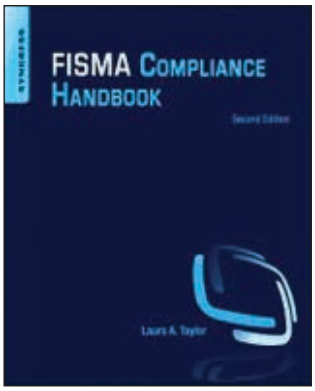
Reviewed by Ibe Etea, CISA, CRISC, CA, CFE, CIA, CRMA, a corporate governance, internal controls, fraud and enterprise risk assurance professional. Etea also serves as a member on the advisory council of the Association of Certified Fraud Examiners (ACFE).

FISMA Compliance Handbook

FISMA Compliance Handbook is a valuable reference guide to compliance requirements in the US. The US Federal Information Security Management Act (FISMA) applies to federal agencies and to all private companies that have contracts with US agencies, making the book a value-add for IT professionals globally.

Author Laura Taylor not only serves as chair of the FISMA Center Advisory Board, but she also founded the Certified FISMA Compliance Practitioner (CFCP) qualification program. In addition to explaining FISMA, Taylor also provides an outline of information systems (IS) requirements that can be applied by professionals who are developing IT systems. *FISMA Compliance Handbook* can also be used as a reference on how to implement statute-driven information systems' compliance reviews or audits. The book transcends the typical policy paperwork analysis to be an IS reference that can educate chief information officers (CIOs) and IS professionals in the public and private spheres.



By Laura Taylor

The book has 23 chapters, and the first 3 chapters cover various compliance methodologies. In the fourth chapter, the key roles of IS professionals, including the CIO, authorizing officials and assessor teams, are discussed, and the processes of FISMA compliance are outlined. The crux of setting up a FISMA compliance program is addressed in chapter 5, while chapters 6 to 16 cover other important parts of FISMA, such as system setup inventory, data sensitivity categorization, awareness training and privacy impact assessment, which is an important aspect of contemporary data management across all sectors.

The book contains a plethora of information about incident response, business impact analysis, and developing contingency and configuration management plans, all of which are relevant events for IS professionals. Full chapters are devoted to the Independent Assessor Audit Guide, developing the security assessment report and addressing FISMA findings: and the FISMA application for the cloud is also addressed in the book.

While this book is especially valuable for practitioners in US government agencies, the reach of FISMA into all private companies with government contracts adds to the book's value for a worldwide audience. With illustrations, templates, tables and appendices, the book is highly engaging and gives the reader a full overview of the requirements to prepare for, execute and document FISMA compliance projects.

EDITOR'S NOTE

FISMA Compliance Handbook is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, email b*ookstore@isaca.org* or telephone +1.847.660.5650.