Managing the Compliance Risk of Dodd Frank (and other regulations) with RSA Archer Author: Ted Dziekanowski – CISA, CISSP, RSA-AA, MCSA, MCTS, MCT and Global Knowledge Instructor

# Introduction

Rules, regulations are becoming an increasingly difficult part of running a business today. They can impact your business no matter the size or type. It does not seem to matter what kind of business you’re operating, being able to prove you are following the law when the Information Technology system you are using is growing more complex with the mix of IT assets extending not only globally but into the cloud as well. Recent Archer classes I’ve taught for Global Knowledge prove this point. I had someone from a transit system who needed to interface with DHS. Another student who worked for a mega church trying to demonstrate compliance with Payment Card Industry Standards. Many students from a global financial services firm who needed to deal with not only the recently passed Dodd Frank legislation and other global regulations. Countless students from the insurance industry dealing with not only HIPAA but the Affordable Care Act.

If you’re reading the first paragraph and think “Well that’s not my problem”, you may be in for a very unpleasant surprise. The number one Archer application request in my classes is Vendor management. Why you may ask? Because if you are a vendor that in any way shape or form touches, manages or handles data that is owned by a “Supervised Entity” you may be required to fill out forms that make you as responsible as the owner of the data for the data’s safe handling. You could be a company that literally carries out the trash and may still need to prove that your internal Governance, Risk and Compliance (GRC) programs satisfy the requirements of your customers.

If you are still skeptical as to why managing compliance risk with a product like Archer is a good idea let me give you some other good reasons.

* Your customers will be happy. Think about it, your customers face the same regulatory issues you do and your business relationships may depend on the perception of your customers in the way you manage the risk in your organization.
* Money. You can spend smarter and buy smarter if you don’t toss money at perceived issues and instead focus on those where the risk is quantifiable. Cost of risk transfer (insurance or acceptance) may also be lower.
* Shareholders. If you aren’t on the front page of the Wall Street Journal because of some huge fine, the organization’s brand reputation is better and shareholder value improved just because money is being spent fighting some agency.
* You are going to make better decision about the future of your IT infrastructure. You may decide that running your own shop may not be worth the risk and you will be willing to use a vendor who can provide you with the evidence that they are complying with all of the rules and regulations the world presents. I teach Microsoft Exchange and often show students Microsoft’s compliance page and ask the simple question. Can your organization provide the same kind of documentation?

Before we go any further into the process of managing compliance risk with RSA’s Archer, let’s explain what Archer is. First it is a Gartner Quadrant award winning [product](http://www.gartner.com/technology/reprints.do?id=1-1IWARRL&ct=130828&st=sb.) that allows you to centrally manage and process everything you need to prove you do what your policies and controls say you do. It is a very popular and well respected program. I was somewhat surprised that a certain company in Washington state that had it choice of any product including their own was looking to hire someone who knew how to use Archer.

Having worked in IT for many years and having worked with many products RSA Archer reminds me of several other products which if you ever used them will provide you some context if you have never seen or used Archer before. It reminds me of IBM’s Domino product in that it has defense in depth down to the field level, is easy to configure a user interface capable of selectively exposing or hiding whatever data elements you wish and it can pull users and groups easily from any LDAP directory and can be customized fairly simply if your requirements are straightforward.

Archer is like Microsoft’s SharePoint in that it sits on a Windows Server Platform, using Microsoft’s SQL Server, which if you elect to operate your own Instance, gives you the comfort of knowing how to make Archer highly available and site resilient. Archer also integrates well with Microsoft Office and Exchange, uses C# and Silverlight if you want to perform deep customization.

Archer also supports feeding data to and from other data sources, can use EMC’s Documentum and is used by other RSA products such as Security Analytics as a means of communicating notification of data breech incidents and is a repository of the same. Archer is offered as Software as a Service or something one could manage on one’s own. There is an Android and iPhone app for the Business Continuity Solution which might be a good idea to get as a service.

