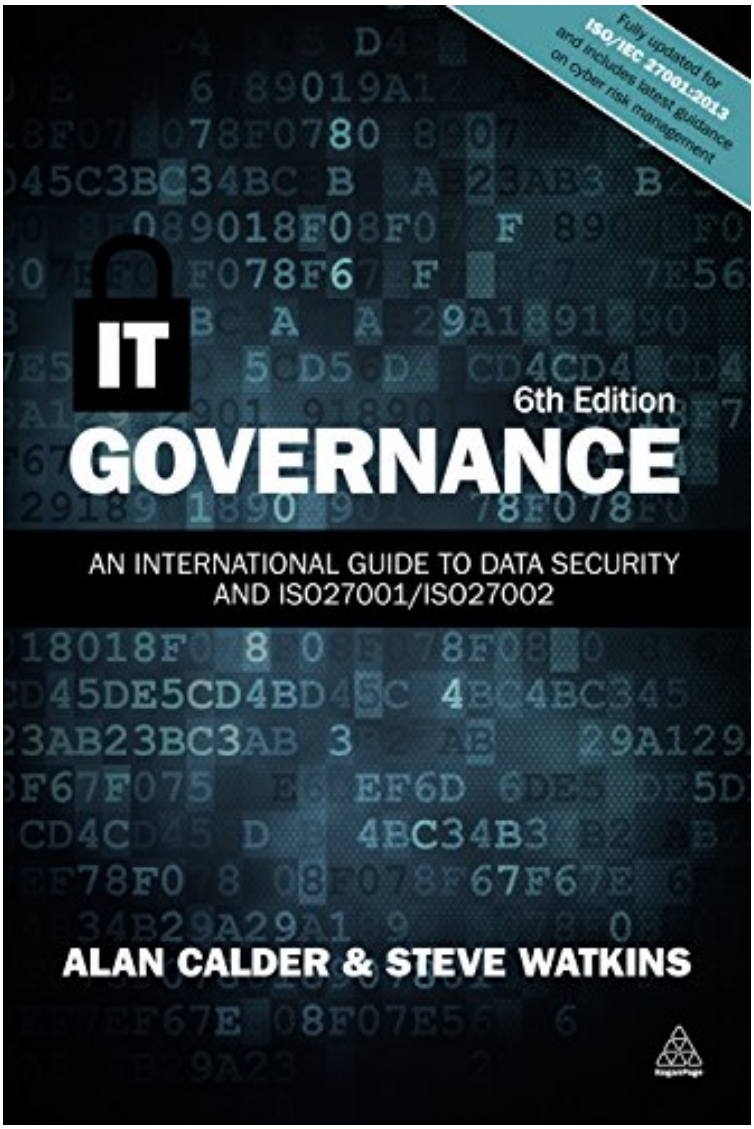
IT Governance: An International Guide to Data Security and ISO27001/ISO27002

Alan Calder, Steve Watkins
*ebooks | Download PDF | *ePub | DOC | audiobook*



#758881 in eBooks 2015-09-03 2015-09-03File Name: B014H56TQC | File size: 39.Mb

Alan Calder, Steve Watkins : IT Governance: An International Guide to Data Security and ISO27001/ISO27002 before purchasing it in order to gage whether or not it would be worth my time, and all praised IT Governance: An International Guide to Data Security and ISO27001/ISO27002:

9 of 9 people found the following review helpful. Comprehensive and accurate non-technical guide to information security standardsBy Aaron C. BrownThis is primarily a guide to the regulations and major standards for information security. It's a tweener book, not precise enough for legal and compliance professionals, not technical enough for IT

