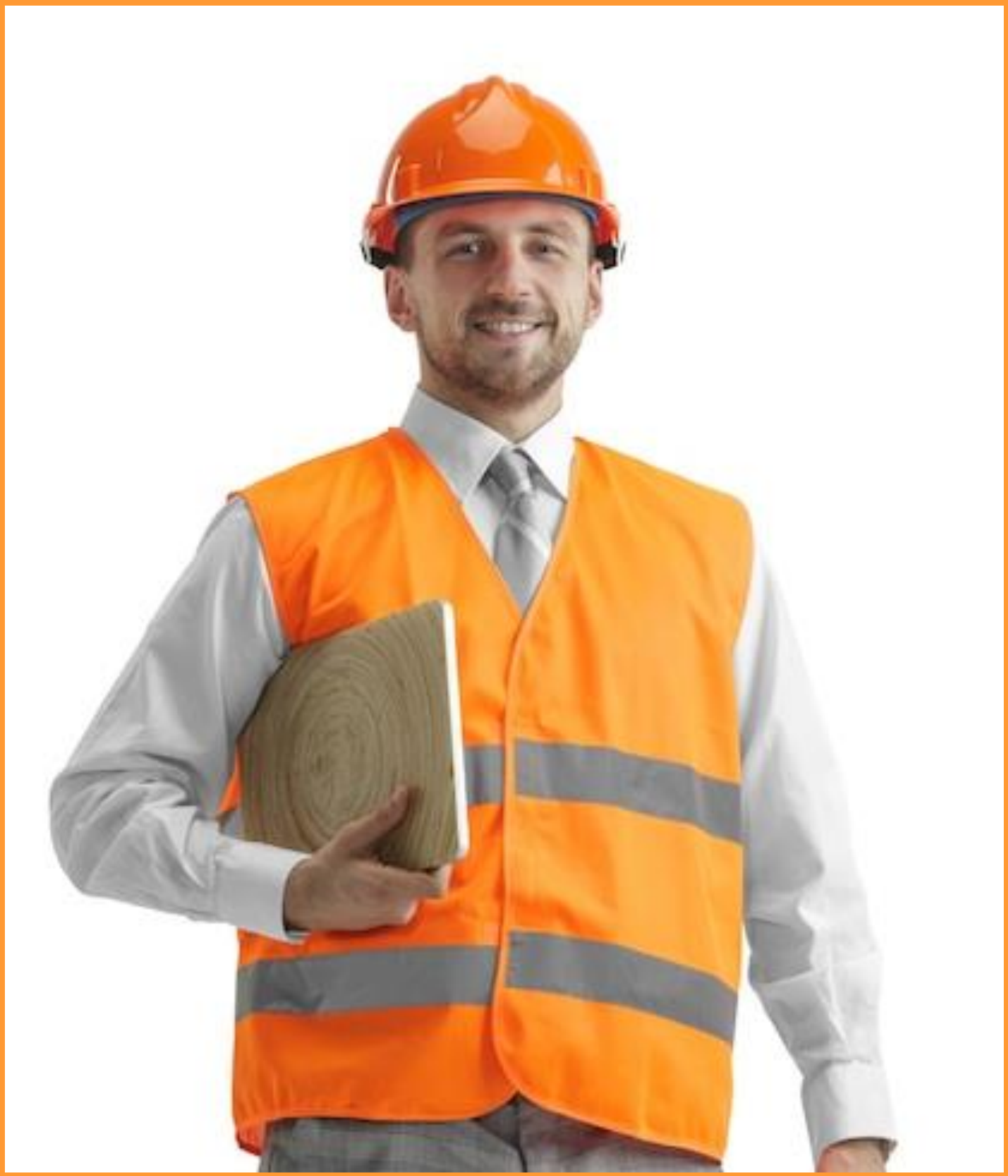
P4P Compliance Management Limited

Simplifying Compliance

# Regulatory Compliance Guide 2024



## Table of Contents

# Introduction

This Guide has been produced as an overview of Regulatory Compliance to help organisations and individuals understand and take necessary measures to comply with current and future laws, policies, regulations, and specifications applicable to their business.