RSA Archer as a program is structured and sold as a solution with applications that are capable of connecting to each other that are also reusable. You can create your own applications in Archer and use it for things like scheduling classes. That’s one of the many things Archer is used for at RSA itself. There is an Archer community exchange which may have an application that meets your needs and lots of documentation that describes best practices, more on that later. There are specialized modules as well that deal with for example feeding updated Federal Regulations into your Archer system.

While there are many kinds of compliance risk from which to choose for a case study, I’ve selected the Dodd Frank legislation as one to demonstrate what might be involved in setting up a eGRC (Enterprise Governance, Risk and Compliance) program using Archer for a Hedge Fund who might be privately owned and who now needs to deal with Dodd Frank. Since I get to hear all kinds of stories as an instructor about how the text book often clashes with reality I’ll share some concerns and problems faced by students in the Archer classes I’ve taught along with my experience in IT teaching not only Archer but security and Microsoft but as an auditor and security professional as well.

# What is Dodd Frank?

In the wake of the financial crisis of 2008, Congress has attempted to prevent not only a repeat of a Lehman Brothers like moment, where the stability of the entire financial system seem to be in peril, but also at the same time address one of the causes of the crises as well, the packaging of mortgage based derivatives and the seeming lack of oversight in the issuance of mortgages to less than qualified individuals often fraudulently.

With a stated aim of the legislation being “To promote the financial stability of the United States by improving accountability and transparency in the financial system, to end "too big to fail", to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes.” the Consumer Financial Protection Bureau was created. As of the writing of this paper (September 2013) in a report on [CNBC](http://www.cnbc.com/id/100906282) there were some 14,000 pages and finalized 155 rules and they are only 39% done.

The scope and reach of this legislation is truly amazing. “Supervised Entities” include investment advisers, hedge funds, and private equity firms subject to new registration requirements.[[38]](http://en.wikipedia.org/wiki/Dodd%E2%80%93Frank_Wall_Street_Reform_and_Consumer_Protection_Act#cite_note-38) It could also include foreign corporations that do significant business involving consumer financial services in the United States and could impact providers of services to “Supervised Entities” where the service provided is a requirement for compliance.

It is impossible to cover every aspect of the Dodd-Frank law as it pertains to IT and how RSA’s Archer product can help. What we will attempt to do is build the use case for RSA Archer product facilitating and providing the supporting documentation as proof of compliance for several sections of 17 CFR Part 39 RIN 3038-AC98 Enhanced Risk Management Standards for Systemically Important Derivatives Clearing Organizations. We will also briefly review a new RSA Archer solution that deals with Model Risk Management that specifically deals with the securitizing and pricing of mortgage based assets.

# 17 CFR Part 39

In reviewing both the Dodd-Frank act and the rules and proposed rules on the United States Commodity Futures Trading Commissions [web site](http://www.cftc.gov/index.htm) and the Consumer Financial Protection Bureau’s [site](http://www.consumerfinance.gov/), 17 CFR Part 39 [link](http://www.cftc.gov/LawRegulation/FederalRegister/FinalRules/2013-19791) drew my attention immediately as an Archer Instructor, CISA and CISSP. Two sections in particular focus on typical control gaps in a lot of organizations.

* You need a business continuity plan that ensures you’ll be able be back in business quickly.
* You need a risk management program.

Both need to be maintained and attested to by a Designated Compliance Officer (DCO). Imagine you are this lucky individual who needs to sign off on this under penalty of law. Even if your systems are highly available or not, they now need to be and you need to be able to prove that they are. In addition if you do not have a formal risk management system in place you now need one. While many organizations have a formal risk management systems able to prove that they are if you do not have a formal risk management system in place you now need one.

