

Best Practices

- **Steven Weiss**, General Counsel/CCO, Roosevelt Investment Group, New York
- **Brian Renelt**, Deputy CCO, Galliard Capital Management, Minneapolis
- **Aaron De Angelis**, CCO, Spring Mountain Capital, New York



Preparing for Form CRS

- **What Should Firms Do to Get Ready?**

A photograph of Independence Hall in Philadelphia, a large red brick building with a prominent clock tower and a white portico. The building is illuminated at dusk, with warm lights glowing from the windows and the clock tower. The sky is a deep blue, and some trees are visible in the foreground.

Conflicts Inventory

- **Create A Conflict Of Interest Inventory Spreadsheet**
- **Send Out, On Annual Basis, A Firmwide Attestation For Employees To Detail Their Current Activities That May Be Considered Conflicts Of Interest**
- **Update The Conflict Of Interest Inventory Spreadsheet**
- **Maintain The Current And Past Conflict Of Interest Inventory Spreadsheets**

A photograph of Independence Hall in Philadelphia, a large red brick building with a prominent clock tower and a white dome. The building is illuminated from within, and the sky is a deep blue. The image is partially obscured by a white circular glow on the right side.

Conflicts Inventory

- **Compliance Needs To Speak To Staff Through The Company To Assess Where Conflicts May Lie**
- **Map potential conflicts to P&Ps**
- **Where are conflicts disclosed?**
- **Tie conflicts to controls**

A photograph of Independence Hall in Philadelphia, a large red brick building with a prominent clock tower and a white dome, illuminated at dusk. The building is set against a clear blue sky with some bare tree branches visible in the foreground.

Exam Prep

Receive The SEC Request Letter

- **CCO Should Notify Appropriate Firm Personnel That The SEC Is Coming To Do An Examination**
- **Firm Has To Respond To The Request Letter In A Timely Manner**
- **Be Sure You Get Clarification On Any Requests That You Don't Understand At The Beginning Of The Examination**
- **Bring Together Firm Personnel Within Or Outside Your Firm To Collect The Required Material**
- **Senior Management Should Have A General Knowledge Of The Compliance Program**
- **Firm Business Units Should Be Sufficiently Aware Of The P&ps Applicable To Their Areas**
- **Senior Management Should Effectively Communicate The Firm's "Tone At The Top" And/Or "Culture Of Compliance"**
- **Compliance Should Review And Stay Current On SEC Risk Alerts, Regulatory Issues, SEC Focus Areas And Exam Priorities Issued By The SEC Examination Staff**
- **Firm's Risk Inventory/Assessment Should Be Current For The Year**
- **Know Your Compliance Manual Inside And Out**
- **Contact The Lead SEC Examiner And Maintain An Open Dialogue At The Start Of The Examination**
- **Consider FOIA Treatment**
- **Involve Outside Counsel And/Or Compliance Consultants (If Necessary)**
- **Make And Maintain A Duplicate Copy Of All Responses Provided**



Exam Prep

During The Examination

- **Prepare A PPT Presentation Detailing The Firm Its Operations And Employees**
- **Appearances Matter**
- **Establish Point Of Contact**
- **Maintain An Open Dialogue With Examiners**
- **Expect Additional Requests And Maintain Log Or Copies Of All Additional Requests**
- **Prepare To Be Interviewed By The Examiners (CCO Should Be Present During All Interviews)**
- **Remedy Issues As They Are Identified Before Exam Completion If Possible**
- **Keep An Open Mind To Best Practices And Enhancements Recommended By The Examiners**
- **Request An Exit Interview And Be Proactive To Any Comments**

After The Examination

- **Continue To Be Responsive To Any Additional Examination Requests**
- **Keep Exam Team Updated On Any Corrections Or Enhancements**
- **Possible Outcomes: No Further Action Letter, Deficiency Letter Or Enforcement Referral**



Exam Prep

- **Day One Presentation**
- **Prep Individuals For Interviews**
- **Mock Exam**



How to Use OCIE's Exam Priorities' List

- **Work Ocie's Priorities List Into Your Risk Matrix And You Annual Compliance Program/Budget**
- **Create Your Own Internal Mock Exam Using The OCIE List**
- **Conduct The Exam And Document**
- **Do The Same With OCIE Risk Alerts**
- **Keep Compliance Committee Informed**



How to Document Your Compliance Work

- **Compliance System Solution**
- **Compliance Program Annual Plan/Budget**
- **Risk Matrix**
- **Annual Review**
- **Testing**
- **Establish a Compliance Committee with Documentation And Minutes**
- **Maintain Copies Of Any Third-Party Audits Or Internal Audits**

A photograph of Independence Hall in Philadelphia, a large red brick building with a prominent clock tower and a white portico. The building is set against a clear blue sky with some bare tree branches in the foreground. The image is partially obscured by a white circular glow effect.

