Texas Cyber Security
Your Digital Security Guard

What is **ISO 27002**?

ISO 27002 is an international standard that specifies the requirements for establishing, implementing, and continually improving an Information Security Management System (ISMS). ISO 27002 offers detailed guidance on the implementation of information security controls listed in ISO 27001's Annex A. It provides best practices for managing these cybersecurity controls effectively.

Published by the International Organization for Standardization (ISO), the ISO 27002 framework includes contributions from a diverse group of experts in information security, including representatives from national standards bodies, industry experts, academics, and other stakeholders.

The most recent revision, ISO/IEC 27002:2022, introduces updates and restructuring to address the evolving landscape of information security threats and best practices.

CMGRC_DATASHEET_ISO-27002-1.jpg

What organizations use **ISO 27002**?

ISO 27002 is a versatile standard that can be applied to any organization aiming to improve its information security management practices, regardless of the industry. Many organizations across various industries comply with ISO 27002 to enhance their information security management practices.

Some notable users of ISO 27002 include:

1. **Microsoft:** Microsoft's Azure platform and other cloud services comply with ISO 27001, incorporating ISO 27002 guidelines to ensure robust information security controls.

2. **CitiBank**: As a major financial institution, CitiBank implements ISO 27002 standards to enhance the security of its financial services and protect customer information.

3. **Siemens:** Siemens, a global industrial and manufacturing leader, complies with ISO 27002 to protect its intellectual property and secure its operational technology systems.

4. **World Wildlife Fund (WWF):** The WWF employs ISO 27002 standards to secure sensitive environmental research data and donor information.

5. **Cleveland Clinic:** This academic medical center implements ISO 27002 to protect patient information and comply with healthcare regulations.

Likewise, Small and medium-sized businesses may wish to adopt ISO 27002 to enhance their cybersecurity posture, protect sensitive data, and demonstrate their commitment to security to clients and partners.

STREAMLINE YOUR ISO 27002 COMPLIANCE WITH EASE – NO EXPERTISE REQUIRED!

Compliance Manager GRC is simple to use, and you don't have to be a compliance expert to perform a robust ISO 27002 assessment. Compliance Manager GRC guides you through each requirement using an intuitive, interactive assessment dashboard. In less than 30 minutes, you can perform a Rapid Baseline Assessment to gain a high-level overview of your ISO 27002 compliance posture.

As you dive deeper into your assessment, you can leverage an array of automated IT scanning tools to collect technical data as evidence of compliance. Likewise, you can import data from other Kaseya 365 solutions to determine instantly whether you comply with a technical control.

Best of all, you can track all compliance standards in scope for your IT operations simultaneously and on the same dashboard, regardless of the source.

CMGRC_DATASHEET_ISO-27002-2.jpg

The Four Areas of **ISO 27002** Compliance

ISO 27002 details four major areas for information security management, each defined by a series of relevant controls. These areas are summarized as follows:

Organizational Controls

Organizational Controls provide a comprehensive approach to data protection across the operations and management of a company. These controls include policies, rules, processes, procedures, and organizational structures. (37 controls)

People Controls

People Controls allow organizations to regulate the people component of their information security program by defining how employees and other workforce members interact with data and with each other. These controls include secure HR onboarding, offboarding, personnel security, remote working, and security awareness education and training. (8 controls)

Physical Controls

Physical Controls are protection measures to ensure the safety of physical assets. This may include access to facilities and systems, visitor access, equipment disposal procedures, storage media protocols and clear desk policies. These controls are critical to protecting confidential information and its integrity. (14 controls)

Technological Controls

Technological Controls specify the IT security practices that organizations should implement to establish a secure IT infrastructure, from access control to information system security, backup and data recovery strategies, audit logging, and monitoring. (34 controls)

What is **ISO 27002**?

TCS
Texas Cyber Security
Your Digital Security Guard

CMGRC_DATASHEET_ISO-27002-3.jpg

EMPOWER YOUR ENTIRE TEAM FOR ISO 27002 COMPLIANCE – COLLABORATIVE TOOLS FOR EVERY STAKEHOLDER

Compliance Manager GRC doesn't just allow a single auditor to evaluate and demonstrate compliance with ISO 27002. It provides you with tools to engage the entire team in your compliance effort, including internal stakeholders, subject matter experts, and even external auditors.

