Assessment Frameworks

SecurityGate.io

INFO@SECURITYGATE.IO • SECURITYGATE.IO

TSA Pipeline Cyber Security 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.

Revision Date 21 Jun
Assessment Type Compliance
 # Questions 47
Complexity/Level of Low
Industries Used By Energy, Oil & Gas

DFARS 800-171 Assessment

Defense Federal Acquisition Regulation Supplement. Assesses data safeguarding standards required for all Department of Defense (DOD) contractors. Based on DoD requirements from NIST 800-171.

Revision Date 18 Dec
Assessment Type Compliance
 # Questions 110
Complexity/Level of Low
Industries Used By All sectors supporting the DOD

Australian Energy Sector Cyber Security Framework (AESCSF)

For Australian energy companies. Derived from the May 2021 Framework Core. Contains Australian-specific controls, along with questions from existing frameworks, such as the United States' ES-C2M2 and NIST-CSF.

Revision Date 21 May
Assessment Type Compliance
 # Questions 282
Complexity/Level of Medium
Industries Used By Energy, Power Utility

20
Industry Frameworks Available

16
Critical Infrastructure Sectors Covered

3,089
Cybersecurity Control Questions

+Module Builder
Bring your framework, Create a framework, Customize a standard framework

C2M2-Electric

Electricity Subsector Cybersecurity Capability Maturity Model. Evaluates cybersecurity posture of organizations within the energy sector.

Revision Date 19 Oct
Assessment Type Compliance
 # Questions 315
Complexity/Level of Medium
Industries Used By Energy, Power Utility

C2M2-Oil & Gas

Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model. Evaluates cybersecurity posture; specific to oil & gas organizations, based on ES-C2M2

Revision Date 19 Oct
Assessment Type Compliance
 # Questions 315
Complexity/Level of Medium
Industries Used By Energy, Oil & Gas

SOC 2: TSP - 2017

SOC2: Trust Services Criteria evaluates security, availability, processing integiry, confidentiality, and privacy compliance controls for service organizations.

Revision Date 18 Dec
Assessment Type Compliance
 # Questions 61
Complexity/Level of Low
Industries Used By All critical infrastructure sectors

Critical Infrastructure Maturity Model (CIMM)

Guides organizations in understanding the maturity of their cyber risk program.

Revision Date 20 Jul
Assessment Type Maturity
 # Questions 17
Complexity/Level of Low
Industries Used By All critical infrastructure sectors

NIST 800-53 Rev. 5

This NIST special publication provides a catalog of security and privacy controls for information systems and organizations from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

Revision Date 21 Jun
Assessment Type Compliance
 # Questions 298
Complexity/Level of Medium
Industries Used By All critical infrastructure sectors

TSA Pipeline Site-Specific 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. These measures should be tailored explicitly for each facility and address specific actions to be taken in response to pertinent NTAS Bulletins or Alerts.

Revision Date 21 Jun
Assessment Type Compliance
 # Questions 31
Complexity/Level of Low
Industries Used By Energy, Oil & Gas

TSA Pipeline Site-Specific Measures - Baseline + Enhanced

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. These measures should be tailored explicitly for each facility and address specific actions to be taken in response to pertinent NTAS Bulletins or Alerts.

Revision Date 21 Jun
Assessment Type Compliance
 # Questions 62
Complexity/Level of Low
Industries Used By Energy, Oil & Gas

TSA Pipeline Cyber Security Measures - Baseline + Enhanced

Based on TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)), 7.3 Security Measures for Pipeline Cyber Assets, requirements are centered around protection of facilities against cyber threats.

Revision Date 21 Jun
Assessment Type Compliance
 # Questions 59
Complexity/Level of Low
Industries Used By Energy, Oil & Gas

SG OT Cyber Maturity

Evaluates an entity's OT environment. Based on NIST 800-53 and IEC 62443.

Revision Date 18 Nov
Assessment Type Compliance
 # Questions 151
Complexity/Level of Low
Industries Used By All critical infrastructure sectors with industrial operations

SG IT Cyber Maturity

Evaluates an entity's IT environment, based on NIST 800-53 and ISO 27001/2.

Revision Date 18 Nov
Assessment Type Maturity
 # Questions 122
Complexity/Level of Low
Industries Used By All critical infrastructure sectors

NERC CIP

Compliance standard for the reliability and security of the Bulk Electric System of North America.

Revision Date 20 Dec
Assessment Type Compliance
 # Questions 135
Complexity/Level of High
Industries Used By Energy, Power Utility

NIST Cybersecurity Framework (CSF)

Evaluates adherence to NIST cybersecurity standards and best practices

Revision Date 19 Oct
Assessment Type Compliance
 # Questions 108
Complexity/Level of Low
Industries Used By All critical infrastructure sectors

General Data Protection Regulation (GDPR)

Data protection and privacy compliance to the European Union & European Economic Area General Data Protection Regulation.

Revision Date 21 Aug
Assessment Type Compliance
 # Questions 365
Complexity/Level of High
Industries Used By All critical infrastructure sectors

Cybersecurity Maturity Model Certification (CMMC)

Cybersecurity Maturity Model Certification. Evaluates handling of CUI for a Defense Industrial Base contractor. It consists of 171 practices that are mapped across five levels.

Revision Date 20 Jul
Assessment Type Maturity
 # Questions 171
Complexity/Level of Medium
Industries Used By All sectors supporting the DOD

NIST 800-82 Section 6.2

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

Revision Date 18 Nov
Assessment Type Compliance
 # Questions 86
Complexity/Level of Low
Industries Used By All critical infrastructure sectors with industrial operations

Maritime

Vessel/entity compliance based on both BIMCO and IMO guidelines.

Revision Date 19 Jun
Assessment Type Compliance
 # Questions 354
Complexity/Level of High
Industries Used By Energy, Oil & Gas, Transportation, Defense