

## ISO27001/ISO27002: Guida Tascabile

**This useful pocket guide is an ideal introduction for those wanting to understand more about ISO 38500. It describes the scope, application and objectives of the Standard and outlines its six core principles.**

**Proteggi le informazioni della tua organizzazione con ISO27001:2013 Le informazioni costituiscono una delle risorse più importanti della tua organizzazione, e proteggerne la sicurezza è di importanza vitale per la tua attività. Questa pratica guida tascabile costituisce una panoramica essenziale di due norme di sicurezza delle informazioni che prende in esame i requisiti formali (ISO27001:2013) per la creazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), e le procedure consigliate (ISO27002:2013) rivolte ai responsabili dell'avvio, dell'attuazione o del mantenimento di tale sistema. Un SGSI basato sulle norme ISO27001/ISO27002 presenta numerosi vantaggi: Una maggiore efficienza derivante dalla messa in atto di sistemi e procedure di sicurezza delle informazioni, consentendoti di concentrarti maggiormente sul tuo core business. Protegge il tuo patrimonio informativo da un gran numero di minacce informatiche, attività criminose, compromissione interna dei dati e errori di sistema. Gestisce i tuoi rischi in modo sistematico e stabilisce piani d'azione per eliminare o ridurre le minacce informatiche. Consente il rilevamento precoce di minacce o errori d'elaborazione e la loro rapida risoluzione. Qual è il passo successivo verso la certificazione? Puoi disporre una verifica indipendente del tuo SGSI per accertarne la conformità alle specifiche dello standard ISO27001 e, in caso di conformità, ottenere quindi la certificazione accreditata. Pubblichiamo una vasta gamma di compendi e libri documentativi sullo standard SGSI (come I Nove Passi Per il Successo) che possono aiutarti a conseguire tale obiettivo. Indice Il gruppo di norme sulla sicurezza delle informazioni ISO/IEC 27000 ; Il contesto delle norme; Specifica e codice di comportamento a confronto; Il processo di certificazione; Il SGSI e l'ISO27001; Panoramica dell'ISO/IEC 27001:2013; Panoramica dell'ISO/IEC 27002:2013; Documentazione e registrazioni; Responsabilità della direzione; Approccio al processo e ciclo PDCA; Contesto, politica e campo di applicazione; Valutazione dei rischi; La dichiarazione di applicabilità; Attuazione; Check and Act; Riesame della direzione; Allegato A ISO27001**

**This pocket guide serves as an introduction to the National Institute of Standards and Technology (NIST) and to its Cybersecurity Framework (CSF). This is a US focused product. Now more than ever, organizations need to have a strong and flexible cybersecurity strategy in place in order to both protect themselves and be able to continue business in the event of a successful attack. The NIST CSF is a framework for organizations to manage and mitigate cybersecurity risk based on existing standards, guidelines, and practices. With this pocket guide you can: Adapt the CSF for organizations of any size to implement Establish an entirely new cybersecurity program, improve an existing one, or simply provide an opportunity to review your cybersecurity practices Break down the CSF and understand how other frameworks, such as ISO 27001 and ISO 22301, can integrate into your cybersecurity framework By implementing the CSF in accordance with their needs, organizations can manage cybersecurity risks in the most cost-effective way possible, maximizing the return on investment in the organization's security. This pocket guide also aims to help you take a structured, sensible, risk-based approach to cybersecurity.**

**This book provides an accessible overview of the changes you need to make in your organization to comply with the new law. --**

**Follow Me**

**Cyber Essentials**

**How to Achieve Personal and Business Goals**

**Full Fledged Information on Implementing End-to-End Information Security with Real Time Statistical Data and Analysis**

**PCI DSS: A pocket guide, sixth edition**

**EU Code of Conduct for Cloud Service Providers - A guide to compliance**

*In the third in Katharine Ashe's Prince Catchers series, the eldest of three very different sisters must fulfill a prophecy to discover their birthright. But if Eleanor is destined to marry a prince, why can't she resist the scoundrel who seduced her? She can pour tea, manage a household, and sew a modest gown. In short, Eleanor Caulfield is the perfect vicar's daughter. Yet there was a time when she'd risked everything for a black-eyed gypsy who left her brokenhearted. Now he stands before her—dark, virile, and ready to escort her on a journey to find the truth about her heritage. Leaving eleven years ago should have given Taliesin freedom. Instead he's returned to Eleanor, determined to have her all to himself, tempting her with kisses and promising her a passion she's so long denied herself. But if he was infatuated before, he's utterly unprepared for what will happen when Eleanor decides to abandon convention—and truly live . . .*