Cybersecurity Training

- **Employee Awareness and Responsiveness is Critical to Maintaining a Successful Information Security Program. Toward that End, IT Should Conduct Mandatory Cybersecurity Training for All Firm Employees on at Least an Annual Basis. The Adviser Needs to Maintain Documentation of the Cybersecurity Training Conducted, Which May Include The Following:**
 - **Dates Of Such Training;**
 - **Nature Of The Topic(s) Discussed (E.G., Phishing, Passwords, Mobile Devices, Etc.);**
 - **Slide Deck, Handouts, Or Other Supporting Materials; And**
 - **Attestations By Employees Acknowledging Their Attendance.**

Incident Response Planning

- **Staff Survey**
- **Adviser Needs To Define Incident Management And Response As The Capability To Effectively Manage Disruptive And Potentially Disruptive Cybersecurity Events (“Incidents”) Through A Defined, Consistent, And Repeatable Process Designed To Minimize Impact To The Firm And Its Clients.**
- **Disruptive Cybersecurity Incidents Can Take Many Forms, Including But Not Limited To Distributed Denial Of Service (DDoS) Attacks; Malware, Ransomware, And Other Malicious Code, Whether Launched Via Phishing Attacks Or Through Other Means; Unauthorized Access To The Firm’s Premises, Systems, Applications, Network, Or Data; Unavailability Of Critical Systems; Or The Loss Or Theft Of A Device, Machine, Hard Drive, Thumb Drive, Or Portable Media. A Non-exhaustive List Of Incident Types Are As Follows: Brute Force Password Attack; Cross Site Scripting (XSS); Data Loss; Denial Of Service (DOS); Distributed Denial Of Service (DDoS); Flooding; Malware; Phishing; Ransomware; Malware; Social Engineering; Trojan Horse; Virus Etc.)**

Adopt Policies & Procedures

- **Rule 206(4)-7 Under The Advisers Act Requires Each Investment Adviser To Adopt And Implement Written Policies And Procedures Reasonably Designed To Prevent The Adviser From Violating The Advisers Act. Rule 204-2(g)(3) Requires That For Books And Records Maintained Electronically, The Adviser’s Procedures Must Be Designed:**
 - To Reasonably Safeguard The Records From Loss, Alteration, Or Destruction;**
 - To Limit Access To The Records To Properly Authorized Personnel; And**
 - To Reasonably Ensure That Any Reproduction Of A Non-electronic Original Record On Electronic Storage Media Is Complete, True, And Legible When Retrieved.**

Establish A Risk Committee

- **The Risk Committee Will Be Responsible For Overseeing The Implementation And Documentation Of The Adviser’s Incident Management And Response Program, And For Updating The Incident Management And Response Program As Necessary.**

Incident Response Planning

Establish An Incident Management Team

- **The Incident Management Team (“Team”) should Be Prepared To Address Potential Incidents As They Occur.**
- **The Team Should Consist Of Standing Members.**
- **Depending Upon The Nature Of A Specific Incident, Additional Staff And Third Parties May Be Called By The Team To Join Them From Time To Time To Assist. The Personnel And Department Participation On The Team May Be Added To Or Reduced Based Upon The Priority And Scope Of Any Given Incident As Determined By The Team.**
- **In Most Advisory Firms The Chief Compliance Officer Is Designated As The Team Lead. The Team Lead Is Responsible For Invoking The Incident Management Team Upon Becoming Aware Or Notified Of A Potential Incident. In The Absence Or Unavailability Of The Team Lead, A Secondary Team Lead Should Be Named And Assume The Duties Of The Team Lead. In Addition, The Team Lead Should Be Responsible For Debriefing The Team On Incidents And For Determining, In Coordination With The Team, Whether A Reported Incident Requires Escalation Or A Formal Response. The Team Lead Is Responsible For Debriefing Other Members Of Senior Management Of The Firm On Incidents As Applicable.**