professionals, but putting a foot in each camp. I assume the intended audience is business executives with oversight responsibility for IT, who are not involved in day-to-day technical IT management. However, it could also be read for profit by an IT manager seeking to understand some of the strange requirements being imposed by people in suits who don't seem to do any actual work, or by a compliance professional who wants to understand some of the simpler technical implications of the legal rules without the brain damage of actually talking to geeks.The first issue I have with this book is the authors don't seem to know what it is. The book defines "IT Governance" as, "The framework for the leadership, organizational structures and business processes, standards and compliance to those standards, which ensures that the organization's information systems support and enable the achievement of its strategy and objectives." Problem one is the layering on of random consultant-speak buzzwords, which is unfortunately common in this book. Problem two is none of these topics are covered in this book, it's only about external requirements for information security. You could comply with all the rules that are covered by destroying your entire IT infrastructure, because you would then have total information security. No information, no possibility of harming or losing it.Problem three is the authors aren't even trying to make sense. "Governance" has to be a process, not a "framework". But okay, I can see a framework for organizational structures, businesses processes and standards; a template for storing the organization chart and IT rules. I wouldn't call it "IT governance," but at least it makes sense in isolation. But what is a framework for leadership? And people either comply with standards or not, there's no way to build a framework for compliance with standards. Finally, you can't have a "which" clause in a definition. If the authors mean "that" (a restrictive clause), then you get the silly result that if the IT systems don't work well, you don't have bad IT governance, you have no IT governance. This was not a definition written to communicate useful information to anyone, and it's defining the title of the book.A deeper problem is this is an old-fashioned view of IT that applies to fewer and fewer businesses. It asserts that business objectives and strategy are set outside IT, and the function of IT is to support and enable them. But how about businesses driven by IT, where the innovations come from IT and the job of the rest of the business is to monetize those ideas? Obviously that's going to be at least partly true in technology businesses, as well as information businesses like finance, but even in fields like retail, travel and entertainment, many of the largest and fastest growing companies are defined by their technology more than by how they produce actual goods and services. A modern view would put at least as much emphasis on ensuring IT innovation and keeping abreast (or ahead) of progress, as on bending IT to the will of the money guys.Once the authors forget about governance and start discussing information security, things get a little better. They do a pretty good job of laying out the major regulations and standards. It's not exciting stuff, but it's easier to read than the standards themselves, and it's compiled so you don't have to align overlapping parts of different documents. This is a real service. As far as I can tell, and I'm no expert, it's comprehensive and accurate.The biggest problem with the book is the authors fail to make a key distinction. There are things you do to get things right, like testing code, making frequent backups, segregation of duties, clear ownership, authority aligned with responsibility and training people. These will differ enormously in different organizations. There are places it makes sense to test things in Production, and places where that risks global themonuclear war. There are places where empowering individual creativity is critical to success, and places that never heard of individual creativity, and are happy about that. Then there are things you do to prove you tried to do things right, like audit trails, maker/checker, written policies and procedures and so on. These things are largely the same across organizations. They will differ in detail, but not a lot in general outline.Of course, you don't do these things independently. For one reason, it would be too much work and too confusing to do everything twice. For another, your compliance to regulatory and legal standards would seem superficial if you put your real trust in different standards. So the trick is usually to take what you do to get things right, and put it into the boxes demanded by auditors, lawyers and regulators. It's never a perfect fit, you have to do some overhead to make outsiders happy that doesn't improve your actual processes, but that's life.But this book lays down rules that mix standard requirements with good practice tips, and it never tells the reader which is which. There are very few actual references. So when they tell you to allow three login attempts before locking out a user (amusingly, right after they told you not to tell anyone how many login attempts are allowed, so I guess you should burn this book after reading it) you don't know if that's an ISO/IEC requirement, a law, a standard that has been tested in courts and seems to pass muster, or just what the authors think is a good number. This seems to me to be something that should vary depending on the application and the circumstances, but maybe I'm risking my certification if I allow two or four attempts.More generally, the book has a lot more prescriptions than rationales for those prescriptions. I trust that if you do everything the authors say, you're probably in decent compliance with most rules, but a lot of the stuff would be irritating, expensive or useless in many organizations, and there's no way to tell whether you can safely ignore it. Sometimes it gets ridiculous, like, "third parties should be required to comply with their contractual responsibilities." So you need to sign a contract, then post a rule that signers have to abide by the contract. Why not a rule that people have to obey the rule to comply with contracts? The attitude of the book seems to be do everything possible to avoid possible future criticism, which is no way to run an IT department.A minor gripe is a lot of the material seems dated. The section on mobile devices, for example, seems written for Blackberries and full-featured laptops; with the words "smart phone" added (and no mention of tablets or watches). WiFi is treated as if it's a promising technology found in some airport lounges, and that