*Risk management: how to achieve personal and business goals is a book with a completely didactic approach where the author explains how risk (or uncertainty) affects both in our personal life and in the business environment. He defines risk as the effect of uncertainty on the achievement of objectives and that is why it is essential to know how to identify, measure and establish controls to meet those objectives. Diego guides us through different examples, with different approaches in which risk has been managed successfully and others not so much. In the latter, he explains what the errors were or why the methodologies used did not work. Likewise, it presents us with various situations in our daily life in which we deal with risk and the fulfillment of objectives (health, professional career, personal finances, sports practices or risky activities). In general, our treatment is rather intuitive and we react in different ways to risk. Without a doubt, we will be more likely to meet our goals and objectives using a proven method. At the end of the book, you will have tools to identify, analyze, evaluate, manage and monitor the risks that could prevent you from achieving your objectives or goals, both in your daily life and in your professional or organizational life.*

*This pocket guide is perfect as a quick reference for PCI professionals, or as a handy introduction for new staff. It explains the fundamental concepts of the latest iteration of the PCI DSS, v3.2.1, making it an ideal training resource. It will teach you how to protect your customers' cardholder data with best practice from the Standard.*

*Information technology plays a fundamental role in the operations of any modern business. While the confidentiality and integrity of your organisation's information have to be protected, a business still needs to have this information readily available in order to be able to function from day to day. If you are an information security practitioner, you need to be able to sell complex and often technical solutions to boards and management teams. Persuading the board to invest in information security measures requires sales skills. As an information security professional, you are a scientific and technical specialist; and yet you need to get your message across to people whose primary interests lie elsewhere, in turnover and overall*

*performance. In other words, you need to develop sales and marketing skills. This pocket guide will help you with the essential sales skills that persuade company directors to commit money and resources to your information security initiatives.*

*ISO 27001 controls – A guide to implementing and auditing*

*PCI DSS: A Pocket Guide, fifth edition*

*Guida Tascabile*

*Implementing and Auditing an Information Security Management System in Small and Medium-Sized Businesses*

*Risk Assessment for Asset Owners*

*Information Security Risk Management for ISO 27001/ISO 27002, third edition*

Work-life balance is one of the most important issues facing employers and managers today. Employees at all levels are no longer willing to trade their quality of life in order to get a decent standard of living. Managers can no longer afford to ignore the fact that the long-hours culture imposes on their organisation. Overwork causes stress-related absenteeism, poor retention levels, low creativity, appalling customer service and unethical employee behaviour. Combine that with the risks of being sued by a stressed employee or a parent who wanted to work flexibly, and the business case for paying real attention to work-life issues has never been stronger. This text sets out a roadmap for moving your organisation towards a positive work-life culture. With clear and practical advice for HR and line managers alike, *Managing Work-Life Balance* shows you how to engage employers, managers and employees in the process of controlling the inherent conflicts between the worlds of work and home.

This new downloadable pocket guide in the Practical IT Governance series, is designed to provide the reader with a basic understanding of how an organization's Information Technology supports and enables the achievement of its strategies and objectives. Presents the compelling business case for implementing ISO27001:2013 to protect information assets. Perfect for supporting an ISO27001 project proposal.

Understand the basics of business continuity and ISO 22301:2019 with this concise pocket guide, which will help you ensure your organisation can continue to operate in the event of a disruption.

*A Guide for HR in Achieving Organisational and Individual Change*

*IT Governance*

*Implementing ISO 27001 Simplified*

*EU GDPR*

*An ISO27001:2013 Implementation Overview, Third edition*

*The IT Governance Standard*

The emergence of ISO/IEC 38500 OCo the international standard for the corporate governance of information and communication technology OCo puts boards around the world in a position from which they can take effective action to apply core governance principles to their information and communication technology."