While many organizations have a formal risk management systems many “Supervised Entities” because of their legal standing and organizational structure do not. Putting together a Risk Management system that helps you identify, quantify and develop policy and controls to manage risk while also helping you manage controls around your Business Impact Analysis/Business Continuity/High Availability is a monumental task that requires specialized expertise in a variety of products especially if you elect to build it yourself in say something like Microsoft’s SharePoint or Service Manager. A much better solution to the problem presented is RSA Archer’s Framework of Compliance Solutions.

# Requirements

Like any undertaking in creating an IT solution to a business problem, defining requirements is essential to the success of any project. Requirements will be the foundation upon which a solution will be designed. It goes without saying that if your organization has a system development life cycle that it should be followed. Putting in a compliance system that it is not compliant is a contradiction itself. Based on an understanding of what Archer can and cannot do, here is a simple list of what might need to be addressed by the Archer implementation so it provides supporting evidence for compliance with Dodd Frank.

* A repository for documentation and a way to organize the workflow associated with a Business Impact Analysis
* Something that will facilitate Business Continuity Management
* A means to keep Disaster Recovery Plan and test results plans current
* If external vendors provide critical services their systems also need to be validated
* The law requires a Risk Management system be put in place
* Model’s used to value the worth of mortgage need to be treated like other critical applications
* Establishment of policies and documentation of exceptions
* Creation of controls based on questionnaires derived from authoritative sources
* A way a feeding and updated rules and regulations
* Managing assets
* Managing security incidents and have the ability to accept and process feeds from security appliances
* Making the systems to support the stated requirements highly available
* Provide training to not only users of the system but also administrators and developers as necessary
* Manage audits

This list may by no means be complete. The intent here is to show the level of effort that may be required to implement the solution to our two major requirements in Dodd Frank, Business Continuity and Risk Management. One other method of identifying requirements may be to use the [Examination Manual](http://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf) of the Consumer Financial Protection Bureau as a guide to identify gaps in existing controls and procedures and then use Archer to close those gaps

# Involvement of Senior Management

First what I consider the most important preliminary step that needs to be communicated by senior management to all involved. Everybody plays. If participation needs to be tied to performance reviews so be it. The values entered by participants are tied to VERY sophisticated Excel like formulas (look in the back of the Risk Practitioners Guide if you don’t believe me) that will produce metrics that can significantly alter the allocation of funds and change the organizational structure of the company using the tool.

Senior management needs to understand that the level of effort, especially in defining authoritative sources, setting up data feeds, testing and ensuring the reliability and availability of the RSA Archer environment may becoming higher if requirements are not defined and the project managed as though Archer was going to be the most important project ever started. If the objective is a single pane of glass to see all of your risk and have everything in one place that is something that can be accomplished but not without the cooperation of all and making sure resources are available.

Training is essential to the success of this project as well. Lack of training may result in the most important system in your organization being unavailable and users not fully understanding what is expected of them. This is not your normal application. Users are more likely than not individuals with other important responsibilities. Not wasting their time has a higher value than the typical application user.

# Administration of Archer Itself

Back to our earlier description of Archer. Archer uses SQL Server and IIS to present data in a browser to users. Being a systems kind of person my mind is always looking at the non-Archer things that need to be accounted for. Here is a short list of what my concerns would be.

* Archer is going to have a lot of really important and sensitive information. How will I secure the system?
* How are users going to get to the server? Simple test case. Someone get an email link to a record in Archer on their iPhone. What’s supposed to happen?
* How are we provisioning user and group access?
* How do we de-provision users?
* Who is responsible for access role creation?
* Is high availability and site resilience a requirement?
* Can we recover the system in the event of a catastrophic failure?
* If we are backing up Archer and sending tapes offsite are the tapes encrypted?
* How and who will manage version and change control?

The list could go on for a while. Check the Archer website for the latest configuration guidance.

# Seeking Outside Help

The sizing, securing and licensing associated with the solution should also be part of the Statement of Work that will be part of any request for proposal made by the organization implementing Archer. Certainly the number of hours that will be required to implement this solution will be a function of how much of a risk management and BIA/BCM/DR is currently in place. A significant amount of time and effort may be required to integrate external systems to ensure data integrity and minimize the impact on external systems.

