The QUARTET

Issue 1. April 2024

SANCERT AND ISO 13485 FOR MEDICAL DEVICES

ISO 13485 is a crucial certification for medical devices, manufacturers, and suppliers alike. It sets comprehensive requirements for quality management tailored to the industry. Compliance with this standard assures commitment to the highest standards of quality, safety, and regulatory compliance. It also serves as a foundational framework for meeting regulatory requirements, harmonizing with regulatory frameworks worldwide. **ISO 13485** certification instills confidence in the reliability and safety of medical devices and assures stakeholders that products have undergone rigorous quality assurance processes. It also facilitates access to international markets and enhances competitiveness on a global scale. If you need guidance or information related to **ISO 13485**, please contact **SANCERT** at **info@sancert.global**.

Q: What is ISO/IEC 27001?

It is a standard that specifies requirements for an Information Security Management System (ISMS). **ISO/IEC 27001:2013** and **ISO/IEC 27001:2022** have key differences. The latest version includes revised requirements to reflect changes in technology and cybersecurity threats. It offers enhanced guidance and aligns more closely with related standards. There are changes to the approach to risk assessment and treatment, and it incorporates provisions to address evolving legal and regulatory requirements. It also emphasizes the importance of resilience and continuity planning.

GENERAL UPDATE – Climate Change and ISO

The International Organisation for Standardisation (ISO) has amended thirty-one existing management system standards to integrate climate change considerations. This development highlights the importance of environmental sustainability and resilience for businesses worldwide. This means that companies must review and update their management systems to integrate climate change considerations. **Key aspects include climate risk assessment, mitigation and adaptation strategies, stakeholder engagement, monitoring and reporting, and continuous improvement.** The integration of climate change considerations can help organisations mitigate risks and unlock new opportunities for growth, innovation, and competitive advantage.

The primary difference between ISO/IEC 27001:2013 and ISO/IEC 27001:2022 is the updates and revisions made to ensure its relevance and effectiveness in addressing modern cybersecurity challenges and emerging threats.

Welcome

to Issue 1 of ***The QUARTET*** *newsletter! We are excited to share valuable insights with you!*

DID YOU KNOW

Organisations certified to ISO/IEC 27001:2013 must upgrade to ISO/IEC 27001:2022 by October 2025. Get the compliance guide at www.sancert.global under "Resources". Contact leon@sancert.global for further assistance.

QUality and Reliability Through Expertise and Teamwork

71-75 Shelton Street
Covent Garden
London
WC2H 9JQ
UK
Company No: 10801005

1st Floor, Block B, North Park
Black River Park
2 Fir Street
Observatory,
Cape Town, 7925
Reg No: 2005/037342/07

www.sancert.global

info@sancert.global

The QUARTET

Issue 1. April 2024

CLIMATE CHANGE AND ISO

The International Organisation for Standardization (ISO) has taken a significant step towards addressing the growing concerns over climate change by adding climate change considerations into organisational management systems. **On February 22, 2024, an amendment was issued that impacted thirty-one existing management system standards.** This development highlights the urgent need for businesses worldwide to prioritise environmental sustainability and resilience in their operations.

The standards affected by this amendment include ISO 9001 (Quality Management Systems), ISO 14001 (Environmental Management Systems), ISO 27001 (Information Security Management Systems), and ISO 45001 (Occupational Health and Safety Management Systems). These are widely recognised standards that guide organisations towards operational excellence and compliance.

The amendment seeks to ensure that climate change risks and opportunities are systematically incorporated into organisational management systems. This integration helps businesses manage their environmental impacts, enhance resilience, and seize opportunities towards sustainability.

Organisations certified under ISO standards need to review and update their management systems to integrate climate change considerations. This involves revisiting policies, procedures, risk assessments, and performance indicators to align with new requirements.

Key aspects that organisations may need to address include:

- **Climate Risk Assessment:** Conduct thorough assessments to identify and evaluate climate-related risks and opportunities pertinent to the organisation's operations, supply chain, and stakeholders.
- **Mitigation and Adaptation Strategies:** Developing and implementing strategies to mitigate greenhouse gas emissions, adapt to climate impacts, and enhance resilience across the value chain.
- **Stakeholder Engagement:** Engaging with stakeholders, including customers, suppliers, employees, and communities, to foster collaboration, transparency, and shared responsibility towards climate action.
- **Monitoring and Reporting:** Establishing robust monitoring and reporting mechanisms to track progress towards climate-related goals, comply with regulatory requirements, and communicate performance effectively.
- **Continuous Improvement:** Embracing a culture of continuous improvement to drive innovation, optimise resource efficiency, and enhance the organisation's overall environmental performance.

The amendment underscores the pivotal role of ISO standards in **driving sustainable development** and **fostering resilience** in the face of climate change. By integrating climate considerations into management systems, organisations can not only mitigate risks but also unlock new opportunities for growth, innovation, and competitive advantage in a rapidly evolving global landscape.

In summary, the recent amendment to ISO standards calls for businesses to embrace sustainability as a core principle guiding their operations.

By leveraging ISO standards, businesses can navigate uncertainties, build resilience, and contribute to a more sustainable future.