Helping you to conduct effective, value-for-money penetration testing, this guide is designed to enable your organisation to plan for a penetration test,

select an appropriate third party provider and manage all important related activities

For many companies, their intellectual property can often be more valuable than their physical assets. Having an effective IT governance strategy in place can protect this intellectual property, reducing the risk of theft and infringement. Data protection, privacy and breach regulations, computer misuse around investigatory powers are part of a complex and often competing range of requirements to which directors must respond. There is increasingly the need for an overarching information security framework that can provide context and coherence to compliance activity worldwide. IT Governance is a key resource for forward-thinking managers and executives at all levels, enabling them to understand how decisions about information technology in the organization should be made and monitored, and, in particular, how information security risks are best dealt with. The development of IT governance - which recognises the convergence between business practice and IT management - makes it essential for managers at all levels, and in organizations of all sizes, to understand how best to deal with information security risk. The new edition has been fully updated to take account of the latest regulatory and technological developments, including the creation of the International Board for IT Governance Qualifications. IT Governance also includes new material on key international markets - including the UK and the US, Australia and South Africa.

This book is a pocket guide to the ISO27001 risk assessment, and designed to assist asset owners and others who are working within an ISO27001/ISO17799 framework to deliver a qualitative risk assessment. It conforms with the guidance provided in BS7799-3:2006 and NIST SP 800-30.

I Loved a Rogue

It Governance

An Introduction to the Linux Operating System and Command Line

A Primer, second edition

The Prince Catchers

Thrive under the GDPR (General Data Protection Regulation) wherever you are in the world. This pocket guide will help you understand the Regulation, the broader principles of data protection, and what the GDPR means for businesses in Europe and beyond.

An ideal introduction and a quick reference to PCI DSS version 3.2 All businesses that accept payment cards are prey for hackers and criminal gangs trying to steal financial information and commit identity fraud. The PCI DSS (Payment Card Industry Data Security Standard) exists to ensure that businesses process credit and debit card orders in a way that effectively protects cardholder data. All organisations that accept, store, transmit or process cardholder data must comply with the Standard; failure to do so can have serious consequences for their ability to process card payments. Product overview Co-written by a PCI QSA (Qualified Security Assessor) and updated to cover PCI DSS version 3.2, this handy pocket guide provides all the information you need to consider as you approach the PCI DSS. It is also

an ideal training resource for anyone in your organisation involved with payment card processing. Coverage includes: An overview of PCI DSS v3.2.A PCI self-assessment questionnaire (SAQ).Procedures and qualifications.An overview of the Payment Application Data Security Standard (PA-DSS).About the authors Alan Calder is the founder and executive chairman of IT Governance Ltd, an information, advice and consultancy firm that helps company boards tackle IT governance, risk management, compliance and information security issues. He has many years of senior management experience in the private and public sectors. Geraint Williams is a knowledgeable and experienced senior information security consultant and PCI QSA, with a strong technical background and experience of the PCI DSS and security testing. He leads the IT Governance CISSP Accelerated Training Programme, as well as the PCI Foundation and Implementer training courses. He has broad technical knowledge of security and IT infrastructure, including high performance computing and Cloud computing. His certifications include CISSP, PCI QSA, CREST Registered Tester, CEH and CHFI. This new book sets out for managers, executives and IT professionals the practical steps necessary to meet today's corporate and IT governance requirements. It provides practical guidance on how board executives and IT professionals can navigate, integrate and deploy to best corporate and commercial advantage the most widely used frameworks and standards.

This important new book - 'IT Governance: Guidelines for Directors' provides directors, executives, managers and professional advisers with clear,pragmatic guidelines for ensuring that IT and the business work together for thesamestrategic objectives.

A Guide to Effective Internal Management System Audits

Procuring Penetration Testing Services

EU GDPR – An international guide to compliance

Information Security Risk Management for ISO27001/ISO27002

Risk Management

ISO/IEC 38500

*Ideal for information security managers, auditors, consultants and organisations preparing for ISO 27001 certification, this book will help readers understand the requirements of an ISMS (information security management system) based on ISO 27001.*

*Drawing on international best practice, including ISO/IEC 27005, NIST SP800-30 and BS7799-3, the book explains in practical detail how to carry out an information security risk assessment. It covers key topics, such as risk scales, threats and vulnerabilities, selection of controls, and roles and responsibilities, and includes advice on choosing risk assessment software.*

*A penetration test involves the use of a variety of manual and automated techniques to simulate an attack on an organisation's information security arrangements – either from malicious outsiders or your own staff. Undertaking a series of penetration tests will help test your security arrangements and identify improvements.*

