EBOOK

THE CYBER SECURITY AND COMPLIANCE CHECKLIST FOR RIAS

An easy-to-use, compliance readiness tool for investment advisors

Introduction

Give yourself a cyber security and compliance check up

Checklists are powerful tools. They let you quickly assess where you stack up on a project or topic. Whether it is a shopping list, a packing list for an upcoming trip, or an assessment of your cyber security readiness as an organization, a checklist will help you understand if you are halfway there, nearly finished, or just getting started.

Use this cyber security and compliance checklist to assess whether your firm is well on your way to a solid cyber security foundation or are just getting started. We encourage you to use this checklist in concert with our whitepaper, *7 Cyber Security and Compliance Foundations for RIAs*, where you find a deeper discussion on each item on the checklist below.

Lastly, the itSynergy team is standing by to help you on any aspect of your journey. Don't hesitate to give us a call. We are ready to help.

SEC Requirements and Standards

It is vital for RIAs to be fully aware of the importance of cyber security as a key component of the overall compliance framework for investment advisors. The SEC publishes several key guidance documents, along with frequent news and best practice documents on the SEC website. Every RIA firm should research and select a cyber security technology standard for your organization.

- [ ] **Download:** Cybersecurity Guidance for Investment Advisers and Registered Investment Companies, SEC *[http://www.sec.gov/investment/im-guidance-2015-02.pdf]*
- [ ] **Download:** Guidance on Business Continuity Planning for Registered Investment Companies, SEC *[http://www.sec.gov/investment/im-guidance-2016-04.pdf]*
- [ ] **Keep up to date:** Regularly visit the SEC website for cyber security updates *[https://www.sec.gov/spotlight/cybersecurity]*
- [ ] **Research:** Study the different cyber security standards available to investment advisors, including COBIT 2019, ISO/IEC 27032:2012, CIS, or NIST CSF
- [ ] **Select a standard:** Choose one standard to benchmark your organization and assess your current cyber risks

Top Tip

itSynergy recommends the NIST Cyber Security Framework (NIST CSF). The NIST CSF is referenced by the SEC's Division of Examinations (formerly OCIE) as an example of an acceptable standard for all of their cyber security compliance audits. The Division of Examinations (the Division) specifically mentions the NIST CSF in the footnotes of their cybersecurity guidelines. Therefore, when an inspector from the Division conducts an investigation, you are well positioned if you align with the NIST CSF standard.

Conduct a Risk Assessment

A key part of risk management is knowing your degree of alignment with your preferred cyber security standard. It is vital to assess where you stand and to identify and measure the known risks and gaps. Next, you should quantify the probability and impact should a security incident occur.

- [ ] **Insource vs. outsource:** leverage highly trained, internal cyber security staff or bring in an outside cyber security consultant or service provider to conduct your risk assessment
- [ ] **Assess:** measure your firm's alignment with your preferred cyber security standard and identify gaps
- [ ] **Measure:** quantify the probability and impact of certain types of cyber security risks
- [ ] **Analyze:** prioritize the risks that should be mitigated in the short term, based on an assigned exposure score (probability x impact) and available resources (time, money, and talent)
- [ ] **Plan:** once you have a mitigation plan, upgrades to information technology, infrastructure, policies, and procedures should be made deliberately and in a timely fashion

Ensure you document the entire process including who was involved, when the initial assessment was done, any workpapers or notes on decisions made. Repeat this at least annually and be prepared to show the Division inspector this documentation.

Top Tip

It is wise to consult with an outside third-party consultant or service provider to conduct your cyber security risk assessment. Trained professionals from an outside service provider will have the benefit of having conducted dozens of similar assessments on other organizations. This accumulated experience and expertise is essential for RIA firms that are looking to begin their compliance journey on the right foot.

Strategic IT Planning

Sound cyber security and compliance is a journey, not a destination. No matter how advanced the firm, it is rare to have all of your bases covered on day one. Every good initial risk assessment will surface gaps and additional risks to an organization. Moreover, the external cyber security landscape is evolving daily, with new and different attacks and vulnerabilities. Therefore, forward progress and strategic planning are key in moving an organization ahead on its journey.

- [ ] **Budget:** solid cyber security requires sustained investment in technology, infrastructure, software, services and manpower; annual budgets should be developed to map out phases of investment over months, quarters, and years
- [ ] **Upgrade:** your firm should adequately staff your IT team with the people and resources needed to do the work and perform ongoing cyber security upgrades; outside service providers can turbo-charge your internal team's efforts and/or deliver specialized expertise in the cyber security arena
- [ ] **Invest:** a fully compliant cyber security posture requires continuous investment and ongoing proactive management by IT staff or your IT service provider
- [ ] **Refresh:** your cyber security assessment should be revisited and revised on an annual basis, at a minimum
- [ ] **Document:** thorough documentation and change management best practices should be used to create an ongoing log of all assessments, personnel involved, mitigation decisions, and analysis; showing progress and thorough documentation is a must in the context of an audit by the Division.

