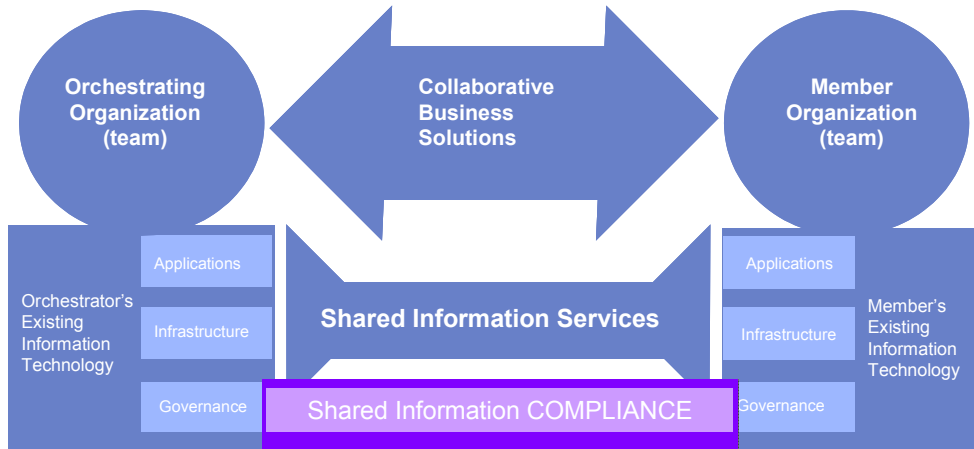


Trends in Compliance - Understanding Costs of Collaboration

Companies are finding more and more ways to add value by improving their product offerings, service levels and reducing costs by working with partners. Booz Allen Hamilton noted that 20% of the revenue for Global 1000 companies comes from strategic alliances and will grow to 30% by 2004.

The new challenge is the increased cost involved in becoming more dependent on reliable information from your partners and how you manage that cost. While organizations typically have initiatives to measure the business value provided by the relationship, there is a significant and



increasing need to better manage the security, quality and fiduciary aspects of information flowing between partners. There are significant risks / costs involved if you have become dependent on information sharing with a

partner or entrust that partner with sensitive information such as customer data, pricing information or inventory information (i.e., Is the partner managing information with the same care you do?).

This paper will focus on the increasing challenge of Shared Information Compliance costs and how organizations are approaching the management of those costs.

Shared Information Compliance Costs

Shared Information Compliance includes two costs, the cost of failure and the cost of putting controls in place to mitigate the costs of failure. We will take a closer look at each cost and its drivers.

Failure Costs:

A Shared Information Compliance Failure is caused by an information resource (e.g., application, technology, data, facility, or person) not performing as expected in a shared environment. For example, if a partner is managing inventory at a remote location, and the partner's system (due to a faulty change in application code) sends inaccurate inventory data at the end of the month, both the balance sheet and income statements will be incorrect. It was expected that the partner would send accurate inventory information and that did not happen. The root cause of the failure was a faulty code change, which caused the partner's system to incorrectly account for returns. The following table highlights several categories of causes of failures and examples of Shared Information Compliance failures.

Category of Cause	Example of a Shared Information Compliance Failure
Reliability of data / Change Management	A distributor (due to an erroneous change in application code) failed to send accurate inventory to a manufacturer who had consigned them inventory, causing the manufacturer to incorrectly state financial statements resulting in Sarbanes – Oxley Act compliance problems
Security of systems	A third party processor of credit card transactions failed to stay current

Category of Cause	Example of a Shared Information Compliance Failure
	with operating system security patches, thus allowing a hacker to come in and steal customer data from several different partner banks
Availability of system	A product company failed to keep their systems up during a critical window of time to receive shipments from their outsource manufacturing partner leading to a failure to send orders for the next day's production and costing the thousands of dollars of lost productivity
Confidentiality of data	A third party processor of checks, incorrectly indexed the check images resulting in images being viewed by customers that had not written the checks
Integrity of transactions	A hardware failure at a partner processing returns for a seller of computer equipment caused only a partial file of return information to be sent to the product company, resulting in significant complaints about over-billing and hours of lost productivity chasing down and correcting the problem.
Personnel & training	A fired employee from a supplier (which revoked access to their systems, but failed to tell customers) accesses a global 50 customer's collaborative web supply chain system and places orders for millions of dollars of equipment from multiple plants, causing significant lost productivity in both companies to identify and correct the problems

The costs of failure can be seen in general categories such as lost opportunity costs, lost productivity, cost to correct failures such as data problems, lost current sales and future sales due to perceived poor quality (i.e., offended customers), regulatory penalties, loss of intellectual property and most significantly damage to a company's image. The following chart highlights an analysis of a contract between a service company and an Application Service Provider (ASP) concerning the embedding of the service company's application in the ASP's web site. The contract specified over 60 requirements for the ASP which attempted to mitigate the problems identified in the left hand column and the costs across the top.