QUality and Reliability Through Expertise and Teamwork

71-75 Shelton Street
Covent Garden
London
WC2H 9JQ
UK
Company No: 10801005

1st Floor, Block B, North Park
Black River Park
2 Fir Street
Observatory,
Cape Town, 7925
Reg No: 2005/037342/07

www.sancert.global

info@sancert.global

The QUARTET

Issue 1. April 2024

ISO 13485 MEDICAL DEVICES

In the complex and crucial field of healthcare, maintaining high standards of precision, safety, and reliability is of utmost importance. Adherence to strict quality standards is non-negotiable. One of the most critical certifications in this domain is **ISO 13485**. This globally recognised standard is specifically designed for the medical device industry. **SANCERT** has obtained accreditation for this standard from SANAS and is in the process of registering with SAHPRA (South African Health Products Regulatory Authority) as an accredited certification service provider. We have developed a cost-effective approach for carrying out ISO 13485 accredited certifications for all SAHPRA members. This will become a mandatory requirement by the end of 2025, therefore anyone operating in the medical devices space should consider this.

ISO 13485 outlines the complete requirements for creating and maintaining a quality management system (QMS) that is tailored to the needs of medical device manufacturers, repair operations, importers, and suppliers. Being compliant with this standard shows the commitment of an organisation to maintain the **highest standards of quality, safety, and regulatory compliance** throughout the lifecycle of its products.

In an industry subject to stringent regulatory oversight across jurisdictions, ISO 13485 certification serves as a **foundational framework for meeting regulatory requirements**. It harmonizes with regulatory frameworks worldwide, including the European Medical Device Regulation (MDR) and the U.S. Food and Drug Administration (FDA) Quality System Regulation (QSR), facilitating smoother regulatory approvals and market access.

ISO 13485 certification assures healthcare providers, patients, and regulatory bodies that medical devices are reliable and safe. It signifies rigorous quality assurance processes, and adherence to industry best practices and standards, leading to improved patient outcomes and satisfaction.

ISO 13485 places a strong emphasis on **risk management** throughout the product lifecycle. By systematically identifying, assessing, and mitigating risks associated with medical devices, manufacturers can proactively address potential hazards and ensure the safety and efficacy of their products, minimizing the likelihood of adverse events or recalls.

ISO 13485 certification serves as a passport to **global markets**, facilitating access to international markets and enhancing competitiveness on a global scale. In an industry where even the smallest oversight can have profound consequences, ISO 13485 certification stands as a beacon of **quality, safety, and reliability in medical device manufacturing**.

By adhering to this rigorous standard, organizations demonstrate their unwavering commitment to excellence, regulatory compliance, and the well-being of patients worldwide.

QUality and Reliability Through Expertise and Teamwork

71-75 Shelton Street
Covent Garden
London
WC2H 9JQ
UK
Company No: 10801005

1st Floor, Block B, North Park
Black River Park
2 Fir Street
Observatory,
Cape Town, 7925
Reg No: 2005/037342/07

www.sancert.global

info@sancert.global

SANCERT
GLOBAL ISO CERTIFICATION SERVICES

The QUARTET

Issue 1. April 2024

ISO/IEC 27001 Information Security Management System

ISO/IEC 27001 is a standard that specifies requirements for an information security management system (ISMS). The primary distinction between **ISO/IEC 27001:2013** and **ISO/IEC 27001:2022** is that the latter was revised to address **contemporary information security challenges**.

KEY DIFFERENCES MAY INCLUDE:

- **Changes to consider:** Revised requirements to reflect changes in technology, cybersecurity threats, and best practices in information security management.
- **Enhanced Guidance:** The latest version may offer enhanced guidance or clarification on existing requirements to improve understanding and implementation of the standard.
- **Alignment with Other Standards:** ISO/IEC 27001:2022 aligns more closely with other related standards, such as ISO 9001 (Quality Management Systems) and ISO 45001 (Occupational Health and Safety Management Systems), to facilitate integrated management system approaches within organisations. Easier to integrate and reduce documented procedures.
- **Risk Assessment and Treatment:** There may be changes in the approach to risk assessment and treatment, including updates to risk management methodologies and considerations of emerging risks, such as those related to cloud computing, IoT, and remote work. The climate change approach also needs to be considered.
- **Adaptation to Legal and Regulatory Changes:** The latest version incorporates provisions to address evolving legal and regulatory requirements related to information security and data protection, such as GDPR (General Data Protection Regulation) or other regional privacy laws e.g. POPI Act.
- **Improved Resilience and Continuity Planning:** ISO/IEC 27001:2022 emphasises the importance of resilience and continuity planning to ensure organisations can effectively respond to and recover from cybersecurity incidents and disruptions.

Organisations certified to ISO/IEC 27001:2013 must upgrade to ISO/IEC 27001:2022 by the end of October 2025.

Please visit the resources page on the sancert.global website to download a compliance guide for ISO/IEC27001:2022.

71-75 Shelton Street
Covent Garden
London
WC2H 9JQ
UK
Company No: 10801005

1st Floor, Block B, North Park
Black River Park
2 Fir Street
Observatory,
Cape Town, 7925
Reg No: 2005/037342/07

www.sancert.global

info@sancert.global