Compliance For the CIO

By John Supplee in conjunction with Harris Kern's Enterprise Computing Institute

It is near impossible to put a value on corporate data. Some would say it is invaluable. Compliance, at least in the realm of Information Technology, has much to do with how that data is stored and accessed. The amount of data an organization holds and the role of this information has only increased the complexity of IT within the organization. How do you ensure that only those who are supposed to use that data see it while at the same time make it easier for those with permission to get their jobs done? You must intelligently manage this data in order to comply with the thousands of regulations that control how companies store and access their data. In this sense the CIO's job has become more complicated with every new scandal and subsequent regulation.

This article was written mostly for CIO's of small to mid-sized companies looking for some suggestions on how to handle compliance. Most large companies have a compliance team and often in-house lawyers that keep on top of all the regulations. This team can also consist of someone from IT where that is their main job. This person ensures that the CIO doesn't have to spend much time thinking about whether they are compliant. In smaller companies it often falls upon a team of professionals from all the different business units, each having their regular job to do also. In this setting it is imperative the CIO be involved considering they most likely don't have the expertise or manpower in-house to handle compliance. According to Wall Street & Technology (1) "With an unending wave of scandals being revealed in financial services, no one can argue that the focus on compliance will increase. As a matter of fact, a recent Information Week Research survey found that 65 percent of senior executives on Wall Street plan to spend more on compliance this year." It won't be just financial firms bogged down with regulations either. Health care has to figure out HIPPA, and public companies have Sarbanes Oxley.

Why should you have a compliance program and why should a CIO care?

The most pressing reason to have a compliance program would be to comply with the rules and regulations that govern your industry. It would be impossible to ensure compliance with the laws and rules unless you have a strong compliance program and culture. Up to date compliance policies and procedures are essential for an effective program. Falling behind could mean more visits from regulators to ensure you are doing everything to keep up. Everyone at the company affected by these rules must buy in to the procedures and follow them. Employees must be aware that compliance is the law and there are real consequences with not abiding by the rules and regulations. This type of culture is ultimately what will save you in an audit.

All of this talk about the law and rules ignores the fact that most regulations make good business sense. Often these rules are things any good operation should be doing, such as disaster recovery or security policies. Violations of any of the laws could ultimately harm your companies' reputation not to mention the bottom line but a disaster could put you out of business for good. According to Michael Dortch "Beyond lost revenues and productivity, sufficiently disastrous disruptions can threaten an enterprise's very existence. According to some industry-watchers, as many as 20 percent of companies that experience serious,

sustained disasters go out of business completely within 24 months of such events."(2) A compliance program is often a proactive way to head off any problems before they come about. You'll need a method for identifying and controlling risks before they become a violation. A good compliance program should encompass all business lines and operations.

The IT department of any company has the control to be the key in every process within every function. These days nothing gets done without touching some type of technology and that includes compliance. As CIO your job is both strategic and tactical. It is your job to keep your department running smoothly while supporting a whole array of disperse business units. You must also focus strategically on the long-term vision of your business in order to find the best payoff between business objectives and technology.

When something goes wrong in compliance it can suck your staff into an endless cycle of emergencies and fixes. No other group within your organization has this draining affect. By being proactive you can ensure that everything runs on time and on budget. The basis of this chapter is to give you the tools to navigate through the maze of regulations. There is no one size fits all with regards to regulations but I have tried to put together some helpful hints from my experiences.

I. Know who is involved:

It is important when you work as a CIO to fully understand everyone involved in the compliance process. From the agency regulating your business, there could be many, to the internal staff charged with keeping you compliant, to the auditors you hire to find the problems before the government does you should know them well. Quarterly conversations, meetings or updates can help you grasp regulations, and their impact on your business, before the regulators are asking why you are not complying.

a. Regulators

Regulators often offer mailings on a regular basis. These mailings usually come from the post office or electronic mail and are very informative. These newsletters are packed full of information about upcoming regulations and what the hot buttons of that regulatory body currently are. Then can give you insight on what the regulators are up to. I usually don't have time to read them in depth but will peruse them looking for important new or revised items. These are the items you should concentrate on because they are what the regulators will be looking for the next time they are in. Usually the newer subjects are the ones you have spent the least amount of time addressing.