The purpose is to explain in simple terminology (no complicated jargon) the fundamentals of Regulatory Compliance.

Regulatory compliance provides the guidelines and rules used to protect and benefit people, businesses, and the environment and to support economic growth.

Any business that works with digital assets, consumer data, health regulations, employee safety, and private communications is subject to regulatory compliance.

The number of laws, regulations, standards, and guidelines has increased dramatically in the past hundred years, resulting in regulatory compliance management becoming more prominent for all businesses.

Regardless of the industry, or company size, all businesses across the globe will inevitably be subject to regulatory compliance responsibilities that must be adhered to as part of daily operations.

With the regulatory environment constantly evolving, the compliance target is constantly moving. Just when you have achieved full compliance, something changes and you must amend your approach and adapt your business to stay compliant otherwise, your business is at risk.

Businesses need to be transparent about daily operations, their compliance processes, procedures, audits, and reporting activities to avoid the consequences of non-compliance.

Regulatory compliance varies not only by industry but often by location.
The financial, research, and pharmaceutical regulatory structures in one country, for example, may be similar but with particularly different distinctions to that in another country.
These similarities and differences are often reactions to the changing objectives and requirements in different countries, industries, and policies.

Organisations are legally obligated to comply with regulatory compliance laws, failing to do so, and breach regulatory compliance laws can result in damage to business reputation, corporate punishment such as removal of accreditations, hefty fines bankruptcy, business closure. or even imprisonment.

# Local, International and Global Regulations

Regulations and accrediting organisations vary among industries and on the locations of your business operations.

Location specific regulations like the Gramm-Leach-Bliley Act (GLBA) is a United States federal law that requires financial institutions to explain how they share and protect customers' private information.

Internationally recognised regulations such as the food and beverage industry Hazard Analysis and Critical Control Point (HACCP) is a science-based, food safety system that is used to help ensure the manufacture of safe food products.

Health Insurance Portability and Accountability Act (HIPAA) are a series of federal regulatory standards to protect sensitive patient health information from being disclosed without the patient's knowledge or consent in the United States only. HIPAA does not have international or extraterritorial jurisdiction.
In Europe and the UK, we are protected by General Data Protection Regulation (GDPR) Data Protection Act.

Globally recognised regulations such as Payment Card Industry Data Security Standard (PCI-DSS) in the financial industry for ensuring secure card payments.

The new Global Environmental, Social and Governance (ESG) regulation that evolved in 2022, focuses on the environment, and the economic recovery from the impact of the coronavirus pandemic.
Since the pandemic governments and regulators see an opportunity to reshape policies and frameworks encouraged by the global effort to meet the ESG targets set by landmark agreements, including the Paris Climate Agreement and the UN Sustainable Development Goals, by 2030.

Global ESG regulation is set to make a leap with new requirements for private businesses to report on and prevent adverse impacts on climate, the environment, and human rights.

In 2024 we can expect to see many changes in the world of regulatory compliance that will have an enormous impact on many industries globally.

# Industry Specific Regulations

Regulatory compliance standards are designed for specific industries, with the consideration that some industries are more heavily regulated than others.

Highly regulated industries include:

- Finance
- Environment
- Health
- Food
- Utilities / Energy
- Legal
- Engineering
- Construction
- Manufacturing

Least regulated professions include:

- Holistic healthcare
- Management consultants
- Performing Arts
- Pet Sitting / Walking Service
- Civic and Social Organisations

The standards outlined for the food industry for example focus on the entire supply chain to ensure product safety, while financial services industries may focus on storing and handling sensitive data and cybersecurity.

