OTORIO

Guide to Cybersecurity Standards

REPORT

industrial cybersecurity standards **2021**

Copyright OTORIO™ © 2020 All rights reserved | December 2020

Table of Contents

Copyright OTORIO™ © 2021 All rights reserved | February 2021

Guide to Cybersecurity Standards

Cybersecurity standards have existed for decades. Some are standalone while others are a series. Many relate to OT (operational technology) without saying so directly - especially the risk management and risk assessment cybersecurity standards. Others are industry specific - healthcare, credit card. Many people have heard of the European GDPR, which is considered to be a gold privacy standard for handling personal data (PII). **This article contains many of the most prevalent IT and OT cybersecurity standards.**

CERTIFIED
ISO 27000
★★★★★★★

ISO 27000 Series

ISO 27000 is a series of standards published by ISO (International Organization for Standardization) and the IEC (International Electrotechnical Commission).

What it is and Why it is Important

The ISO 27000 series features a total of 46 standards which describe specific controls to secure information and information systems. In addition to IT security, ISO 27000 helps companies comply with laws such as the GDPR. It is a prominent cybersecurity standard and often serves as a prerequisite to do business with large corporations and governments.

Key Point

The ISO 27000 series is an essential starting point for any organization building an information security management system (ISMS).

NIST
National Institute of
Standards and Technology
SP 800-82 Rev. 2

NIST SP-800 Series

Published by the National Institute of Standards and Technology, the NIST SP-800 Series sets US government security policies, procedures and guidelines for cybersecurity.

What it is and Why it is Important

The NIST SP-800 Series covers procedures and criteria for assessing and documenting IT threats and vulnerabilities, as well as implementing security measures geared towards risk mitigation. The series helps organizations enforce security rules and serves as legal references in case of cybersecurity litigation.

Key Point

The NIST SP-800 Series was specifically written for US government agencies and has been widely adopted by non-governmental businesses around the world. Three of the most widely used from the series include:

- **NIST SP 800-53** - Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-30** - Guide for Conducting Risk Assessments
- **NIST SP 800-37** - Guide for Applying the Risk Management Framework

PCI DSS Certified

PCI DSS

PCI DSS is the Payment Card Industry Data Security Standard.

What it is and Why it is Important

PCI-DSS sets security requirements for sellers to safely and securely accept, store, process and transmit credit card holder data during credit card transactions. PCI DSS's main objective is to prevent fraud and data breaches. It comprises six requirements (called control objectives):

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Key Point

MasterCard, American Express, Visa, JCB International and Discover Financial Services formed the Payment Card Industry Security Standards Council (PCI SSC) in 2006 as a governing entity for PCI DSS. The PCI DSS standards have been adopted all over the world. widely used from the series include:

The HIPAA Privacy Rule

The HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule is a United States federal statute signed into law in 1996 by President Clinton.

What it is and Why it is Important

The HIPAA Privacy Rule regulates the flow of healthcare information, stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addresses limitations on healthcare insurance coverage.

The HIPAA Privacy Rule gives patients rights over their health information and grants them the right to examine and receive a copy of their health records as well as to request corrections.

Key Point

Patients have the rights to receive their Protected Health Information (PHI) within 30 days of request.

IMO Standards

The International Maritime Organization was established in 1969 in Geneva, Switzerland by the United Nations. The organization sets international maritime standards.

What it is and Why it is Important

IMO Standards are the global "gold standard" for safety, security and environmental performance of international shipping. They create a regulatory framework for the shipping industry that has been universally adopted and implemented.

Key Point

More than 80% of global trade takes place via international shipping and IMO standards regulate these activities. The IMO has no enforcement mechanism. Nations that adopt IMO standards do so by passing and enforcing laws.

NERC CIP

NERC (North American Electric Reliability Corporation) operates and manages the United States electric grid, officially known as the Bulk Power System. The CIP (Critical Infrastructure Protection) was developed to mitigate cybersecurity attacks on the grid.

What it is and Why it is Important

The NERC Critical Infrastructure Protection standards are a set of requirements designed to secure the US electrical grid. The CIP consists of both standards and requirements.

Key Point

Every US and Canadian utility company adheres to CIP standards. CIP standards are continually updated. In October 2020, a new standard, CIP-013-1, came into effect; it regulates supply chain risk management.

IEC 62443

Published by IEC, the International Electrotechnical Commission, IEC 62443 governs Industrial Automation and Control Systems (IACS).

What it is and Why it is Important

IEC 62443 covers every stage of industrial cybersecurity - from risk assessment to operations. It defines four security levels - from very basic security to resistant against nation-state attacks.

Key Point

The key standards in the IEC 62443 series are the following:

- **IEC 62443-2-4** - Requirements for IACS service providers
- **IEC 62443-3-3** - System security requirements and the security levels
- **IEC 62443-4-1** - Secure development lifecycle requirements
- **IEC 62443-4-2** - Technical security requirements for IACS components

GDPR

GDPR is the General Data Protection Regulation, passed by the European Union in 2016 and enforced in 2018.

What it is and Why it is Important

GDPR is a data privacy standard that governs the transfer, storing and processing of data within and outside the EU and EEA (European Economic Area). The goal of GDPR is to give people control over the personal data and to unify regulation.

Key Point

GDPR's greatest impact is making it mandatory for every organization to clarify data privacy and fining organizations that fail to protect their users' PII on the internet.

Copyright OTORIO™ © 2021 All rights reserved | February 2021

The Most Prominent Cybersecurity Standards

Standard Name	Published By	Focus Area	Obtained	Year Established
ISO 27000 Series	ISO and IEC	Information Security	Purchased	1995
NIST SP-800 Series	NIST	Information Security	Free	1990
PCI DSS	Payment Card Industry Security Standards Council	Credit Card Fraud Prevention	Free	2004
HIPAA	U.S. Department of Health & Human Services	Health Care	Free	1996
IMO Standards	International Maritime Organization	Maritime	Purchased	1959
NERC CIP	NERC	Electricity	Free	2008
IEC 62443	IEC	Industrial Automation Control Networks	Purchased	2009
GDPR	EU	Data Protection & Privacy	Free	2016

About OTORIO

OTORIO designs and markets the next generation of OT security and digital risk management solutions. The company combines the experience of top nation-state cybersecurity experts with cutting edge digital risk management technologies to provide the highest level of protection for the manufacturing industry. Visit our website: www.otorio.com

Copyright OTORIO™ © 2021 All rights reserved | February 2021