Top Tip

Cyber security and compliance is an ongoing journey and discipline, but there is no fixed destination or end point. For instance, a good cyber security risk assessment should be revisited on an annual basis and incorporated into an IT strategic planning process. The key reality is that risk management is an ongoing and dynamic process, which needs continual monitoring and engagement by highly trained cyber security professionals, along with sustained engagement of executive leadership of a company. Being able to demonstrate a strong commitment to compliance efforts from executive leadership is key during audits by the Division.

Cyber Security Training and Accountability

It cannot be repeated enough: people are the weakest link in cyber security. You can have the most expensive firewall, the most robust intrusion detection system, and the most thorough authentication process in place, and people's bad habits and sloppy behaviors can nevertheless lead to massive security incidents. Therefore, we need to build a "human firewall," by training and developing people at all levels in an organization.

- [ ] **Cyber Security Awareness Training:** broad based awareness training should be deployed to all employees in the firm, leveraging phishing simulations, engaging content, gamification, and automated deployment for consistent execution; the goal is to raise the bar across the organization and develop a security-minded culture
- [ ] **Executive Training:** specialized training should be employed for executives and leaders who have access to sensitive information, such as trade secrets, intellectual property, and employee and customer information, along with financial resources, such as access to banking, wire transfers, accounts payable, and check disbursements
- [ ] **IT Training:** advanced and ongoing training for IT and cyber security staff is key to upskill and develop the security practitioners in the organization, especially since the cyber security landscape is rapidly evolving
- [ ] **Accountability:** develop and document an Accountability Chart, which details responsibilities for various cyber security and IT systems and processes; think of this like an organization chart for IT systems and processes

Top Tip

Cyber security training should leverage principles of adult learning, including hands-on and practical exercises for deeper skills development, along with frequent quizzes, tests and knowledge validations. Adult learners will want to understand the practical value of the training, especially for career advancement. And never underestimate the value of gamifying the process, to engage peoples' competitive spirit.

Assume Breach

We live and work in a fluid and fast changing work environment. New cyber security threats and criminal tactics are evolving all the time. Meanwhile, organizations are becoming more highly distributed, increasing the range of systems, devices, and locations that can fall prey to cyber criminals. Therefore, it makes sense to assume that a security breach of some sort is inevitable. It is a case of when, not if.

- [ ] **Protect:** invest in cyber security technology, best practices, and employee training to reduce the overall risk of a cyber security incident; table stake protections include multi-factor authentication, next-gen anti-virus and endpoint protection, security patching, remote monitoring, and management, and security awareness training
- [ ] **Detect:** leverage intrusion detection systems, security incident and event management (SIEM), and next-gen security technologies, such as those that detect not just known threats but the anomalous behaviors that may indicate internal and external threat actors
- [ ] **Respond:** implement data leak prevention (DLP) technology to prevent mass data exfiltration and 24x7 security operations center (SOC) staffing (either internal or outsourced) for rapid response and mitigation
- [ ] **Recover:** implement robust backup and disaster recovery capabilities, to protect data wherever it resides and be ready to rapidly recover data, systems, and operations after a security incident

Top Tip

Defense in depth should be a guiding principle with fortifying your cyber security defenses. No one layer of protection, technology, or tool will provide universal protection. On the contrary, each layer of defense should complement the others, while deepening the overall level of protection. Importantly, with today's highly distributed organizations and work styles, we are not defending the perimeter of the organization with defense in depth, but rather the people, data, privacy, financial resources and operational integrity of an organization.

Conclusion and Getting Started

At itSynergy, we specialize in helping RIAs develop a culture of risk management and compliance, through prudent investments in cyber security. We invite interested firms to get to know us by inviting us to conduct a risk assessment for your firm. As we have shown throughout this ebook, itSynergy's rigorous approach will help you identify and manage your risks and start down the path of building a solid cyber security and compliance foundation.

About itSynergy

itSynergy specializes in helping registered investment advisers grow profitable businesses. itSynergy helps our clients tame their information technology, so they can securely and efficiently focus on their core business. Serving clients throughout the Phoenix and Denver metro areas, itSynergy delivers compliance, cyber security, and managed IT services to investment advisory firms. The company is led by president and founder Michael Cocanower. Mr. Cocanower has over 25 years of experience in the IT field. Mr. Cocanower has been recognized as a Microsoft® Certified Professional and Microsoft® Most Valuable Professional as well as a Certified Ethical Hacker. Mr. Cocanower is also an Investment Adviser Certified Compliance Professional® (IACCP).

www.itsynergy.com
(602) 297–2400

PEOPLE INNOVATION RESULTS
itSynergy®

www.itsynergy.com