A few examples:

**Medical and Healthcare Practices**

These organisations have strict compliance laws to protect sensitive and personal patient data. Their regulating body HIPAA (The Health Insurance Portability and Accountability Act of 1996 a United States federal regulation) outlines data privacy and security regulations designed to secure patients' medical information.

HIPAA requires these organisations and their business associates to notify patients following a data breach.
Any of their Cloud Service Providers (CSP) and other business associates of their organisations must also comply with HIPAA privacy, security, and breach notification rules.

**Financial Services**

Are subject to regulatory compliance rules specifically designed to protect its customers' personal data and investors from disreputable business practices.

The Financial Conduct Authority (FCA) regulates the financial services industry in the UK. Its role includes protecting consumers and promoting healthy competition between financial service providers.

In the United States the Securities and Exchange Commission (SEC), Federal Reserve Board (FRB), the Federal Deposit Insurance Corp. (FDIC), and the Securities and Exchange Commission (SEC) oversee how banks, the stock market, and other major financial institutions are regulated

Several standards may oversee how you do business and store data, but you should always research the regulatory compliance requirements that directly impact your business or industry.

Many organisations need outside consultation to help understand the regulatory compliance standards that affect their business and the business processes that must be put into place.

# Regulatory Organisations

## Regulatory Agencies

Businesses are regulated and policed for compliance by different regulatory agencies, based on their industry, and not on the location of their operations, be it locally, internationally, or globally.
They are regulated to raise standards, protect consumers and the wider public from practitioners who do not have the necessary skills or training to provide quality products and or services.

Appointed government and independent, regulators are responsible for investigating, carrying out audits, enforcing safety standards to ensure compliance to protect consumers.
These regulatory agencies can also fine businesses for non-compliance.
For some businesses to enter a specific industry, they must obtain a license to operate from the sector regulator. This license sets out the conditions by which they must abide.

Regulatory agencies typically have powers to:

- Obligate a company to obtain a license to enter a particular industry
- Require a company to be open with information
- Monitor the performance and investigate a company for regulatory compliance
- Publish findings of any investigations for a company that fails to comply with regulatory compliance
- Direct a company to comply through orders, impose financial penalties and/or revoking its license to operate
- Prosecute a non-compliant company via civil courts