# Implementation of the Risk, BCP/BCM, and Model Risk Solutions

For our hypothetical Hedge Fund let’s see what might be required to satisfy the requirements that an audit might require. Remember we are engaging in generalities here. This a guide not a project plan in detail.

## Dependencies

To successfully implement the modules defined as requirements there are other parts of RSA Archer solution that are also necessary. Archer Risk Management Solution Dependencies include applications within the Enterprise Management, Policy Management and Compliance Management solutions.

## Scope

The Archer Practitioners guide illustrates the dependencies that need to be identified as part of the deployment of the Risk Module. Lots of things can arise as we strive toward meeting our objectives including human error and poorly designed processes that we are trying to duplicate erroneously into Archer. Also the challenge of meeting regulatory deadlines while still trying to execute a business model. Limiting the scope of the project to satisfying the regulatory demands of Dodd Frank regarding Risk, BCP/BCM and Model Management for our financial services firm is the priority.

## Standards, Rules, Regulations

One of the interesting challenges these days is staying abreast of what rules and regulations besides Dodd Frank does an organization need to comply with. First and most important I am not an attorney or providing legal advice. What I have found is a reasonably good guide at CSO Online that lists the rules and regulations as of December 2012 in [one place](http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guidelines-directory). The sand is constantly shifting here and dedicating someone whose job it is to keep up with changes may be required.

TA bit of good news is that Archer provides authoritative sources that meet [ISO 31000](http://www.iso.org/iso/home/standards/iso31000.htm) and the [OCEG GRC Capability Model](http://www.oceg.org/resources/grc-capability-model-red-book/) standards. RSA Archer also has a [Code of Federal Regulations Solution](https://community.emc.com/docs/DOC-25627) that will allow you to maintain the risk modules compliance management.

## Managing the Program

As with any large IT undertaking there is the danger of scope creep. Archer can solve many risk related problems and the danger of a decentralized bottom up approach is that fundamentals such as field names, taxonomy and change control methods may go uncoordinated resulting in systems that may have difficulty in exchange data between units later. Since Risk Management involves the five phases listed in the diagram and each process may have three phases of maturity an honest self-assessment prior to the project initiation may be in order.

## Management of Risk Management

As was discussed earlier, Senior Management needs to ensure that the implementation of the Archer Risk Management Program is giving the highest priority in terms of resource support and emphases. Deciding who will own want risk and how Risk will be managed and communicated may require some changes to the organizations structure. Should the Risk Group work under IT or should the lines of authority go directly to the Board of Directors? These are important considerations and should be considered before the project begins.

## Taxonomy

Simply put we don’t want people typing things in for one very simple reason, search. Think of what happens if you mistype a phrase in a search engine, you don’t get the answer you want. Same thing is true when you search in Archer. By minimizing the inputs performed by users the ability to quickly and accurately find things is improved. I teach SharePoint 2010 and managing the Managed Term Sets in SharePoint is the stuff where dedicated blogs exist just to cover that topic. During the proof on Concept phase of the Archer deployment would be a good time to start developing the process by which terms will be added and managed.

This would also be a good time to have a walk through with the owners of applications from which Archer will be receiving data. Garbage out. Garbage in.

## Identifying Risk

Where we will begin the whole process of Risk Management? Part of decisions that need consideration include

* Are we measuring quantitatively or qualitatively?
* What’s the scale risk should be judged?
* Who is going to be performing the risk assessment?
* How frequently will they be done?
* Do we incorporate the findings into Archer?

Then the second not so good part is what do we do with our results? The greatest danger in performing a risk assessment is finding something really bad and figuring out who to tell and then try and figure out what to do?

Do we accept the risk, reject it as immaterial or try and fix it with the introductions of controls that will hopefully produce a positive finding during our next audit. For organizations newly designated as a Supervised Entity these will certainly produce some interesting moments.

