



Information Security Risk Management for ISO27001 / ISO27002

Alan Calder, Steve G Watkins

Download now

[Click here](#) if your download doesn't start automatically

Information Security Risk Management for ISO27001 / ISO27002

Alan Calder, Steve G Watkins

Information Security Risk Management for ISO27001 / ISO27002 Alan Calder, Steve G Watkins

Expert guidance on planning and implementing a risk assessment and protecting your business information. In the knowledge economy, organisations have to be able to protect their information assets. Information security management has, therefore, become a critical corporate discipline. The international code of practice for an information security management system (ISMS) is ISO27002. As the code of practice explains, information security management enables organisations to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities. ISMS requirements The requirements for an ISMS are specified in ISO27001. Under ISO27001, a risk assessment has to be carried out before any controls can be selected and implemented, making risk assessment the core competence of information security management. This book provides information security and risk management teams with detailed, practical guidance on how to develop and implement a risk assessment in line with the requirements of ISO27001. International best practice 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. Benefits to business include:

- * Stop the hacker. With a proper risk assessment, you can select appropriate controls to protect your organisation from hackers, worms and viruses, and other threats that could potentially cripple your business.
- * Achieve optimum ROI. Failure to invest sufficiently in information security controls is penny wise, pound foolish, since, for a relatively low outlay, it is possible to minimise your organisation's exposure to potentially devastating losses. However, having too many safeguards in place will make information security system expensive and bureaucratic; so without accurate planning your investment in information security controls can become unproductive. With the aid of a methodical risk assessment, you can select and implement your information security controls to ensure that your resources will be allocated to countering the major risks to your organisation. In this way, you will optimise your return on investment.
- * Build customer confidence. Protecting your information security is essential if you want to preserve the trust of your clients and to keep your business running smoothly from day to day. If you set up an ISMS in line with ISO27001, then, after an assessment, you can obtain certification. Buyers now tend to look for the assurance that can be derived from an accredited certification to ISO27001 and, increasingly, certification to ISO27001 is becoming a prerequisite in service specification procurement documents.
- * Comply with corporate governance codes. Information security is a vital aspect of enterprise risk management (ERM). An ERM framework is required by various corporate governance codes, such as the Turnbull Guidance contained within the UK's Combined Code on Corporate Governance, and the American Sarbanes-Oxley Act (SOX) of 2002, and standards such as ISO31000. As the authors point out, Just because a threat has not occurred yet does not mean that it never will.

 [Download Information Security Risk Management for ISO27001 ...pdf](#)

 [Read Online Information Security Risk Management for ISO2700 ...pdf](#)

Download and Read Free Online Information Security Risk Management for ISO27001 / ISO27002 Alan Calder, Steve G Watkins

From reader reviews:

Robin Millard:

The book Information Security Risk Management for ISO27001 / ISO27002 can give more knowledge and information about everything you want. So just why must we leave the best thing like a book Information Security Risk Management for ISO27001 / ISO27002? Wide variety you have a different opinion about e-book. But one aim this book can give many details for us. It is absolutely proper. Right now, try to closer together with your book. Knowledge or facts that you take for that, you may give for each other; you are able to share all of these. Book Information Security Risk Management for ISO27001 / ISO27002 has simple shape however you know: it has great and big function for you. You can appear the enormous world by available and read a reserve. So it is very wonderful.

Eddie Horton:

Information Security Risk Management for ISO27001 / ISO27002 can be one of your beginner books that are good idea. We recommend that straight away because this publication has good vocabulary that may increase your knowledge in vocabulary, easy to understand, bit entertaining but nonetheless delivering the information. The article writer giving his/her effort to put every word into delight arrangement in writing Information Security Risk Management for ISO27001 / ISO27002 however doesn't forget the main level, giving the reader the hottest and also based confirm resource facts that maybe you can be among it. This great information can easily drawn you into fresh stage of crucial pondering.

Pearl Norris:

That book can make you to feel relax. This kind of book Information Security Risk Management for ISO27001 / ISO27002 was colourful and of course has pictures around. As we know that book Information Security Risk Management for ISO27001 / ISO27002 has many kinds or genre. Start from kids until teenagers. For example Naruto or Detective Conan you can read and believe that you are the character on there. So , not at all of book usually are make you bored, any it offers up you feel happy, fun and chill out. Try to choose the best book for you personally and try to like reading which.

Janelle Coe:

Reserve is one of source of knowledge. We can add our information from it. Not only for students and also native or citizen have to have book to know the up-date information of year for you to year. As we know those guides have many advantages. Beside most of us add our knowledge, may also bring us to around the world. By book Information Security Risk Management for ISO27001 / ISO27002 we can get more advantage. Don't someone to be creative people? To become creative person must want to read a book. Only choose the best book that ideal with your aim. Don't possibly be doubt to change your life at this book Information Security Risk Management for ISO27001 / ISO27002. You can more pleasing than now.

**Download and Read Online Information Security Risk Management
for ISO27001 / ISO27002 Alan Calder, Steve G Watkins
#15BG4JXZ72U**

Read Information Security Risk Management for ISO27001 / ISO27002 by Alan Calder, Steve G Watkins for online ebook

Information Security Risk Management for ISO27001 / ISO27002 by Alan Calder, Steve G Watkins Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Information Security Risk Management for ISO27001 / ISO27002 by Alan Calder, Steve G Watkins books to read online.

Online Information Security Risk Management for ISO27001 / ISO27002 by Alan Calder, Steve G Watkins ebook PDF download

Information Security Risk Management for ISO27001 / ISO27002 by Alan Calder, Steve G Watkins Doc

Information Security Risk Management for ISO27001 / ISO27002 by Alan Calder, Steve G Watkins Mobipocket

Information Security Risk Management for ISO27001 / ISO27002 by Alan Calder, Steve G Watkins EPub