*Ideal for risk managers, information security managers, lead implementers, compliance managers and consultants, as well as providing useful background material for auditors, this book will enable readers to develop an ISO 27001-compliant risk assessment framework for their organisation and deliver real, bottom-line business benefits.*

*Foundations of Information Security Based on ISO27001 and ISO27002 - 3rd revised edition*

*An International Guide to Data Security and ISO27001/ISO27002*

*The Case for ISO27001:2013*

*Guidelines for Directors*

*ISO27001/ISO27002: Una guía de bolsillo*

*A Pocket Guide, Second Edition*

Proteja la información de su organización con la ISO27001:2013 La información es uno de los recursos más importantes de su organización y mantener esa información segura es vital para su negocio. Esta guía de bolsillo útil es una visión de conjunto esencial sobre las dos normas de la seguridad de la información clave que cubren los requisitos formales (ISO27001:2013) para crear un Sistema de Gestión de la Seguridad de la Información (SGSI) y las recomendaciones de mejores prácticas (ISO27002:2013) para aquellos responsables de iniciar, implementar o mantenerlo. Un SGSI basado en la ISO27001/ISO27002 ofrece un sinfín de beneficios: Eficacia mejorada implantando procedimientos y sistemas de seguridad de la información, que le permiten concentrarse en su actividad empresarial principal. Protege sus activos de información de un amplio abanico de ciberamenazas, actividad criminal, compromiso de información privilegiada y fallo del sistema. Gestione sus riesgos sistemáticamente y establezca planes para eliminar o reducir las ciberamenazas. Permite la detección temprana de amenazas o errores de procesamiento y una solución más rápida. ¿Siguiente paso para la certificación? Puede organizar una auditoría independiente de su SGSI frente a las especificaciones de la ISO27001 y, si su SGSI se ajusta, finalmente logra la certificación acreditada. Publicamos una variedad de libros y herramientas de documentación del SGSI (como Nueve pasos para el éxito) para ayudarle a lograr esto. Índice La familia de normas de la seguridad de la información ISO-/IEC 27000; Historia de las Normas; Especificación frente al Código de Prácticas; Proceso de certificación; El SGSI y la ISO27001; Visión de conjunto de la ISO/IEC 27001:2013; Visión de conjunto de la ISO/IEC 27002:2013; Documentación y registros; Responsabilidad de la gestión; Enfoque del proceso y el ciclo PDCA; Contexto, política y alcance; Evaluación del riesgo; La declaración de aplicabilidad (SoA); Implementación; 15. Verificar y actuar; Revisión gerencial; ISO27001; Anexo A

A Guide to Effective Internal Management System Audits provides a model for the management and implementation of internal audits that moves beyond simple compliance to ISO requirements and turns the internal audit into a transformational tool that the organization can use to assist with the management of risk, and implement improvements to management systems.

"Cyber Essentials certification will provide numerous benefits, including the opportunity to tender for business where certification to the scheme may be a prerequisite, reducing insurance premiums, and helping to improve investor and customer confidence. This pocket guide explains how to achieve certification to Cyber Essentials in a fast, effective and cost-effective manner."--

This book is intended for everyone in an organization who wishes to have a basic understanding of information security. Knowledge about information security is important to all employees. It makes no difference if you work in a profit- or non-profit organization because the risks that organizations face are similar for all organizations. It clearly explains the approaches that most organizations can

consider and implement which helps turn Information Security management into an approachable, effective and well-understood tool. It covers: The quality requirements an organization may have for information; The risks associated with these quality requirements; The countermeasures that are necessary to mitigate these risks; Ensuring business continuity in the event of a disaster; When and whether to report incidents outside the organization. The information security concepts in this revised edition are based on the ISO/IEC27001:2013 and ISO/IEC27002:2013 standards. But the text also refers to the other relevant international standards for information security. The text is structured as follows: Fundamental Principles of Security and Information security and Risk management. Architecture, processes and information, needed for basic understanding of what information security is about. Business Assets are discussed. Measures that can be taken to protect information assets. (Physical measures, technical measures and finally the organizational measures.) The primary objective of this book is to achieve awareness by students who want to apply for a basic information security examination. It is a source of information for the lecturer who wants to question information security students about their knowledge. Each chapter ends with a case study. In order to help with the understanding and coherence of each subject, these case studies include questions relating to the areas covered in the relevant chapters. Examples of recent events that illustrate the vulnerability of information are also included. This book is primarily developed as a study book for anyone who wants to pass the ISFS (Information Security Foundation) exam of EXIN. In an appendix an ISFS model exam is given, with feedback to all multiple choice options, so that it can be used as a training for the real ISFS exam.