Create An Incident Reporting Form (on your app)

Risk Assessment

- **Tailored To Your Firm**
- **Include Senior Leadership And Smes In The Process**
- **If You Identify A Risk, Be Sure You Address It And Test It**

A photograph of Independence Hall in Philadelphia, a large red brick building with a prominent clock tower and a white dome. The building is illuminated at dusk, with warm lights from the windows and the clock tower. The sky is a deep blue, and some trees are visible in the foreground.

Risk Assessment

Aaron

- **Initial Assessment: Identify And Take An Inventory Of The Problems Or Risks To Which Clients Of An Adviser Or Shareholders Of A Fund Are Exposed As A Result Of Factors Such As:**
 - **Business And Investment Activities,**
 - **Service Providers (“SP”) Used,**
 - **Affiliates/Partners Of The Adviser, And**
 - **Regulations And Regulators.**
- **Periodic Assessment: Ensure Risk Identification And Control Processes Are Effective Through Periodic Assessment.**
- **To Implement An Effective Risk Identification Process, It Is Useful To Work In Context Of The Major Activities Of An Investment Advisory Firm Such As:**
 - **Portfolio Management And Trade Allocations,**
 - **Brokerage Arrangements & Execution Of Orders,**
 - **Personal And Proprietary Trading,**
 - **Valuation Of Clients’ Assets,**
 - **Safety Of Clients’ Assets, And**
 - **Information Creation, Compilation, Retention, Protection And Reporting**

19TH ANNUAL

IA Compliance
Master Emerging Challenges

A photograph of Independence Hall in Philadelphia, Pennsylvania, taken at dusk. The building is illuminated from within, and the sky is a deep blue. The clock tower is prominent, with a clock face visible. The building is surrounded by trees and a fence in the foreground.

Annual Review/Testing

- **Compliance System Solution**
- **Stagger Testing for the Year**
- **Dynamic Testing – Find New Ways To Test**



Annual Review/Testing

- **Perform Daily, Weekly, Quarterly Testing Which You Can Roll Up Into Your Annual Review**
- **Complete An Annual Risk Matrix (See Attached) For The Firm, Which Can Be Used As A Testing Guide/Budget For The Year, Which Can Also Be Rolled Up As Part Of The Firm's Annual Review**
- **Identify Compliance Violations Or Weaknesses And Document How The Issue(s) Was Found, Addressed And Resolved**
- **When Violations Or Weaknesses Are Identified, An Action Plan Needs To Be Developed To Resolve The Issues & Mitigate Future Issues, Promote Proactive Solutions, Not Just Sanctions, Set Reasonable Timeframes For Implementing Procedures, And Most Importantly Get Buy-in And Support From Internal Staff And Senior Management**
- **The Best Way To Avoid An Issue When Memorializing Your Annual Review Issues Is To Resolve The Issues Uncovered In A Timely Manner Even If Not Complete It Is Important To Show That Mitigation Is In Process And Will Be Completed In A Timely Manner**

Email Reviews

- **Do A Random Email Searches On Either A Weekly, Monthly Or Quarterly Basis (Annual Cycle) For Random Firm Employees**
- **Do A Random Email Search For The Riskier Employees (Client Services, Portfolio Management, Trading, Research And Performance Reporting**
- **Do A Random Email Search For Email Service Provider Extensions (Gmail.Com, Aol.Com, Yahoo.Com, Comcast.Com And Verizon.Net Etc.) To Ensure No Firm Employees Are Sending Firm Related Business Emails To Their Personal Accounts**
- **Maintain A List Of Key Words And Phrases To Use To Random Search For Firm Wide Employee Emails. (“Guaranteed Performance With No Losses” “Guaranteed” “Superior Performance” Etc.)**

19TH ANNUAL

IA Compliance
Master Emerging Challenges

Best Practices

- **Steven Weiss, General Counsel/CCO, Roosevelt Investment Group, New York**
- **Brian Renelt, Deputy CCO, Galliard Capital Management, Minneapolis**
- **Aaron De Angelis, CCO, Spring Mountain Capital, New York**