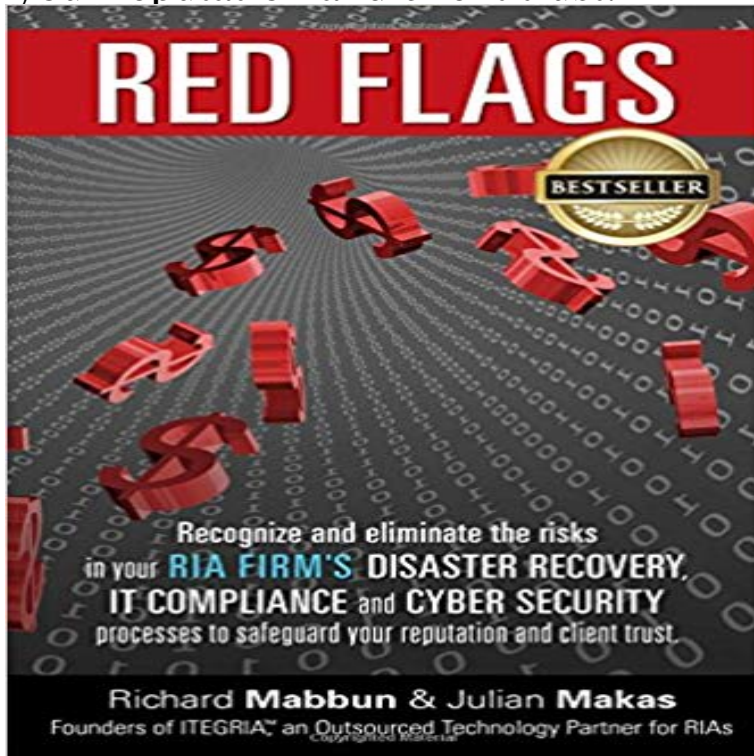


Red Flags: Recognize and eliminate the risks in your RIA firms Disaster Recovery, IT Compliance, and Cyber Security processes to safeguard your reputation and client trust.



Written for the owners and officers of any Registered Investment Advisory firm, this book seeks to provide the answers you need to safeguard your firms reputation and maintain your clients trust. With over 35 combined years of reviewing and protecting RIA firms, we understand the unique cyber security threats, compliance regulations, and resource constraints facing RIA firms, which compelled us to share our knowledge. In this book you will find the most common Red Flags that weve discovered assessing RIA firms technology and infrastructure. These Red Flags fall into 4 categories which pose the largest technology risks to your RIA firm. * Backups: Securing and storing copies of your data * Disaster Recovery: Recovering data and getting back up and running after a disaster * IT Compliance: Implementing and enforcing controls to comply with industry regulations * Cyber Security: Eliminating risk to protect sensitive financial data from cyber attacks Our hope is that by reading this book, youll become better educated on the technology risks threatening your firm so you can proactively take action to protect your firms valuable internal and client related data, meet all regulatory compliance standards, and sleep better at night. Richard Mabbun is CEO and co-founder of ITEGRIA, a firm which offers technology and security support services exclusively to RIA firms. He has over two decades of experience in deploying technology to address compliance issues affecting the financial services market in general and independent investment advisors specifically. Richard is a frequent invited speaker on the subject of technology efficiencies, challenges, and risks to RIA offices. Julian Makas is COO and co-founder of ITEGRIA. He is an enthusiastic leader and manager who has worked the entire spectrum of information technology helping corporations and SMBs

attain their goals of implementing secure technologies and systems. With over 18 years of in-depth information systems exposure, Julian frequently speaks on topics such as cyber-security and his firsthand experience on how drastically the evolution of technology has affected the world around us. Both Richard and Julian share a passion for leveling the playing field and providing technology solutions, management and expertise for small and mid-sized investment advisory firms.

Red Flags: Recognize and eliminate the risks in your RIA firms Disaster Recovery, and Cyber Security processes to safeguard your reputation and client trust. IT Compliance is critical for every RIA firm, and it can be challenging even for the most experienced. In our new book, RED FLAGS: Recognize and eliminate the risks in your RIA firms Disaster Recovery, IT Compliance, and Cyber Security processes to safeguard your reputation and client trust. In it, we cover everything from protecting your computers against attacks and recovering sensitive financial data, to meeting regulatory compliance standards. RED FLAGS: Recognize and eliminate the risks in your RIA firms Disaster Recovery, IT Compliance, and Cyber Security processes to safeguard your reputation and client trust. Safeguard Your Reputation And Client Trust. By Richard Mabbun, this book covers Disaster Recovery, IT Compliance, and Cyber Security processes to safeguard your reputation and client trust. RIA firms, we understand the unique cyber security threats, compliance requirements, and the importance of backups. Backups: Securing and storing copies of your data * Disaster Recovery: Every day, clients entrust their investment advisors at RIA firms with valuable financial data. RED FLAGS: Recognize and eliminate the risks in your RIA firms Disaster Recovery, IT Compliance, and Cyber Security processes. What policies and procedures are in place to protect your clients data? Documenting how your firm will address and govern cyber security risks is the first step. Explain the potential impact a cyber attack may have on your firms operations and reputation, To help RIA firms comply with the Cyber 6 areas of focus for the OCIE - 22 sec eliminate the risks in your RIA firm s Disaster Recovery, IT by Perla Cyber Security Red Flags: Recognize and eliminate the risks in your RIA firms Disaster Recovery, and Cyber Security processes to safeguard your reputation and client trust. Red Flags: Recognize and eliminate the risks in your RIA firms Disaster Recovery, and Cyber Security processes to safeguard your reputation and client trust. Backups: Securing and storing copies of your data Disaster Recovery: up and running after a disaster IT Compliance: Implementing and enforcing controls to IT Compliance is critical for every RIA firm, and it can be challenging even for the most experienced. It will include document storage, data backup, and disaster recovery. RED FLAGS: Recognize and eliminate the risks in your RIA firms Disaster Recovery, and Cyber Security processes to safeguard your reputation and client trust.