Problem	Cost Drivers							Brand, Image / Mkt. Valuation
	# of Controls	Time to Recover	Opportunity cost of lost time	Customers offended	Value of IP	Repeat sales	Penalties	
Unauthorized Access (loss / damage / misuse of data)	26	X	X	X		X		X
Unavailability	15	X	X	X		X		X
Unauthorized IP Use	13				X			X
Poor CS Response	9	X	X	X		X		X
Inadequate Functionality	7			X		X		X
Regulatory Non-compliance	3						X	X

The company has realized that while these requirements may be in a contract, they have no real-time method to monitor for these problems and hence the failure costs have not been sufficiently mitigated.

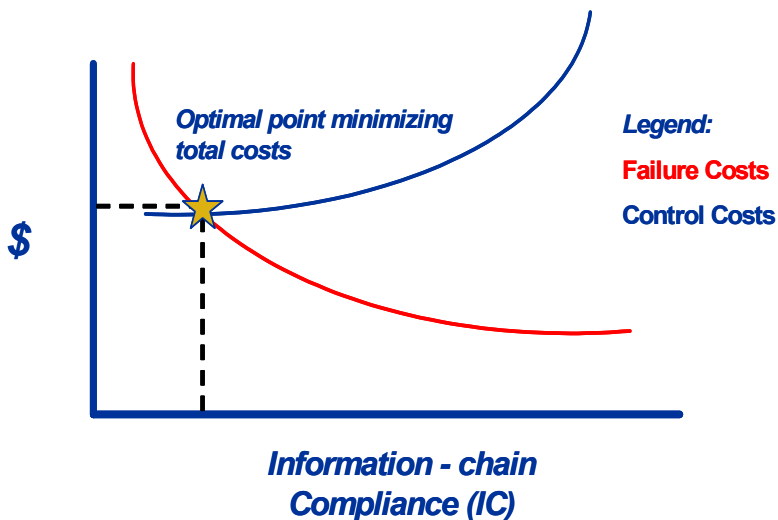
Control Costs:

So what can be done to prevent, deter or mitigate risks of shared information compliance? While organizations typically have processes to establish internal controls, **Shared** Information Compliance Control is more complicated. In a single organization's control environment, the manager would request a control; the staff would promise its implementation, they would implement it and assure the manager it was in place. With Shared Controls the process starts with a proposal, which can either result in acceptance, rejection or a counter-proposal. In other words, you negotiate to align control objectives for the shared information. In fact, virtually everything you have to do to establish Shared Controls requires alignment. You negotiate what controls are needed, how to implement controls and the implementation project. Hence, the costs of Shared Controls include:

- Aligning on objectives, risks, risk responses and what controls to put in place
- Discovering how to implement controls given different technologies
- Aligning on how to implement the controls
- Implementing the controls
- Monitoring the data feeds
- The time to identify a problem and take action (i.e., the longer to identify the higher the cost of the problem)
- The time to manage the life cycle of controls

Managing Failure and Control Costs:

While managing the risks of Shared Information Compliance you discover two costs (failure and controls), that are inversely related. The more controls you put in place the lower will be your cost of failure. Because the control costs are additive, business managers must identify the optimal number of controls to put in place (i.e., the cost of adding one more control will no longer result in an equal or greater reduction in the cost of failure). In the chart, the optimal point is where the cost curves cross.



Because the control costs are additive, business managers must identify the optimal number of controls to put in place (i.e., the cost of adding one more control will no longer result in an equal or greater reduction in the cost of failure). In the chart, the optimal point is where the cost curves cross.

The challenge in managing control costs is to constantly seek that optimal point and move the optimal point down the failure cost curve. Organizations, by finding ways to be more productive in implementing controls can push the control costs curve down. This allows them to implement more controls for less cost, while reducing the cost of failure.

Summary

The costs to share information are more complex than the cost to controls information internally. Even if you are large enough to demand that partners comply with your information rules, the cost of understanding how partners comply and making sure you have timely notification of problems is much more complex than doing the same internally. This increases your risks and puts your brand in jeopardy; yet working with partners is often the most effective way to provide better service to your customers. Given this paradox you may want to consider the following:

1. Do you think it will be important to work with a large number of partners in the future and, if so, do you think you will need a better way to manage the risk of sharing information with them?
2. Do you think your organization has an adequate view of the costs of failure related to sharing information with partners?
3. Do you put information control requirements in your contracts with partners and, if so, are you comfortable that partners are complying with those requirements?
4. Do you need to improve the productivity or maturity of your process for managing the sharing of information with your partners?

If you would like additional information on the cost of managing compliance or any of the above questions, please call our Information toll free at 877-255-4798 or write us at info@complychain.com.