20 CYBER SECURITY FRAMEWORKS ACROSS THE GLOBE

DATA TRUST

#1

ISO 27001

It is considered the internationally recognized cyber security validation standard for both internal situations and across third parties. ISO 27001 requires management to exhaustively manage their organization's information security risks, focusing on threats and vulnerabilities.

ISO **27001** sets the foundation for establishing an information security management system (ISMS). **ISO 27001** includes requirements for establishing, implementing, maintaining, and continually improving an ISMS influenced by the organization's needs, objectives, security requirements, processes, size, and structure.

#2
NIST CSF

NIST is a US non-regulatory government agency that sets standards across the physical sciences. Originally intended for critical infrastructure owners and operators, NIST CyberSecurityFrameworks can be used by any organization.

Many companies outside of the critical infrastructure industry also use the CSF, especially if they need to meet other US federal data protection requirements.

#3
COBIT 5

Control Objectives for Information Technology **(COBIT)** focus on governance creates a security framework that streamlines audits and incorporates continuous improvement to enhance those outcomes.

COBIT's goal is to ensure appropriate oversight of the organization's security posture.

#4

PCI DSS

PCI DSS is a Payment Card Industry Data Security Standard, a cybersecurity framework developed for companies that accept, process, and offer saving credit or debit card information.

This framework aims to improve security of the payment account throughout the transaction process regardless of the channel (online or POS) and works with any organization regardless of its size and transaction volume

#5

NCSC - CEF

National Cyber Security Centre **(NCSC) Cyber Essentials Framework (CEF):** The United Kingdom's NCSC launched the CEF Assessmenet and brings together SMEs, enterprise organizations, government agencies, the general public, and departments to address cybersecurity concerns.

Cyber Essentials is an effective, Government backed scheme that will help organisations, whatever its size, against a whole range of the most common cyber attacks. Cyber Essentials helps organisations to guard against the most common cyber threats and demonstrate your commitment to cyber security.

#2

BIO

(dutch: Baseline Informatiebeveiliging Overheid)

The **BIO** is is a mandatory national (i.e. Dutch) standard. The BIO replaces the **BIG, BIWA, BIR** and **IBI** for municipalities, water authorities, provinces and central government. The BIO is:

- a common standards framework based on the international standard **ISO 27001/2** for the security of government information (systems);
- a derivative of the BIR (Baseline Information Security Government Service) 2017;
- a concretisation of a number of standards into mandatory government measures

#3

NEN7510

The **NEN 7510** is a national (i.e. Dutch) standard, specifically focused on organisations dealing with personal health information (i.e. healthcare institutions and their service providers).

The control measures described (and in some cases mandatory) by the **NEN 7510** are written to complement **ISO 27001**

#6

CIS CONTROLS

CIS framework was developed in the late 2000s to protect companies from cyber threats. It's made up of 20 controls regularly updated by security professionals from many fields (academia, government, industrial).

The framework begins with basics, moves on to foundational, then finishes with organizational.

DATA 2 TRUST

#7
CMMC

The **CMMC** (Cybersecurity Maturity Model Certification) is a framework designed by the US DoD (Department of Defense) to assess its contractor's and subcontractor's security, capacity, and strength.

The cybersecurity maturity model framework helps eliminate the risks and vulnerabilities in the supply chain and enhance the system's online security. Additionally, the framework is developed to ease the US Defense Department from the breaches that could compromise their missions

DATA TRUST

#8

GDPR

General Data Protection Regulation (GDPR) is considered one of the most strict security and privacy programs globally designed to strengthen the EU (European Union) and EEA (European Economic Area includes Norway, Iceland, and Liechtenstein) citizen data security.

#10
ENISA

European Union Agency for Cybersecurity **(ENISA)** National Capabilities Assessment Framework provides the Member States a way to engage in self-assessments so that they can identify their maturity level.

The framework offers a way for countries to assess their cybersecurity capabilities, ultimately giving them guidelines for setting national strategies.

#11

ISA/IEC 62443

International Society of Automation **(ISA/IEC 62443).** ISA is a non-profit professional association that established a Global Security Alliance (GSA) to work with manufacturers and critical infrastructure providers. GSA incorporates various stakeholders, including end-user companies, automation and control systems providers, IT infrastructure providers, services providers, and system integrators.

ISA/IEC 62443 is an industrial security framework focused on both traditional IT environments and SCADA or plant floor environments.

DATA TRUST

#12

NIST SP 800-82

NIST Special Publication (SP) 800-82 Guide to Industrial Control Systems (ICS) Security.

In order to address the unique cybersecurity concerns facing ICS, NIST SP 800-82 provides guidance for Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems (IDS), and other control system configurations found in the industrial control sectors, like Programmable Logic Controls (PLC).

DATA TRUST

#14

IASME Governance

IASME Governance is an Information Assurance standard that is designed to be simple and affordable to help improve the cyber security of Small and medium-sized enterprises (SMEs).

#15
FISMA

FISMA (Federal Information Security Management Act) is a framework developed to safeguard the Federal Government network against cyber threats. FISMA also offers services to the sites and agencies that work on behalf of the U.S Government. The FISMA cybersecurity framework works similarly to NIST standards.

The framework is used to categorize the risk at a high level, establish the minimum baseline controls, document the controls, refine the controls, conduct annual securityreviews, and monitor the security controls. In addition, FISMA automatically encrypts sensitive data.

#16

FAIR Cyber Risk Framework

Factor Analysis of Information Risk (FAIR) CRF: The FAIR Institute is a nonprofit organization whose mission is to establish and promote risk management best practices so that risk professionals can collaborate better with their business partners.

The FAIR cyber risk framework takes an explicit approach to cyber risk management so that organizations can quantify risk regardless of the cybersecurity framework they use. According to FAIR, an implicit risk management approach starts with a compliance requirement and aligns controls to it, creating a reactive risk posture. Meanwhile, FAIR's explicit approach creates a cycle of continuous improvement integrating risk targets, controls, and a proactive risk posture.

DATA TRUST

#17

IoTSF

The Internet of Things (IoT) Security Foundation **(IoTSF)** Security Compliance Framework is a non-profit international organization that brings together IoT security professionals, IoT hardware and software product vendors, network providers, system specifiers, integrators, distributors, retailers, insurers, local authorities, and government agencies

#18
ETSI

European Telecommunications Standards Institute **(ETSI)** is a non-profit standards organization with more than 900 members from across 65 countries and five continents. A European Standards Organization (ESO), ETSI supports European regulations and legislation by creating standards used throughout the EU.

ETSI based the top twenty Enterprise industry level cybersecurity best practices on the **CIS CONTROLS.**

#19

HITRUST CSF

Privacy, information security, and risk management leaders across the public and private sectors worked together to establish a set of safeguards for protecting the security and privacy of protected health information (PHI) and electronic PHI (ePHI).

The **HITRUST Cyber Security Framework** consists of 49 control objectives across 156 control specifications, all of which fall into 14 control categories.

#20
HIPAA

Health Insurance Portability and Accountability Act (HIPAA): It provides a framework for managing confidential patient and consumer data, particularly privacy issues.

This legislation protects electronic healthcare information and is essential for healthcare providers, insurers, and clearinghouses.

Lets talk

info@d2trust.nl