Understand the goals of the regulations in order to understand what the auditors will be looking for. Regulations are often very vague. This is done on purpose because not every company is exactly the same and regulators do not like to tell you how to solve issues. They will rarely tell you what types of technology to use, or if any is needed at all. Figuring out the goal of a new regulation is a great way to build a relationship with a governing body. When a new rule comes out call your regulator for clarity, even if you feel you have a good grasp on it. This twenty-minute talk between audits lets them know you take their jobs seriously and often makes the next audit a little more comfortable, if an audit can be

comfortable. It may also increase the time you have between audits. If you are always known for running a tight ship and being up on all the new regulations, the regulators may push your next audit off when time schedules are squeezed with more egregious companies.

The FFIEC offers a great series of books that explain exactly what they will be looking for and how they will determine whether you are compliant. I have made binders of these manuals and will reference them when needed. If you do not work for a financial institution then check with your governing bodies to see what they have to offer on guidance.

b. Internal Staff

Internal compliance staff can be invaluable when the regulators are about to come in. If your staff is seasoned you want to allow them to do what they are trained to. They have been through this and if they are worth their salt will know what is coming. They will have alerted you in plenty of time when a new regulation has been approved. It will up to you to work with the compliance staff to determine how this will affect Information Technology and have a solution worked out. There are many regulations that have nothing to do with technology but as business processes and technology become more pervasive these regulations often get pulled into the technology mix.

If you are starting a compliance staff from scratch or you are the compliance staff then you need to take a step back and assess strengths and weaknesses. Below is a list of steps that will come in handy when organizing for compliance.

i. Determine how often the regulators will be reviewing your company.

ii. Create a map of all the different regulations. Identify all of the different areas that overlap, this goes for both departments and regulations. Determine what common things that can be done to minimize the amount of work needed to be compliant.

iii. Layout what actions the compliance function will take to ensure compliance. Compliance, with the approval of upper management, should have the ability to take disciplinary steps toward employees who blatantly break regulations.

iv. Policies and procedures for the compliance function must be updated regularly. New regulations seem to be coming out everyday. You must have someone responsible for knowing what those regulations are and updating the company.

v. Internal, or external if your company does not have an internal audit function, audit should review the compliance program on a regular basis.

vi. Publish, maybe on your intranet, procedures for employees to report compliance issues. Be sure these procedures do not inhibit reporting, such as having the employees report issues to their direct reports.

Departmental heads may want to bypass compliance and resolve issues themselves.

vii. Review every business units compliance procedures and their effectiveness. Take corrective action if required to keep each function on track.

viii. Regular training sessions must be held with all staff in order for a compliance program to remain effective.

ix. Report all findings and actions taken to executive management and the Board of Directors. First you'll need to determine within your structure who reports to whom and how difficultly solved issues get resolved, who makes the call.

x. I believe the most important thing you can do to help stay compliant is to get upper management buy in on the importance of compliance and then conveying that to the staff. Have the CEO speak about compliance regularly. When a new regulation comes out have someone high up sign the memo that goes out updating the staff. The staff needs to know that compliance is supported from the top.

II. Compliance Staff Structure:

The structure of your compliance staff can also have a big impact on their ability to meet new challenges and get you through an audit.

a. Head of Compliance:

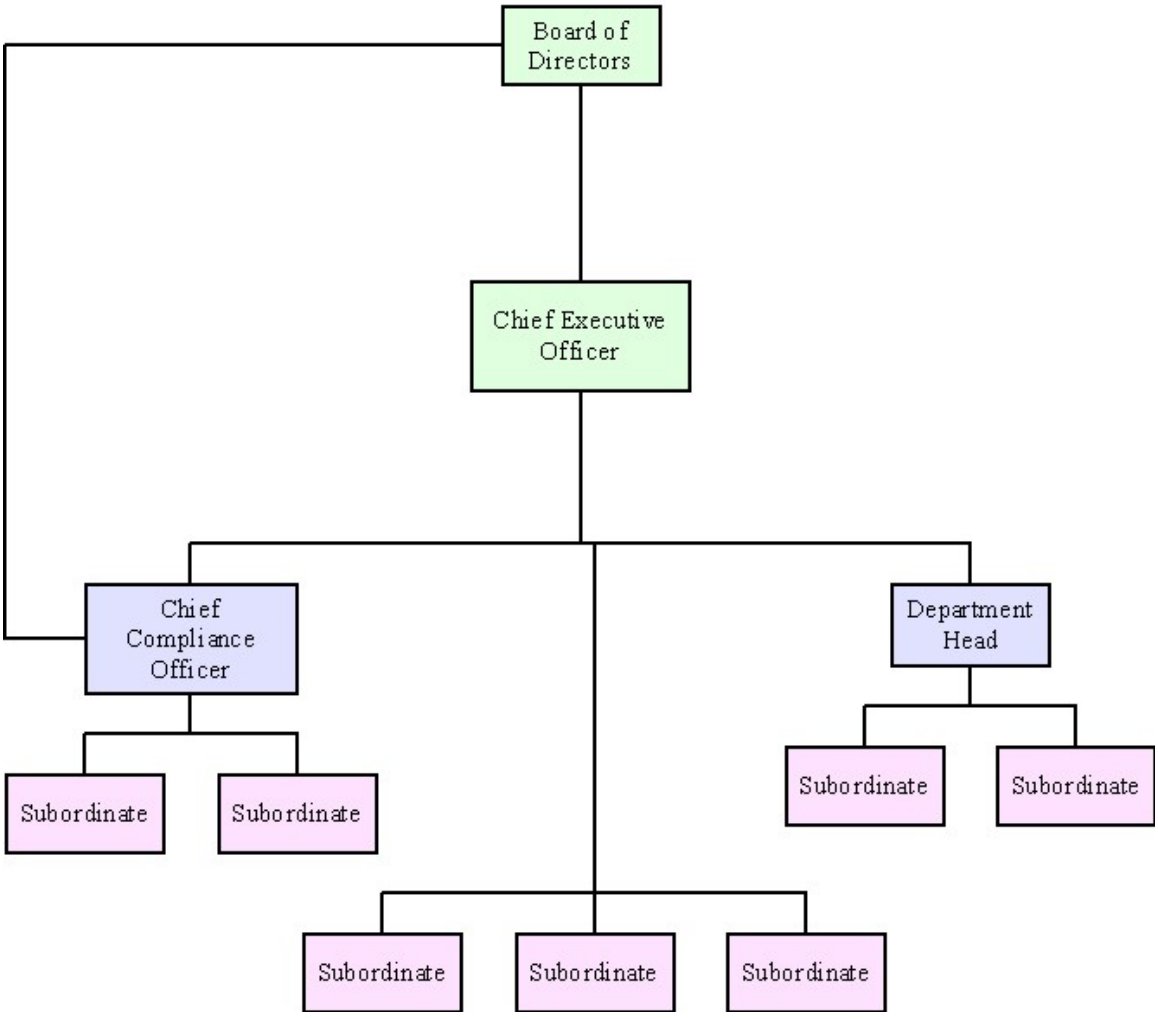
If at all possible the head of compliance should have no other duties. This person should report directly to upper management and not be affiliated in anyway with another department. This person must work closely with department heads to ensure they take compliance seriously. They also must have free reign to be able to talk to any employees at any time. Training is essential not only for the compliance personnel but also for the other staff members.

If you company is too small to dedicate someone as a compliance officer than you should choose someone to head up the position. It is vital not to skip this and think that a committee can handle compliance. In some instances a committee may work fine but having someone responsible is most desirable. Regulations are usually not clear so ideally this employee should be able to think creatively. Often times it is hard to get upper management at a small company to understand but this employee must also be able to report to a high ranking officer of the company on compliance issues. They also must be able to go straight to the Board of Directors with any issues that cannot be worked out with upper management. See table 1 for a sample organization chart.

b. Compliance Staff

Ideally it would be great to have a staff to support the head of compliance but if you are in a smaller company that is not always possible. I believe the next best way to handle support staff for compliance is to assign one person from every department to compliance. Have this person report to two people, department head and compliance head. This helps bring many issues to the forefront of compliance long before they become an issue and also helps create the sense that compliance isn't someone else's problem. Never put the department head or second in command on the compliance team. Since department heads don't like anyone scrutinizing their departments this could inadvertently cause things to be hidden from the compliances view.

Compliance Organizational Chart
Table 1



III. Institutionalize Compliance (make it everyone's job)

a. Formalize procedures

By formalize and publishing your compliance procedures their can be no pleading ignorance of the law. This will also go for you and your staff too. No longer can you tell regulators that you were unaware of a specific regulation or their interpretation of it. At your level, CIO, you should never use this excuse anyway. Getting your procedures in a manual and training staff on them is a very important step in overall compliance. Sometimes, just through the act of training, employees will bring up instances and situations that you may not have been aware were going on. This will allow you to adjust procedures before it becomes an issue with regulators. Task your employees with learning regulations that affect their functions. Make everyone head of compliance by conveying the importance upper management has put on staying compliant.

