation considerations for ICS owners.

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
November 2018	Compliance	85

COMPLEXITY LEVEL	INDUSTRIES
	All critical infrastructure sectors

SG IT Cyber Maturity

(Based on NIST 800-53 r4 & ISO 27001/2)

Cyber maturity: it evaluates an entity's IT environment, based on NIST 800-53 and ISO 27001/2.

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
November 2018	Maturity	122

COMPLEXITY LEVEL	INDUSTRIES
	All critical infrastructure sectors

SG OT Cyber Maturity

(Based on NIST 800-53 r4 & IEC 62443)

Cyber maturity: it evaluates an entity's IT environment, based on NIST 800-53 and IEC 62443.

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
November 2018	Compliance	151

COMPLEXITY LEVEL	INDUSTRIES
	All critical infrastructure sectors

SOC 2: TSP (Trust Services Criteria) - 2017

SOC 2: TSP evaluates security, availability, processing integrity, confidentiality, and privacy compliance controls for service organizations with its unique framework.

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
July 2021	Compliance	61

COMPLEXITY LEVEL	INDUSTRIES
	All critical infrastructure sectors

TSA- Aviation Joint EA 23-01

The Transportation Security Administration (TSA) issued this Emergency Amendment (EA) to address the ongoing cybersecurity threat to airlines and unmanned aircraft systems (UAS), Zero-trust Architecture and cybersecurity framework.

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
May 2023	Compliance	61

COMPLEXITY LEVEL	INDUSTRIES
	Aviation

TSA Pipeline Cybersecurity Measures - Baseline

Based on TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)), 6.3 Site-Specific Security Measures. Requirements are centered around physical protection of facilities (Baseline).

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
June 2021	Compliance	47

COMPLEXITY LEVEL	INDUSTRIES
	Oil & Gas

TSA Pipeline Cybersecurity Measures - Baseline + Enhanced

Based on TSA's 2018 Pipeline Security Guidelines, 7.3 Security Measures for Pipeline Cyber Assets. Requirements are centered around protection of facilities against cyber threats (Baseline + Enhanced).

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
June 2021	Compliance	59

COMPLEXITY LEVEL	INDUSTRIES
	Oil & Gas

TSA Pipeline Site-Specific Measures - Baseline + Enhanced

Based on TSA's 2018 Pipeline Security Guidelines, 6.3 Site-Specific Security Measures. Requirements are centered around physical protection of facilities (Baseline + Enhanced).

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
June 2021	Compliance	62

COMPLEXITY LEVEL	INDUSTRIES
	Oil & Gas

IEC 62443 3-2

ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS).

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
April 2023	Compliance	User-defined

COMPLEXITY LEVEL	INDUSTRIES
	All critical infrastructure sectors

TSA Pipeline Site-Specific Measures - Baseline

Based on TSA's 2018 Pipeline Security Guidelines, 6.3 Site-Specific Security Measures. Requirements are centered around physical protection of facilities (Baseline + Enhanced).

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
June 2021	Compliance	31

COMPLEXITY LEVEL	INDUSTRIES
	Oil & Gas

TSA Pipeline Security Directive Pipeline 2021-02C

The Transportation Security Administration (TSA) issued this Security Directive to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure, under the authority of 49 U.S.C.114(l)(2)(A).

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
May 2023	Compliance	56

COMPLEXITY LEVEL	INDUSTRIES
	Oil & Gas

TSA Pipeline Security Directive Pipeline 2021-01B

The Transportation Security Administration (TSA) issued this Security Directive to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure.

REVISION DATE	ASSESSMENT TYPE	QUESTIONS
June 2023	Compliance	30

COMPLEXITY LEVEL	INDUSTRIES
	Oil & Gas