## Managing and using the Archer Risk Module

When fully implemented the Risk Management solution will be able to role risk from all parts of a company into a solution that will provided the means though calculated Key Risk Indicators (KRIs), Key Performance Indicators (KPIs) and Key Control Indicators (KCIs). Loss events and Insurance used to transfer risk will be documented and the Question Library is used to gather information from Risk Owners.

The Solution will also give us the ability to perform risk reviews at the business unit level and facilitate assessments as well as a platform to project manage the process. What follows is a summary of the functions of each of the components.

### Risk Hierarchy

Risk Hierarchy is an application whose use cases include the ability to generate KRIs that roll up from different parts of the organization. These metrics can be used as validation for statements made in 10-Ks and 10-Qs. The level of detail when implemented is quite impressive.

### Risk Register

The Risk Register is where risk is cataloged, measured and assigned either quantitatively or qualitatively. Information is gathered into the Archer system often by using surveys where the questions were either developed internally or by using the authoritative sources provided by Archer. Care must be taken when assigning weights and values to the questions to ensure that proper valuation of risk occurs. Risk Analysis also maintains a sub form that allow a survey to provide additional classification of risk. Once risk is identified the methods determined to best remediate the risk are detailed in the response and treatment section of the record. As in all of Archer sections are made visible or invisible by data driven events. Depending on the selection made with regards to risk different additional sections will perform additional calculations. Risk monitoring with the application presents not only the status of open items but the loss events associated with the risk.

### Archer Risk Questionnaire

This is that part of the Archer Risk Module that not only feeds values into Archer but leverages institutional memory and knowledge. Questions can come from Archer’s authoritative sources or your own. When you create your own questions the values and weights are part of what is used to calculate risk so you need to be careful when you create the questions and users complete questionnaires accurately.

## Business Continuity Management Sol ution

Archer’s Business Continuity Management Solution not only address the Dodd Frank compliance issues but only adds robustness to your existing infrastructure planning. This is one of the few Archer solutions that has an iPhone and iPad app and an Archer instance might be placed outside your normal datacenter location to enable a speedier recovery. The dependencies include policy and Compliance and Enterprise Management Solutions. Among the solutions benefits are;

* The ability to centrally manage business continuity programs
* Perform business impact and risk analysis
* Test plans and periodically test them
* Track crisis in real time
* Implement business recovery
* Report on the program itself.

The applications and sub solutions include;

* A BCM register which is used to
  + rate the impact and likelihood of each risk
  + Link to the BC/DR application
  + Categorize risk i.e. Natural Threat or Business related threat.
  + Prompt for periodic review
  + Associate crisis to risk
  + Relate risk to multiple targets in the Enterprise Management Solution.
* A BIA Analysis Application that allows for the determination of critical processes and the order of restoration necessary for continued operations
* The BC/DR Sub solution that will act as a repository for
  + BC/DR plans
  + Recovery Strategies
  + Recovery Tasks
  + Requirements
  + Roles and Responsibilities
  + Training / Exercises.
* The Crisis Management Sub Solution allows for the documentation of events, tracking of notifications and the activation of the BR/DR plan. Applications in the sub solution include;
  + Crisis events
  + Emergency Notification and Call Tree
  + Activated Plan application
  + Notification History application.

## Model Risk Management

Finally perhaps the most interesting Solutions in the Model Risk Management. Here the sub solution lets you organize and keep track of all the models very much in the same way applications are tracked and managed. It is possible to track and measure performance across key performance indicators, provide for risk certification and sign off, organize documentation and perform validation and track goodness of fit. The individual applications include;

* A Model Inventory Application
* Model Change Lifecycle
* Module Inventory Documentation
* Performance monitoring
* Performance Monitoring Results
* Model Risk Certification
* Model Inventory Validation and Review
* Model Validation and Review Tools
* Model Validation and Review Tasks
* Model Change Reports

## Summary

We have covered an immense amount of material here merely skimming the surface with the effort required by our hypothetical financial services firm need to comply with Dodd Frank. Considering the alternative of building and similar solution from scratch and trying to develop authoritative questionnaires by hand, RSA Archer with its large installed base and ecosystem, is the better alternative. I’d strongly recommend calling in an RSA rep, take the Administration class or just go and visit YouTube and search RSA Archer and see how Archer can help with all of your Compliance Risk issue not just the use case developed here.