## International Organisation for Standardisation (ISO)

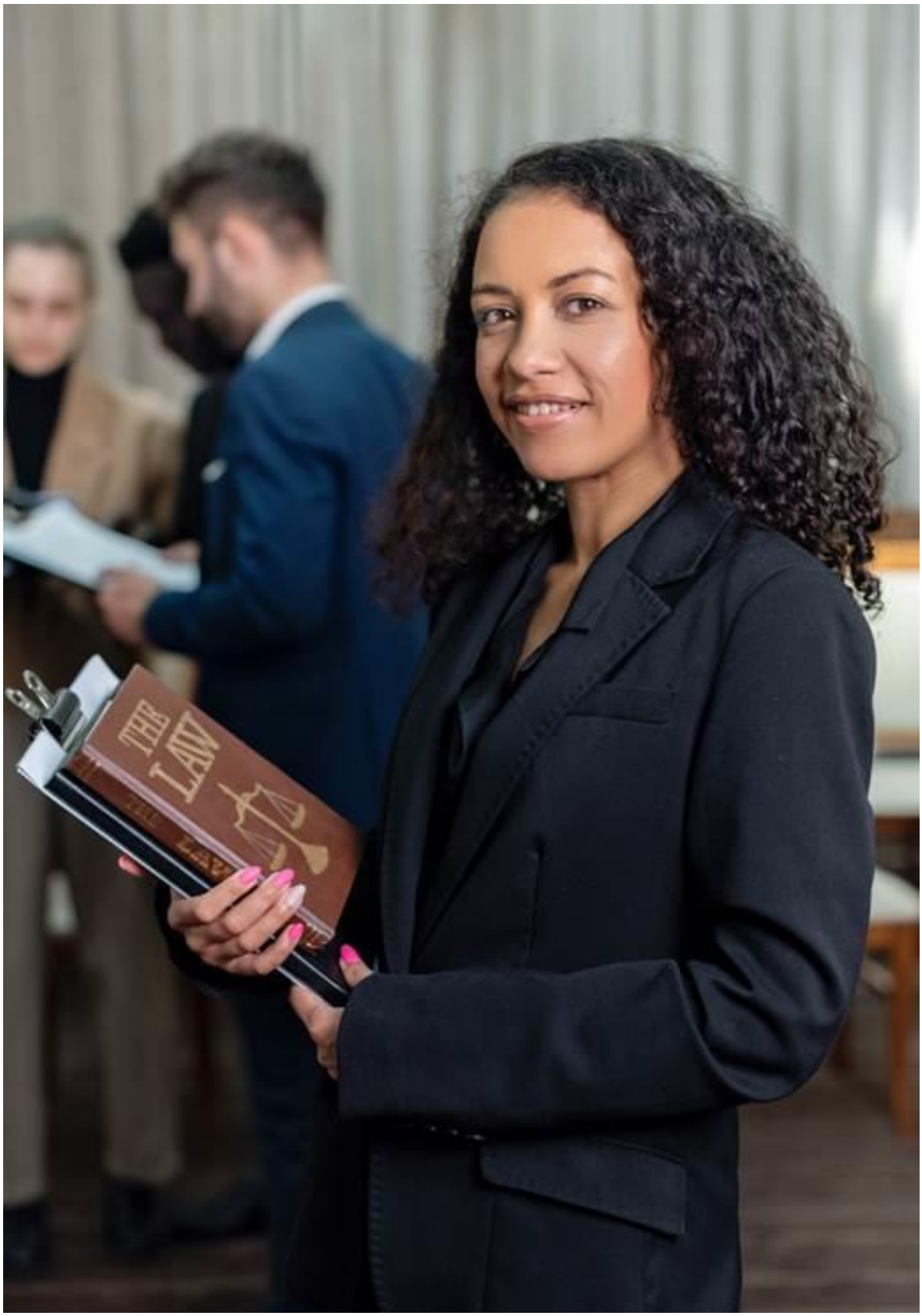
In 1946 London UK, 65 delegates from 25 countries met to discuss the future of International Standardisation, becoming what we know today is the ISO.
The ISO is one of the primary international standards for how businesses handle regulatory compliance.

ISO is an independent, non-governmental international organisation, operating from Geneva, Switzerland with a membership of 167 national standards bodies, made up of people who are subject matter expert that know the needs of the organisations they represent.

The experts that make up ISO share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

ISO standards are internationally agreed by experts, formulating the best way of making a product, managing a process, delivering a service, or supplying materials.

# Industry Regulators



**Professions that are regulated, and their regulators**

**Finance**

Financial Conduct Authority (FCA)

Regulates financial services firms and financial markets in the UK and operates independently of the UK Government.
The FCA provides services to consumers and focuses on the regulation of retail and wholesale financial services firms.

Federal Reserve System (The FED)

Probably the best-known of all the banking regulatory agencies in the U.S is the central banking system of the United States of America central control of the monetary system in order to alleviate financial crises.

For a list of financial regulatory authorities by country Click Here.

**Environment**

The Environment Agency (EA)

Sponsored by the United Kingdom government's Department for Environment, Food and Rural Affairs. The EA is responsible for flood management, regulating land and water pollution, conservation, and for the protection, and enhancement of the environment in England.

The US Environmental Protection Agency (EPA)

The Environmental Protection Agency protects people's health and the environment. They work to ensure Americans have clean air, land and water, research, develops and enforces environmental regulations.