Always be mindful of old regulations when you have a new technology or process being proposed. Sometimes the regulators will assign an old regulation to some new technology your firm may be utilizing. Often these are the types of regulations that can catch you by surprise. An example of this would be the books and records requirements set forth by the Securities and Exchange Commission. These rules may have been written in 1934 but many brokerage firms received multi million dollars fines for not complying with the rule. On a very simplified basis the rule states that you must keep all correspondences with clients and interoffice concerning business as such. With the advent of Electronic mail and instant messaging none of the firms realized, until it was too late, that the procedures they had in place for retaining and then reproducing these types of communications were not good enough.

b. Governance

"Nothing gets a board of directors' attention like the word "liability". In a corporate compliance environment where new privacy and security regulations like Sarbanes-Oxley and USA Patriot Act hold board members to a high degree of responsibility for lax corporate governance, board members are turning to the CIO and IT department for updates, answers and assessments on how tight security measures are operating." said Brian O'Connell of Bank Technology News(3).

Investor confidence in corporate governance has dipped to an all-time low. This has prompted a move by politicians and regulators to try and reform corporate governance. Regulations in this area will only increase and it is imperative that management and the boards of directors keep current with the latest developments and implement necessary changes to handle the ever-changing rules. Since every company is different there is no standard way to handle governance although a formal corporate governance structure is a key way to ensure you meet any standards that have been put in place.

Corporate governance is a system of checks and balances between the board of directors and management to produce an efficient company that allows investors to feel comfortable with the ethics of that company. Recently the board of directors at every company has had to take their responsibilities much more seriously. Audit committees that used to be a rubber stamp for accounting are now scrutinizing every detail in hopes of heading off any minor issues before they become major problems. The CIO should strive to create a board of directors committee to help in oversight of information technology. This

helps increase exposure to the inherent risks technology has within businesses and allows the CIO a forum to get things done.

Some keys to successful corporate governance are:

i. Training board of directors on what is expected of them. There are courses offered at many colleges these days covering this topic and geared toward directors.

ii. Identification of potential conflicts of interest and the board's responsibility.

iii. Strategy and planning for the company. This could be for the company overall and for individual departments such as IT or HR.

iv. A risk management and compliance process that is robust.

v. Understanding financial statements and critical policies in financial reporting. This touches on Sarbanes Oxley where financial transparency and disclosure are critical. The CIO is instrumental in helping to facilitate this transparency.

Some ways to help you improve the structure already in place:

i. Understand any existing changes in regulations.

ii. Determine what resources are available to the company and whether you'll need to look outside the company to fill any needs.

iii. Review and, if necessary, change any existing governance programs to create a program that meets the companies' needs and circumstances.

iv. Ensure that regulators are kept up-to-date with any changes made.

c. Risk Management

Every company should ensure an adequate risk management structure exists. Some companies can afford to have a separate department dedicated to risk management that review such areas as audit, compliance, information security and disaster recovery. Edward Hurley of CIO News says, "Many federal regulations require a risk assessment. A thorough risk assessment may show holes that the company didn't know existed. A risk assessment may also help identify programs to cut."(4) An overall risk assessment is the first step in comprehensive risk management.

i. Determine which functions/departments within your company will need to have a risk assessment done. A key determinate is whether you need that department to keep functioning in a disaster situation. Some examples are:

a. Operations

b. Information Technology

c. Marketing

d. Trading

e. Banking

ii. Determine what the risks are that could occur in each area. Perform a risk matrix for the department as a whole and then on each risk within the departments. See Table 2 for an example risk matrix for the Information Technology department as a whole. This matrix is a modified version of what the Federal Reserve Bank of Philadelphia recommends.

iii. Determine how each of those risks impacts the company as a whole. Some examples of categories are:

a. ***Credit Risk*** – arises from the potential that a borrower, other counterparty, or vendor will fail to perform on an obligation

b. ***Market Risk*** – is the risk to the company, or an external vendor you rely upon, condition resulting from adverse movements in market rates or prices, such as interest rates, or capital market prices

c. ***Liquidity Risk*** – is the potential that the company, or an external vendor you rely upon, will be unable to meet its obligations as they come due because of an inability to liquidate assets or obtain adequate funding.