Implementing internal audits as a risk management tool

ISO 22301:2019 and business continuity management – Understand how to plan, implement and enhance a business continuity management system (BCMS)

Linux for Beginners

The Ransomware Threat Landscape - Prepare for, recognise and survive ransomware attacks

Managing Work-life Balance

Selling Information Security to the Board

The EU Data Protection Code of Conduct for Cloud Service Providers provides guidance on how to implement the Code within your organisation, exploring the objectives of the Code and how compliance can be achieved with or without a pre-existing ISMS (information security management system) within the organisation.

Aligned with the latest iteration of the Standard – ISO 27001:2013 – this new edition of the original no-nonsense guide to successful ISO 27001 certification is ideal for anyone tackling ISO 27001 for the first time, and covers each element of the ISO 27001 project in simple, non-technical language

ISO 22301:2019 and business continuity management – Understand how to plan, implement and enhance a business continuity management system (BCMS) walks you through the requirements of ISO 22301, explaining what they mean and how your organisation can achieve compliance. It is an essential companion guide for those working in business continuity.

This book is a comprehensive cyber security implementation manual which gives practical guidance on the individual activities identified in the IT Governance Cyber Resilience

Framework (CRF) that can help organisations become cyber resilient and combat the cyber threat landscape. Start your cyber security journey and buy this book today!

IT Governance Implementing Frameworks and Standards for the Corporate Governance of IT  
ISO/IEC 38500: A pocket guide, second edition

The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks

ISO22301: 2019 - An introduction to a business continuity management system (BCMS)

A Pocket Guide

Penetration Testing Services Procurement Guide

Ransomware will cost companies around the world \$20 billion in 2021. Prepare for, recognise and survive ransomware attacks with this essential guide which sets out clearly how ransomware works, to help business leaders better understand the strategic risks, and explores measures that can be put in place to protect the organisation.

In this book, the following subjects are included: information security, the risk assessment and treatment processes (with practical examples), the information security controls. The text is based on the ISO/IEC 27001 standard and on the discussions held during the editing meetings, attended by the author. Appendixes include short presentations and check lists. CESARE GALLOTTI has been working since 1999 in the information security and IT process management fields and has been leading many projects for companies of various sizes and market sectors. He has been leading projects as consultant or auditor for the compliance with standards and regulations and has been designing and delivering ISO/IEC 27001, privacy and ITIL training courses. Some of his certifications are: Lead Auditor ISO/IEC 27001, Lead Auditor 9001, CISA, ITIL Expert and CBCI, CIPP/e. Since 2010, he has been Italian delegate for the the editing group for the ISO/IEC 27000 standard family. Web: [www.cesaregallotti.it](http://www.cesaregallotti.it).

If you want to learn how to use Linux, but don't know where to start read on. Knowing where to start when learning a new skill can be a challenge, especially when the topic seems so vast. There can be so much information available that you can't even decide where to start. Or worse, you start down the path of learning and quickly discover too many concepts, commands, and nuances that aren't explained. This kind of experience is frustrating and leaves you with more questions than answers. Linux for Beginners doesn't make any assumptions about your background or knowledge of Linux. You need no prior knowledge to benefit from this book. You will be guided step by step using a logical and systematic approach. As new concepts, commands, or jargon are encountered they are explained in plain language, making it easy for anyone to understand. Here is what you will learn by reading Linux for Beginners: How to get access to a Linux server if you don't already. What a Linux distribution is and which one to choose. What software is needed to connect to Linux from Mac and Windows computers. Screenshots included. What SSH is and how to use it, including creating and using SSH keys. The file system layout of Linux systems and where to find programs, configurations, and documentation. The basic Linux commands you'll use most often. Creating, renaming, moving, and deleting directories. Listing, reading, creating, editing, copying, and deleting files. Exactly how permissions work and how to decipher the most cryptic Linux permissions with ease. How to use the nano, vi, and emacs editors. Two methods to search for files and directories. How to compare the contents of files. What pipes are, why they are useful, and how to use them. How to compress files to save space and make transferring data easy. How and why to redirect