For a list of environment regulatory organisations by country Click Here

**Health**

Care Quality Commission (CQC)

The CQC's are independent regulator of health and social care in England whose role is to make sure that hospitals, care homes, dental and general practices and other care services in England provide people with safe, effective, and high-quality care, and to encourage those providers to improve.

Medicines & Healthcare products Regulatory Agency (MHRA)

The MHRA is an executive agency of the Department of Health and Social Care in the UK responsible for ensuring that medicines and medical devices work and are acceptably safe.

The Centers for Medicare and Medicaid (CMS)

In the US the CMS is part of the Department of Health and Human Services (HHS). supervise and regulate the conditions linked to the healthcare system, providing care at a subsidized rate through different programs.

Control of Substances Hazardous to Health (COSHH)

COSHH is a set of regulations put in place to protect workers from ill health that requires employers to control substances that are hazardous to health when working with specific substances and materials. Breach of COSHH regulations by an employer or employee is a crime, punishable by an unlimited fine.

The Drug Enforcement Agent (DEA)

The DEA is the federal organisation in charge of enforcing the controlled substances laws of the United States.

## Food and Drugs

Food Standards Agency

A non-ministerial department of the Government of the United Kingdom, responsible for protecting public health in relation to food in England, Wales and Northern Ireland.

Food and Drug Administration (FDA)

The US FDA is a federal agency of the Department of Health and Human Services responsible for protecting, promoting and enforcing public health through the control and supervision of food safety, tobacco products, caffeine products, dietary supplements, prescription and over-the-counter pharmaceutical drugs (medications), vaccines, biopharmaceuticals, blood transfusions, medical devices, electromagnetic radiation emitting devices (ERED), cosmetics, animal foods & feed, and veterinary products.

For a list of health regulatory organisations by country Click Here

Good Manufacturing Practice (GMP)

Endorsed by the US Food and Drug Administration, GMP has been incorporated into in more than 100 countries as their national medicines law.

GMP regulations requires the manufacturers, processors, and packagers of drugs, medical devices, and some foods, to take proactive measures to ensure that their products are safe, pure, and effective, and protect consumers from purchasing dangerous or non-effective products.

Firms failing to comply with GMP regulations including record keeping, personnel qualifications, sanitation, cleanliness, equipment verification, process validation, and complaint handling, can result in product recall, confiscation, fines, or even prison.

GMP is also referred to as current Good Manufacturing Practice (cGMP) as a reminder to manufacturers that they must employ technologies and systems which are up to date to comply with the regulation.

Good Distribution Practice (GDP)

Organisations that must comply with good manufacturing practice (GMP) may also need to comply with GDP.

Organisation that manufactures or distributes human or veterinary medicines, need to apply for a manufacturer or wholesaler dealer license.
The Medicines and Healthcare products Regulatory Agency (MHRA) are obligated to carry out inspections to check that their manufacturing and distribution sites comply with GMP or GDP.

**Legal**

Are primed to protect consumers' interests, promote high professional standards and encourage a diverse and effective legal profession.

The Solicitors Regulation Authority (SRA)

The SRA is the regulator of solicitors and law firms in England and Wales.
Responsible for regulating the professional conduct of solicitors and other authorised individuals law firms, those working in-house at private and public sector organisations.

**Data Protection**

Almost all professions globally will be compelled to comply with data protection laws.

Information Commissioner's Office (ICO)

Reporting directly to the Parliament of the United Kingdom, ICO is the independent regulatory office (national data protection authority) dealing with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).
Their role includes protecting personal information, providing access to official information, and to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

California Consumer Privacy Act (CCPA)

The CCPA gives California consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law.

**Utilities**

The Office of Communications (Ofcom)

The UK government-approved regulatory and competition authority for the broadcasting, telecommunications, and postal industries.
Ofcom has wide-ranging powers across the television, radio, telecoms, and postal sectors.
It has a statutory duty to represent the interests of citizens and consumers by promoting competition and protecting the public from harmful or offensive material.