- **Track your progress in remediating technical and compliance issues from the Plan of Action & Milestones, a unified assessment dashboard. You can also export identified issues in the form tickets to Autotask, where your tech team can move into action.**
- **Instantly generate Policies and Procedures to guide ISO 27002 implementation across the organization.**
- **Make it easy for personnel to read and acknowledge policies and receive cybersecurity training with the built-in Employee Portal. Managers can quickly access a dashboard to track employee compliance.**
- **Engage third-party vendors outside of the organization in assessing their cybersecurity posture with the Vendor Portal.**

UNLOCK POWERFUL FEATURES WITH COMPLIANCE MANAGER GRC

- **Rapid Baseline Assessments – Quickly identify gaps where you are not compliant with the ISO 27002 standard before performing comprehensive Controls and Requirements assessments.**
- **Technical Risk Assessments – Leverage a comprehensive set of automated data collection tools to perform a full risk assessment and meet the ISO 27002 security requirements.**
- **Auditor's Checklist – Provide easy access for auditors to quickly verify compliance with every requirement .**
- **Plan of Action & Milestones – Track and manage the tasks needed to achieve compliance.**
- **Policies and Procedures Manuals – Access automated documentation for everything you and your team need to do.**
- **BullPhish ID Integration – Deploy your entire BullPhish library of training content to jumpstart end-user training.**
- **Kaseya 365 integration - Import data from other Kaseya products you frequently use directly into your assessment as evidence of compliance. This includes technical data such as proof of patch management, backups for endpoints, and evidence of two-factor authentication.**

What is **ISO 27002**?

TCS
Texas Cyber Security
Your Digital Security Guard

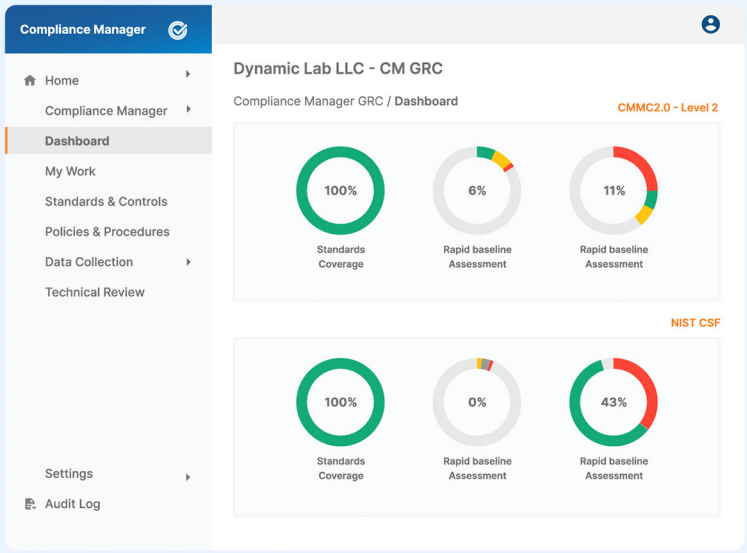
CMGRC_DATASHEET_ISO-27002-4.jpg

AUTOMATED ASSESSMENTS & REPORTS

Ensuring compliance with ISO 27002 – as well as all your other IT requirements – is easy with Compliance Manager GRC. You get more work done with less labor, thanks to automated data collection, automated management plans, and automated document generation.

AFFORDABLE FOR ALL

Compliance Manager GRC is affordable, yet boasts the power and functionality most often found in expensive, enterprise-class governance, risk, and compliance platforms. Whether you manage compliance for your own organization or are an MSP delivering compliance-as-a-service, there's a sensible subscription for you.



Request A Demo Today

Request a Demo Today and discover the advantages of Compliance Manager GRC — the purpose-built compliance management platform for IT professionals.

What is **ISO 27002**?

CMGRC_DATASHEET_ISO-27002-5.jpg