



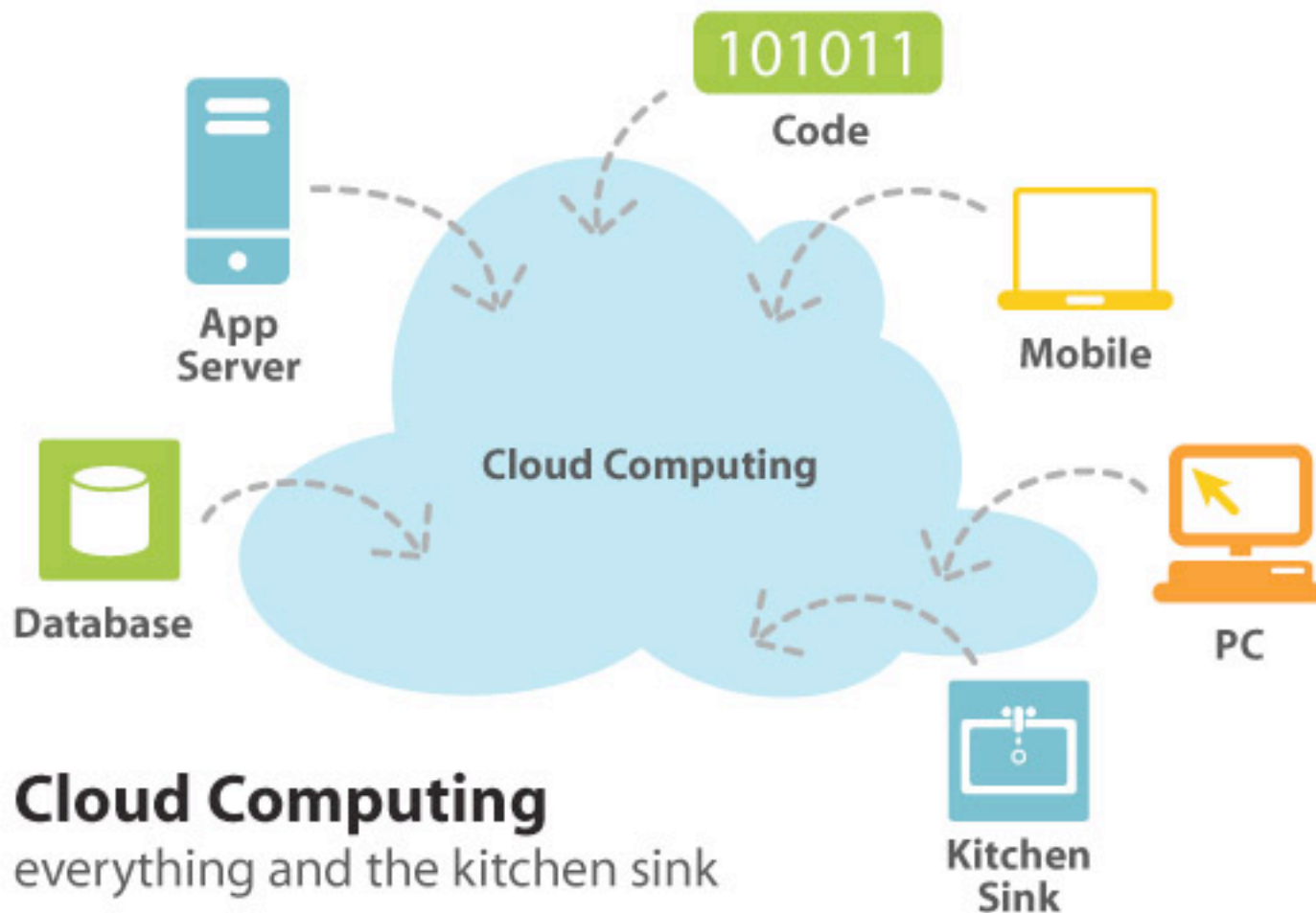
Understanding and Conquering Cloud-based Security and Compliance Issues



Today's Agenda

- ▶ Regulatory Framework – RIAs
- ▶ Why consider cloud systems?
- ▶ Data Protection
- ▶ Initial Due Diligence
- ▶ Ongoing Testing and Due Diligence
- ▶ Regulatory Exams
- ▶ Compliance Benefits in the Cloud
- ▶ Common Mistakes
- ▶ Questions

What is Cloud Computing to you?



So how do you protect your firm and your clients?

Regulatory Framework - RIAs

Registered Investment Advisors are required pursuant to IA Rule 206(4)-7 to design and implement a compliance program.

And YES, the CCO has responsibility for Technology!!!

- ▶ Rule 206(4)-7 -- Compliance Procedures and Practices
- ▶ Rule 204-2 -- Books and Records
- ▶ Rule 206(4)-2 – Custody Rules
- ▶ Regulation S-P
- ▶ Review adequacy at least annually



Regulatory Framework – cont.

Advisers Act discusses the principles and expectations, but does not impose standards on how to meet them.