Federal Communications Commission (FCC)

The FCC is an independent agency of the United States federal government that regulates communications by radio, television, wire, satellite, and cable across the United States. The FCC maintains jurisdiction over the areas of broadband access, fair competition, radio frequency use, media responsibility, public safety, and homeland security.

The Office of Gas and Electricity Markets (Ofgem)

Supporting the Gas and Electricity Markets Authority (GEMA), Ofgem is the UKs government independent energy regulator for electricity and natural gas markets, responsible for protecting energy consumers, especially vulnerable people, by ensuring they are treated fairly and benefit from a cleaner, greener environment.

The Federal Energy Regulatory Commission (FERC)

An independent federal regulatory agency established by the United States Congress to license hydroelectric facilities and to regulate wholesale sales of electric energy and natural gas.

## Engineering

Regulators set and maintains internationally standards to ensure confidence to the public of professionally registered engineers.

The Engineering Council

The UK regulatory body for the engineering profession, that holds the national registers of engineers.

## Manufacturing

These firms are regulated to ensure that the products they make, or import, comply with the law in their jurisdiction, and are safe for consumers to use.

Health and Safety Executive (HSE)

In the UK the HSE oversee the health and safety in the manufacturing sector to reduce work-related deaths, injuries, and ill health.

## Construction

Regulators establish the minimum standards that building firms must achieve in the construction of buildings.

Building Safety Regulator (BSR)

The Building Safety Act names Health and Safety Executive (HSE) as the new Building Safety Regulator in England.

The BSR will have 3 main functions:

- Overseeing the safety and standards of all buildings
- Helping and encouraging the construction professionals to improve their competence
- Leading implementation of the new regulatory framework for high-rise buildings

## Consumer Protection

The Consumer Rights Act 2015

TBA - UK Government announced in 2021 a potential revised and enhanced 2023 Bill

This Act is in place to safeguard buyers and the public when purchasing goods and or services against unfair practices.

The Consumer Protection Association (CPA)

Regulated by the FCA, The CPA safeguard and protect consumers against unfair practices when purchasing goods and or services, and can assist resolve problems with:

- Faulty goods
- Poor service
- Builders
- Rogue traders
- Credit and store cards

# Non-Regulatory Organisations

Below are some useful non-regulatory organisations to be familiar with:

The Competitions and Markets Authority (CMA)

The Competition and Markets Authority (CMA) is not an economic regulator but has overall responsibility for the UK's competition regime.
This is good to know if you need to report any competition or consumer issues.