d. ***Operational Risk*** – arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen catastrophes will result in unexpected loss to the company

e. ***Legal Risk*** – arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of the company

f. ***Reputational Risk*** – is the potential that negative publicity regarding the companies business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions

iv. Upon identification and analysis of risks, each product/business line must then be assessed as high, moderate, or low depending upon the risk associated**:**

   a. ***High inherent risk*** exists when the activity is significant or positions are large in relation to company resources, when the number of transactions is substantial, or when the nature of the activity is inherently more complex than normal. Thus, the activity potentially could result in a significant and harmful loss to the company.

   b. ***Moderate inherent risk*** exists when positions are average in relation to company resources, when the volume of transactions is average, and when the activity is more typical or traditional. Thus, while the activity potentially could result in a loss to the company, the company in the normal course of business could absorb the loss.

   c. ***Low inherent risk*** exists when the volume, size, or nature of the activity is such that even if the internal controls have weaknesses, the risk of loss is remote, or, if a loss were to occur, it would have little negative impact on the companies overall financial condition.

v. Within the risk matrix assign what direction each of these risks are moving.

   a. ***Decreasing*** exists when the type of risk has been addressed and the risk is no longer one of the below categories.

   b. ***Stable*** exists when the risk has remained the same over a previous assessment.

   c. ***Increasing*** exists when a risk has increased, either because of new regulations or lack of compliance.

Table 2 (modified risk assessment)

Information Technology Risk Assessment

Risk Assessment Matrix As of Date

Type of Risk	Quantity of Risk	Quality of Risk Management	Overall Risk	Direction of Risk
Credit	N/A	N/A	N/A	N/A
Market	N/A	N/A	N/A	N/A
Liquidity	N/A	N/A	N/A	N/A
Operational	Moderate	Moderate	Moderate	Stable
Legal	Low	High	Low	Stable
Reputational	Moderate	Moderate	Moderate	Stable
Overall Risk	**Moderate**	**Moderate**	**Moderate**	**Stable**

Definition of Terms -

Quantity of Risk: assesses the nature, complexity, and volume risk within each component and is expressed as low, moderate, or high.

Quality of Risk Management: assesses the strength of risk management processes and controls for each risk and is expressed as strong, acceptable, or weak.

Overall Risk: balances the level of quantity of risk with the quality of risk management for each risk and is expressed as low, moderate, or high.

Direction of Risk: indicates the likely change of the risk profile over the next twelve months and is expressed as increasing, stable, or decreasing.

Acknowledged By:

_____

Board of Directors, Chairperson

_____

President, Chief Executive Officer

IV. Get Involved

There cannot be enough said about knowing what is going on around you. Recently I had to deal with a large financial firm whose employees were not following their email and Internet policies. My well-trained and knowledgeable employees alerted my compliance officer to the situation who in turn alerted me. Together we approached the other company about its employee's behavior. No one in compliance or upper management was aware it was going on until I brought to his attention. Regular meetings with department heads and training sessions would have resolved this issue long before it became a problem with us.

As CIO you'll want to meet with compliance on a regular basis. As with all department heads I view compliance as a partner in keeping the business running as efficiently as possible. I have a formal meeting once a quarter with informal meetings as needed. Find out how you can help prior to them asking for help. Often by the time they get around to asking it is already an emergency and your pulling staff off of important projects to handle regulations that have most likely been out for over a year.

Have the head of compliance alert you immediately when a new regulation comes out. Even if the deadline is far into the future sit down with compliance and do the following:

a. Figure out what new capabilities will be required to address the issue.

b. If no new capabilities are required assess the impact on current procedures.

c. Determine how you will implement and support these capabilities.

d. Assess who, what departments, will be impacted.

This is a good time to bring in to the discussion any department that is impacted. Often the department heads already know what is going on with new regulations and have thought of some solutions on their own. This is where you can start to discuss how to get some value out of the regulation. Often time upper management perceives regulatory requirements as generating no value. You should strive to consistently show value each time a new rule comes out. This way anytime a new rule is instituted that doesn't generate value upper management won't feel so overwhelmed by useless regulations.

V. Communicate often with upper management

There are many books and magazines out there to help you in communicating with your boss, whether that is the CEO or CFO, so I will not go into great detail on this subject. Within the realm of compliance it is very important that you do indeed have an open line of communication with you superiors and the Board of Directors. When your compliance team has a new regulation or existing issue to deal with it is best that you present the information pertaining to technology to the CEO. Ultimately the CEO is responsible to the Board and you are responsible to the CEO so the information has to be correct and timely.