input and output from applications. How to customize your shell prompt. How to be efficient at the command line by using aliases, tab completion, and your shell history. How to schedule and automate jobs using cron. How to switch users and run processes as others. Where to go for even more in-depth coverage on each topic. What you learn in "Linux for Beginners" applies to any Linux environment including Ubuntu, Debian, Linux Mint, RedHat, Fedora, OpenSUSE, Slackware, and more. Scroll up, click the Buy Now With 1 Click button and get started learning Linux today!

This book helps you to bring the information security of your organization to the right level by using the ISO/IEC 27001 standard. An organization often provides services or products for years before the decision is taken to obtain an ISO/IEC 27001 certificate. Usually, a lot has already been done in the field of information security, but after reading the requirements of the standard, it seems that something more needs to be done: an 'information security management system' must be set up. A what? This handbook is intended to help small and medium-sized businesses establish, implement, maintain and continually improve an information security management system in accordance with the requirements of the international standard ISO/IEC 27001. At the same time, this handbook is also intended to provide information to auditors who must investigate whether an information security management system meets all requirements and has been effectively implemented. This handbook assumes that you ultimately want your information security management system to be certified by an accredited certification body. The moment you invite a certification body to perform a certification audit, you must be ready to demonstrate that your management system meets all the requirements of the Standard. In this book, you will find detailed explanations, more than a hundred examples, and sixty-one common pitfalls. It also contains information about the rules of the game and the course of a certification audit. Cees van der Wens (1965) studied industrial automation in the Netherlands. In his role as Lead Auditor, the author has carried out dozens of ISO/IEC 27001 certification audits at a wide range of organizations. As a consultant, he has also helped many organizations obtain the ISO/IEC 27001 certificate. The author feels very connected to the standard because of the social importance of information security and the power of a management system to get better results.

ISO27001/ISO27002: Guida tascabile

Information security: risk assessment, management systems, the ISO/IEC 27001 standard

Nine Steps to Success

ISO 27001 Handbook

NIST Cybersecurity Framework: A pocket guide

Milk Production and Processing

*In this book, users will get to know about the ISO 27001 and how to implement the required policies and procedures to acquire this certification. Real policies and procedures have been used as examples with step by step explanations about the process which includes implementing group polices in windows server. And lastly, the book also includes details about how to conduct an Internal Audit and proceed to the Final Audit Questa indispensabile guida tascabile fornisce un'utile panoramica di due importanti norme sulla sicurezza delle informazioni Così ricco di consigli*

*pratici per l'attuazione di un sistema di gestione della sicurezza delle informazioni che vi chiederete come avete potuto farne a meno prima d'ora. Acquista la tua copia oggi stesso.*

*The book covers various aspects of dairying and milk products such as dairy farm establishment, management, production and utilisation of various dairy products. Information has been included on various aspects of dairy farming starting with selection and purchase of dairy cattle, their care and management, with respect to housing, feeding, breeding and health care during various physiological states such as growth, pregnancy and lactation and during different seasons. Details of health care management along with common diseases have been covered with all information required for educated farmers and technicians working in these areas. Various means for consistent improvement of the stock has also been included. Production of clean milk, its procurement, processing and distribution has been covered with more emphasis on common processing technologies such as pasteurisation and sterilisation. Different forms of liquid milk available in the market has been described along with its standards and other specifications for the knowledge of common man and technicians. Manufacturing methods of milk products have been included with appropriate flow chart wherever required and various categories of milk products have been covered in detail under different chapters under milk products. This book has been prepared with emphasis on second year syllabus of Vocational higher secondary course on milk products and dairying and considering the lack of a suitable textbook for this subject. Hence the book is expected to fill the gap of a textbook for the above said and similar courses. Also the book may be accepted as a textbook/manual for educated farmers, other teaching and training programmes covering similar syllabus like that of dairy farm instructors and as a handbook for Veterinary Students and Dairy Extension Officers. With these introductory notes, we presume that the book will satisfy its readers' requirements and form a valuable textbook/reference book for all those concerned with dairy animal production and utilisation of their products ultimately benefiting the farming community.*

*Iso27001/Iso27002*