may get popular. There is little mention of even the highest profile recent information security disasters, or the evolution of threats. I suspect this is a result of coming out with new editions too frequently for the authors to revise things thoroughly. While I accept the need for frequent new editions, it would make more sense to produce a small (and cheap) update booklet covering just the new stuff. Or (here's a bold idea!) put it in a Wiki!Another minor gripe is information is not always organized sensibly. The section on firewalls gives advice about selecting a vendor, which is all general stuff like finding a solid business with a track record that gives you confidence it will be around to support the product. I don't think you need stuff like that in an information security book, you could refer the reader to a vendor management book. But if you include it, it should be in an appendix, because it applies to pretty much any vendor of critical infrastructure support. Also, as noted above, it's advice to avoid criticism. If it were a universal rule, there would be no new companies. There are times to take a chance on a smart newcomer, especially in a critical and fast changing area where the big name suppliers may be more concerned with protecting their legacy business than coming up with the best new ideas.If you want a comprehensive and accurate non-technical guide to information security standards, this book delivers exactly that. I learned a lot from reading it. When the authors aren't spouting consultant-jargon, they have a clear style. The book has a lot of flaws, but I don't know of a better one for the purpose.1 of 1 people found the following review helpful. Useful overview of ways to control information security risksBy John GibbsFaced with the emergence and speed of growth in the information economy, organizations have an urgent need to adopt IT governance best practice, according to Alan Calder and Steve Watkins in this book. The authors define IT governance as lsquo;the framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that the organizationrsquo;s information systems support and enable the achievement of its strategies and objectivesrsquo;.There are so many different things that can go wrong with an organisationrsquo;s IT resources that it is hard to know where to start even identifying the possible risks, let alone working out how to get them under control. The old risks of data loss due to hardware failure and financial loss due to project failure still exist, but there are vast numbers of new risks including the risks of data theft or destruction by highly skilled malicious agents who are bent on finding ways to harm your organisation.Only large organisations will have the resources to go through the full ISO27001 certification process, but in its discussion of the various controls needed for certification, this book provides a very useful overview of the steps which an organisation can take to protect against a large range of information security risks.0 of 0 people found the following review helpful. ValidBy DarrenIngram_dot_comThis is a bit of a specialist book that focussed on data security issues and ISO27001/2, all under the heading of IT governance. Now in its sixth revision, this updated book still continues to provide timely, informative counsel to those who are looking to establish best practice guidelines in this challenging, changing area.Clearly this book cannot focus on legislation from every country in the world, yet it does look at many key international markets and provides advice on compliance within key information security responsibilities. This is not a practical guide to securing your server or network in that sense, yet it will give you sufficient advice to develop and operate a manageable policy that, in turn, will work through practical cases and structures to secure your systems and stored data. Capable advice about developing information security policies and underlying risk assessment procedures is given in a clear, unambiguous and overtly jargon-free manner. Even often overlooked areas such as human resources security and asset management are discussed.In many ways this is a book of doom, full of things yoursquo;d rather not happen and its advice will help you strategize and implement a delivered solution that will hopefully reduce or mitigate the risk. With IT there is never a true risk-free solution, but as much advanced planning and focussed on-going strategic operation as possible will be a wise investment. Then, should you suspect the worst to happen, you may be in a better position to respond and reduce the damage.As you may expect, this book is crammed full of information and thus the extensive, comprehensive index is welcomed. This is not a book for everyone, but for those who need this kind of information it will be an indispensible aid. Many others may get a passing benefit from a chapter or two and it could be one of those best-shared books within a company. You might want to get your own copy though, as it can become a regularly consulted companion.

Faced with constant and fast-evolving threats to information security and with a growing exposure to cyber risk, managers at all levels and in organizations of all sizes need a robust IT governance system. Now in its sixth edition, the bestselling IT Governance provides best-practice guidance for companies looking to protect and enhance their information security management systems and protect themselves against cyber threats. IT Governance has been fully updated to take account of current cyber security and advanced persistent threats and reflects the latest regulatory and technical developments, including the 2013 updates to ISO27001/ISO27002. Changes for this edition include:Full updates throughout in line with the revised ISO27001 standard and accompanying ISO27002 code of practice for information security controlsFull coverage of changes to data-related regulations in different jurisdictions and advice on complianceGuidance on the options for continual improvement models and control frameworks made possible by the new standardNew developments in cyber risk and mitigation practicesThe latest technological developments that affect IT governance and securityGuidance on the new information security risk assessment process and treatment requirementsIncluding coverage of key international markets including the UK, North America, the EU and Asia

Pacific, IT Governance is the definitive guide to implementing an effective information security management and governance system.

About the AuthorAlan Calder is a founder-director of IT Governance Ltd. He is also the author of Corporate Governance and International IT Governance (Kogan Page). Steve Watkins is an expert in the field of management system standards.nbsp; He has authored several books on the topic and provides training and consulting services in this area.