When communicating compliance to upper management you need to focus on all possibilities. Is it clear to the BOD, CEO, CFO and so on? Did you cover what each of these positions might be concerned with? If you are communicating to the group as a whole it is often a challenge to be concise and yet thorough. If I have to present to a committee consisting of upper management I will often do the following:

a. Take the time to write up what I think each of the members will want to hear about. This means thinking of how the CFO, CEO, BOD will react to any given topic and tailor a response.

b. Find any commonality in the response and make it more concise

c. Finally take all of the responses and build a case for how to handle the compliance matter.

VI. Talk to vendors about solutions

Vendors can be your best friend and worst enemy all in one package. When Sarbanes Oxley (SOX) came out I had an army of consultants and vendors in an out of the CFO's office. Each vendor had the 'silver bullet' product or method on handling SOX. Just install their dashboard or tracking system or methodology and you'll be compliant with minimal cost, effort and time.

I give vendors a hard time, usually deservedly, but they do come in handy. Though it was time consuming the process of talking to many vendors made us realize there were no 'silver bullets' and in fact there were no specific ways you had to handle SOX. SOX is mostly about controls and documentation. If your business is relatively orderly and you haven't had a crazy number of recent mergers you'll probably find that you can document and create these controls without a million dollars in software and fees.

Have a list of trusted vendors that are involved with and know your company and industry. You can then call them when a new regulation comes out and see how they are telling their other clients to handle it. By having multiple vendors to contact you cut down on the misinformation you can often get from vendors. Many opinions are better than one.

VII. Talk to your outside auditors

This in a way is a lot like talking to the vendors. The difference is that the relationship with an auditor is much more trusted. Whether it is your financial or IT auditor they know your company inside and out and often tailor their response to fit your situation better than a vendor could. They are also, usually, independent of any product or consulting relationship so they don't give you specific ways to solve a problem but can help in guiding you to a solution. You are not the auditors' only client so they see how many different companies are tackling the same issue. They can offer insight to what others are doing in your industry and have often been in contact with the same regulators that will be visiting

your office. In this way they can tell you exactly what that regulator looked for in their last examination so you can be prepared.

VIII. Use regulations to produce value, competitiveness and productivity.

This is one of those phrases that gets a little worn out. As CIO you are always looking to produce value, competitiveness and productivity. You cannot always achieve each of these items when new regulations come about but that should be your goal.

a. Look at all regulations and how they can fit together.

b. Spend ample time in the planning stage to understand all aspects of the issues so as to help produce the value.

c. Take this chance reevaluate and manual processes and either change or automate them.

Conclusion:

A CIO's job is one of the toughest in business. You must understand both the business your company is in and how the technology handles that business. You must always be weary of rogue employees and hackers while still trying to accommodate an ever-growing list of wants and needs from your employees. Each new gadget or technology suddenly becomes a must-have even though that same employee was able to productively do his or her jobs for decades without it.

Whether you are responsible for setting up compliance or just one voice in many there are certain things you should always do. Structure the compliance staff in such a way that it will not inhibit the discovery and correction of issues. Know each of the individuals involved in the compliance process. Make compliance everyone's job, including the CEO and Board. Create a comprehensive risk assessment for the organization and each function. Talk about the issues with upper management and the board and train employees so as to create a culture of compliance. Talk to outside vendors and auditors when looking for solutions. And last but certainly not least try and use each new regulation as an opportunity to create business value.

Compliance with federal and state regulations just adds the complexity involved with the CIO position. You now have to worry about what every department is doing and the inherent risks with those activities. You'll need to ask yourself, is it safe for accounting to send that information through email or how well is the operations department trained on technology compliance. Each new regulation brings with it a new challenge. The key is to get your company in a situation where everyone knows and understands what it is to be compliant and can assist in helping you stay compliant.

References:

1. "Outlook 2004: Compliance tops the Charts," Wall Street & Technology, Feb. 12, 2004 URL: http://www.wallstreetandtech.com/showArticle.jhtml?articleID=17603335

2. Micael Dortch, "Disaster Recovery and Business Continuance: Best Practices," CIO, January 6, 2003.

3. Brian O'Connell, "Good Question: Bank Directors Want Answers From CIOs on IT Issues," Bank Technology News, September 2004.

4. Edward Hurley, "A holistic approach to compliance," CIO News, Dec. 12, 2003.