- ▶ Often more flexibility than Exchange and FINRA rules
- ▶ Email and data retention. No WORM requirement
- ▶ Due diligence requirements
- ▶ Privacy laws – more than Regulation S-P
 - Example – MA Privacy Law – specific rules if you hold private data

Regulatory Framework – Summary

- ▶ All firms must have Policies and Procedures that address Privacy, Data Security, Use of Technology, Escalation of Issues, etc.
- ▶ All financial services firms must have a Business Continuity Plan. Cloud systems can make this easier.
- ▶ All Compliance Programs must be tested at least annually
- ▶ Systems and controls must be adequately designed to protect Client interests and private information
- ▶ Firms must conduct both initial and ongoing testing and due diligence of their technology and service providers.

So why even consider cloud systems?

- ▶ Ease of systems and data access
- ▶ Lower IT costs
- ▶ Integration between systems
- ▶ 24 x 7 Access
- ▶ Ability to supervise remote teams
- ▶ Share data seamlessly with clients
- ▶ Enhanced Business Continuity
- ▶ Stronger data redundancy
- ▶ ...the list grows daily!



Regulations are still lagging innovation, but cloud systems can be more sound and secure than in-house systems – with the right controls!

Data Protection

Protecting data goes far beyond passwords...

- ▶ All critical data in single location is a risk – Hackers only have to get lucky once!
- ▶ Implementation of access controls with roles/privileges.
- ▶ Complex password requirements and expiration policy.
- ▶ What is an API? Yes compliance folks, you need to know.

Data Protection – cont.

- ▶ Vendor privacy and data policies? Who's the vendor to the vendor? **You need to do your due diligence.**
- ▶ Implementation of strong authentication and passing on vendors with loose controls.
- ▶ Vendor viability – don't bet it all on a vendor that might no be there in month!
- ▶ Data location – do you know where your data resides? Is it even in the U.S.?

Initial Due Diligence

- ▶ Develop a requirements matrix
 - End user needs
 - Technology integration and management
 - Compliance oversight
- ▶ Understand the data security model
- ▶ Location of data center(s)
- ▶ Redundancy model
- ▶ Assess before you buy
- ▶ Talk to existing users of the provider (not just the salesperson's referrals)
- ▶ Financial viability of Providers
- ▶ Customer service model. Are they open when you are open?

Ongoing Testing and Due Diligence

- ▶ Vendor's attitude towards testing
- ▶ SAS-70?
- ▶ At least Annually. Pick a time of year that is best for your firm.
- ▶ Perform a “*real*” test.
 - Data security
 - Business continuity
 - Data retention
 - Compliance and IT Staff TOGETHER
 - Document gaps, consider remediation alternatives
- ▶ Output = Assessment report with gaps and enhancement recommendations.

Ongoing Testing and Due Diligence – cont.

What do we test?

- ▶ Inventory all systems and integrations. Are they reflected in your BCP Plan and IT Policies?
- ▶ Review the vendor's controls and testing performed on their end (i.e., SAS-70). Any security breaches? What is their BCP Plan?
- ▶ Data retention – can you find a specific client record from last week, last month or 3 years ago on random date?
- ▶ Data security – ask for the API and port logs. Where is your data going? Any abnormalities on time of day?
- ▶ User access. Which users are embracing the cloud systems. Any with low use? Check their laptops for local files.

Regulatory Exams

What to expect...

- ▶ Many questions! This is still new territory for regulators
- ▶ Review of policies and procedures – use of the Cloud
- ▶ Review of Due Diligence Plan and Testing
- ▶ Sample Testing of Books and Records
- ▶ Review of your BCP Plan. Can you really do everything from everywhere?
- ▶ Data security and privacy
- ▶ Review of the changes and evolution of the Cloud Policy and Records management

The Compliance Benefits in the Cloud

There are some risks, but benefits may outweigh them..

- ▶ Remove geography from books and records storage
- ▶ Supervise remote personnel and offices
- ▶ Monitor who is using which systems and when
- ▶ Control access to sensitive data
- ▶ Reduce input error through re-keying of data
- ▶ Reduce need to send private information via email
- ▶ Audit trails and redundancy models

Top 10 Common Mistakes

Learn from others. Don't make these common mistakes.

- ▶ Purchased systems based on marketing and reputation
- ▶ Not integrating cloud systems – re-keying
- ▶ Not implementing complex passwords or single sign on protocols
- ▶ Not designating power user(s) within the firm
- ▶ Inadequate training
- ▶ Testing not performed at least annually
- ▶ CCO unaware of all systems and data flows

About AdvisorAssist

AdvisorAssist provides comprehensive services for new and established Registered Investment Advisors, Hedge Funds and Broker-Dealers.

AdvisorAssist Provides:

- ▶ Advisor Registration
- ▶ Advisor Compliance
- ▶ Advisor Technology Consulting
- ▶ Business Continuity Planning
- ▶ Mock Exams and Assessments



For more information, visit our website at <http://AdvisorAssist.com> or call Chris Winn at 617-532-0925.

Questions

If you have questions that do not get answered during this session, please feel free to contact me.



Chris Winn

Founder and Managing Principal
AdvisorAssist, LLC

617-532-0925

cwinn@AdvisorAssist.com

www.AdvisorAssist.com