The World Health Organisation

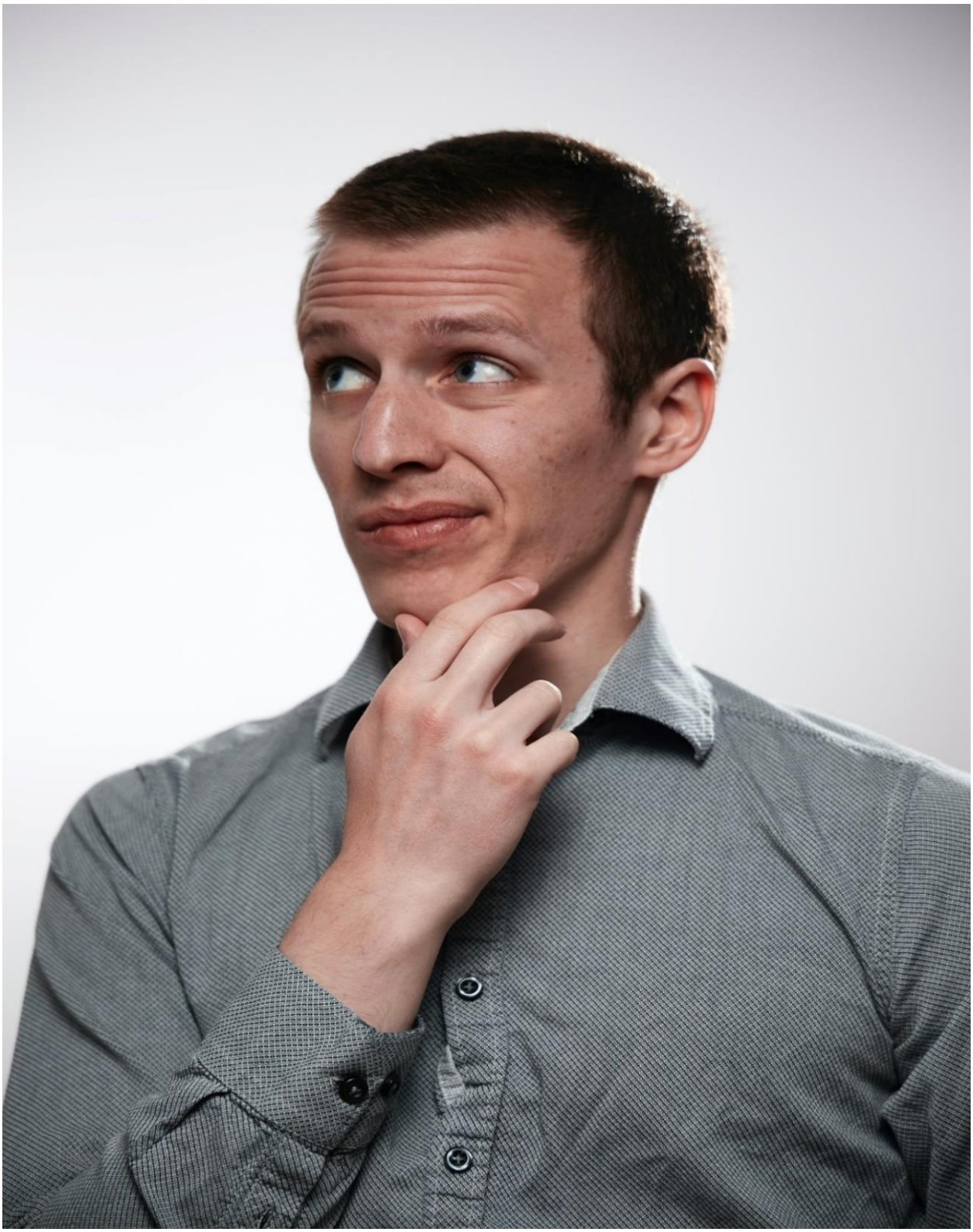
WHO is the United Nations agency, that connects nations, partners, and people to promote health, keep the world safe, and serve the vulnerable, so everyone, everywhere can attain the highest level of health.

The World Trade Organisation

The World Trade Organization (WTO) is the only global international organisation that deals with the rules of trade between nations.

The primary purpose of the WTO is to open trade for the benefit of all, operate a global system of trade rules, acting as a forum for negotiating trade agreements, settles trade disputes between its members and, supports the needs of developing countries.

# Why the Need to Comply?



Companies that do not follow mandatory regulatory compliance laws, face consequences, including on-site compliance audits, inspections by the appropriate regulatory agency, fines, penalties, and in some cases a prison sentence.
Brand reputation can also be damaged, resulting in the loss of customers, suppliers, and prospects, all of which could result in the potential loss of the business.

Regulatory compliance rules require companies to evaluate and develop processes to enable them to meet obligations specific to their industry and locations.

Steps an organisation can take to achieve regulatory compliance:

**Plan, Do, Check, Act rule**

1. Define your goals, identify, and determine all applicable industry and operational compliance regulations, in alignment with your organisation.

2. Plan how your organisation will implement processes and procedures to enable your company meets its applicable regulatory laws.

3. Establish, document and train staff on company compliance policies, processes, and procedures, with specific instructions for each role involved in maintaining compliance.