## Resources

### Archer Training –

* RSA Archer Administration - Global Knowledge Course 9738 ([Link](http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=17849&catid=542&country=United+States))
* RSA Archer Advanced Administration – Global Knowledge Course 9739 ([Link](http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=17851&catid=542&country=United+States))
* Getting Started with Enterprise Risk Management – Global Knowledge Course 9781 ([Link](http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=19725&catid=542&country=United+States))
* Getting Started with Policy and Compliance Management - Global Knowledge Course 9780 ([Link](http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=19367&catid=542&country=United+States))

## RSA

### Customer Support –

* Information - <http://www.emc.com/support/rsa/contact/phonenumbers.htm>
* Customer Support E-mail <mailto:archersupport@rsa.com>

### RSA Archer Community –

<https://community.emc.com/community/connect/grc_ecosystem/rsa_archer>

### RSA Archer Exchange –

<https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange>

Access the documentation from the Documents page on the RSA Archer Community at

<https://community.emc.com/community/connect/grc_ecosystem/rsa_archer> (Registration Required)

RSA Archer Demonstrations are also available on [YouTube](http://axp.zedo.com/asw/pfr/305/1523691/8/o.html?cdm=xads.zedo.com&a=1523691&x=3869&g=172&c1=305017112&c2=305017112&i=0&n=305&s=1029&1=4&2=1&tg=1377795314&vr=8&m=24&w=30&os=3&p=6&h=747871&f=1354039&b=30&o=20&y=3&v=1&t=i&u=J3wxkx8zTfWiTUVMptuMWw**~072113&z=0.2998643006620564&mb=29&dm=.zedo.com&pt=3Interactive&q=&sk=&l=&cd=&adm=c5.zedo.com&r=2&ldm=l1.zedo.com&exp=0&cm=&tt=0&wm=Transparent&dnt=1&tsad=0&p1=&p2=&p3=&p4=&p5=&prfl=&ct=0)

## About the Author

I think of myself as a specialist in the area of IT governance, IT risk identification and mitigation as well as managing a broad range of regulatory and statutory mandates along with extensive IT technical skills. I've done things that includes being a session speaker at the 2006 North America Audit, Control and Security Conference, where I presented on the security and the auditing of Active Directory and Exchange. I have 15 years of directory services, identity management and messaging experience providing system designs to numerous clients of varying sizes. Other things includes performing Sarbanes Oxley compliance testing and providing guidance that has helped organizations deal with the compliance and business risk that can come from the use of electronic messaging. Among my certifications include being an IT Systems Auditor (CISA), Certified Information Security Professional (CISSP) along with product certification from IBM, Microsoft and RSA. I also have a BS in Accounting and an MBA with experience in dealing with regulatory issues such as Sarbanes Oxley, BASEL II, FFIEC, PCI and HIPAA as well as numerous privacy mandates. I have been training representatives of large enterprises for Global Knowledge to identify and remediate institutional risk from email and to develop a message management solution using Exchange 2010 and reducing operation risk by using System Center Operations Manager and System Center Configuration Manager I’m currently teaching Archer, System Center, Exchange and SharePoint for Global Knowledge.

You can email me at [ted@chathamtech.com](mailto:ted@chathamtech.com)

Follow me on Twitter – [Tdziekanowski](https://twitter.com/TDziekanowski)

Linkedin:<http://tinyurl.com/bv75fee>

Blog: <http://www.chathamtech.com>