4. Maintain all documentation as evidence for regulatory audits.

5. Keep up to date with changing laws and regulations.

6. Schedule regular internal audits, and check employees follow procedures Set Reminders, make checklists available and have appropriate signage at the right points around your business to help make sure your procedures are followed.

7. Regularly monitor company compliance processes and procedures to determine if they are current and still relevant to the company.
   If they are outdated, make and communicate any changes where necessary.

8. Keep documentation up to date, and ensure employees are familiar with revised processes and procedures to meet the organisations compliance requirements.

# Conclusion

Constantly evolving consumer technologies present compliance complications for all companies globally in the future.

The increased use of mobile devices, the growth of the internet of things (IoT) has led to huge expansion in the number of endpoints and interconnected devices.
This presents new compliance concerns, as these devices can store sensitive, compliance-relevant company data that can get lost or stolen.

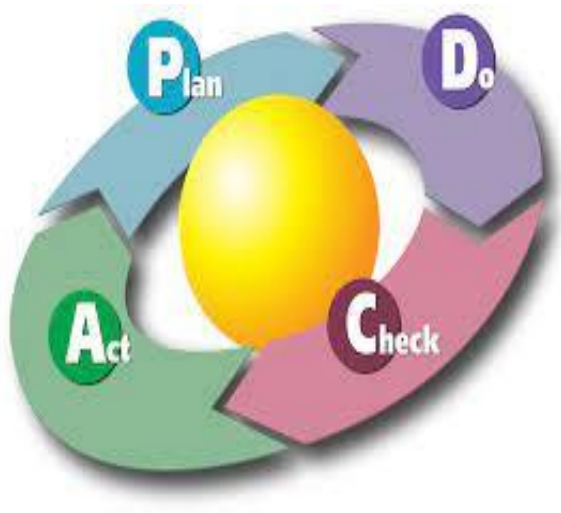
For organisations that have not fully digitised and still maintain manual paper-based systems to manage regulatory compliance, face a future of even more time consuming, and costly processes and procedures.

Companies that have transitioned to digital ways of working, cannot sit back, and relax, they too face updating and maintaining systems to remain compliant.
They must stay on top of required system updates and immediately patch or upgrade compliance software when vulnerabilities are detected, paying particular attention to increase in the risks of cyberattacks.

In recent years a host of new regulations have come into force, and no doubt new ones will appear, making managing compliance potentially daunting.

Developing a strong compliance strategy may seem challenging, requiring significant changes in the way that your organisation operates.
However, it is essential to future proof your business, avoid significant financial penalties, preserve business reputation and remaining on the correct side of the law, you must ensure to have proper procedures in place to maintain compliance with the shifting regulatory landscape.

**4 Phases of a Compliance Management**




**Plan**
Define your goals, and plan how your organisation will implement processes and procedures to meets regulatory laws
**Do**
Establish, document and train staff on company compliance policies, processes, and procedures
**Check**
If any laws or regulations have changed, and employees are following procedures.
**Act**
Monitor, make necessary changes and communicate any changes.

**Image Credits**

Regulatory Compliance Guide by Master1305
Industry Specific
- Clockwise
- Image by aleksandarlittlewolf
- Image by ASphotofamily
- Image by wavebreakmedia
- Image by Gpointstudio

Industry Regulators by Mikhail Nilov
Consumer Protection by cookie studio
Why do I need to comply by Ludovic Migneault
The Consumer Rights Act 2015 by freepik.com

**Disclaimer**

P4P Compliance Management Limited work very hard to provide up-to-date accurate information through comprehensive research at the time of publishing; however, some information may understandably be less accurate as time passes.

We make no representations or warranties of any kind (expressed or implied) about the completeness, accuracy, reliability, suitability, or availability of any information, products, services, or related graphics contained in this article.

No liability is assumed for losses or damages due to the information provided.
You are responsible for your own choices, actions, and results.