

Trends in Compliance - Today's methods for managing shared information risks

What are the risks of sharing information?

Organizations that share information with other partners have experienced problems related to sharing information. Our white paper on Understanding the Costs of collaboration details examples of risks / failure costs in a variety of categories including the following:

Category of Cause	Failure Costs
Reliability of data / change management	Penalty for regulatory failure
Security of systems	Brand damage
Availability of systems	Lost productivity, poor customer service
Confidentiality of data	Regulatory penalties, poor customer service
Integrity of transactions	Poor customer service
Personnel and training	Increased operational costs

Clearly, sharing information has some risks that can lead to significant lost value in terms of fines, lost productivity, poor customer service and brand damage.

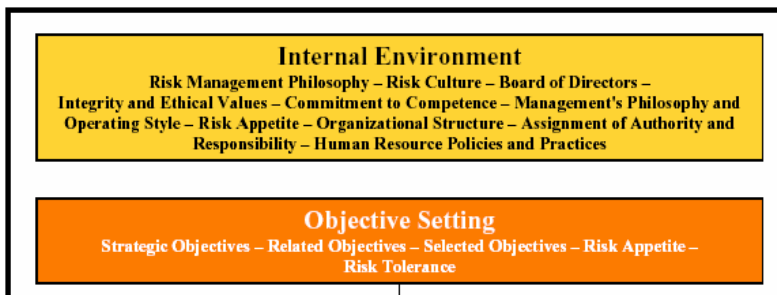
Why is this important

Sharing information with partners is increasingly valuable to organizations as they seek ways to better serve customers faster. Deloitte's research identifies Complexity Masters as those manufacturers with many partners across the world, excellent customer, product and supply-chain-related business process and excellent synchronization across those processes (i.e., only 7% of manufacturers). Deloitte cites Complexity Masters as being 73% more profitable than other manufacturers. GE wants to cut \$10B out of its cost and is working with partners to accomplish that goal. Healthcare organizations are experimenting with sharing vital patient information (e.g., going online so an emergency room physician can find what medicines have been prescribed to the unconscious patient) to improve the quality of care to patients. Companies are finding that working with partners increases their ability to serve customers and to reduce their expenses and infrastructure costs.

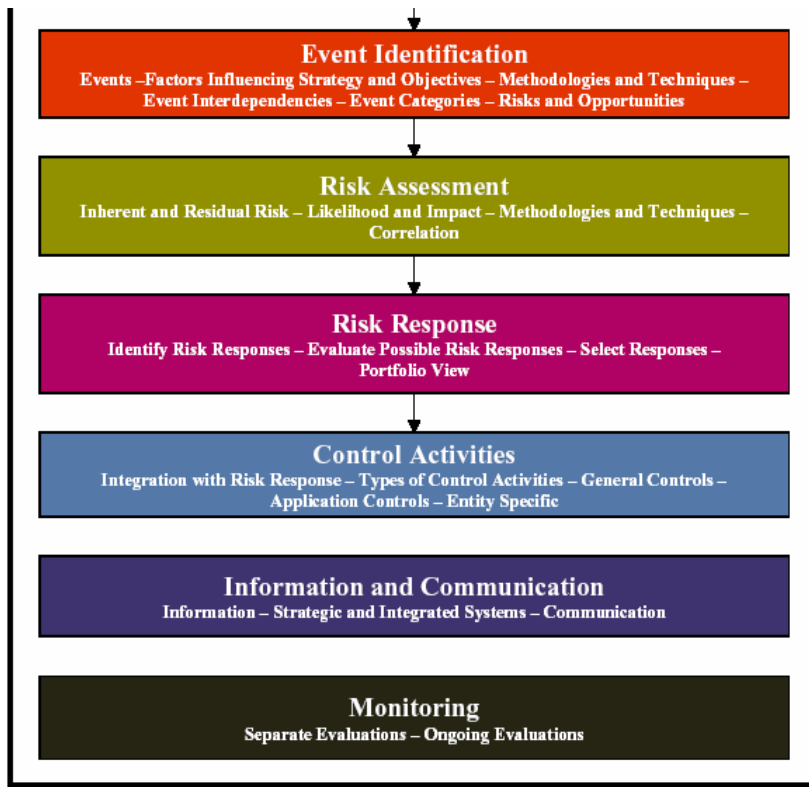
Regrettably, there are increasing attacks on information making it difficult to trust the data or rely on its availability. The increasing risks of sharing information make it even more important to have an effective process for managing shared information risks and controls.

Background

COSO, an association of accounting and audit professionals, has established a common framework for discussing Enterprise Risk Management, which applies to the risk of sharing information with partners. Their framework includes the components represented in the graphic.



While complicated by collaboration (see white paper on Understanding the Costs of Collaboration), we believe these basic components are also the foundation for an effective system of shared information risk management. They are also the basis for our observation about today's methods for



implementing shared information risk management and controls. Through our work with several different organizations and surveys of others we have developed detailed findings in each of the eight components and have aggregated those findings into the following observations.

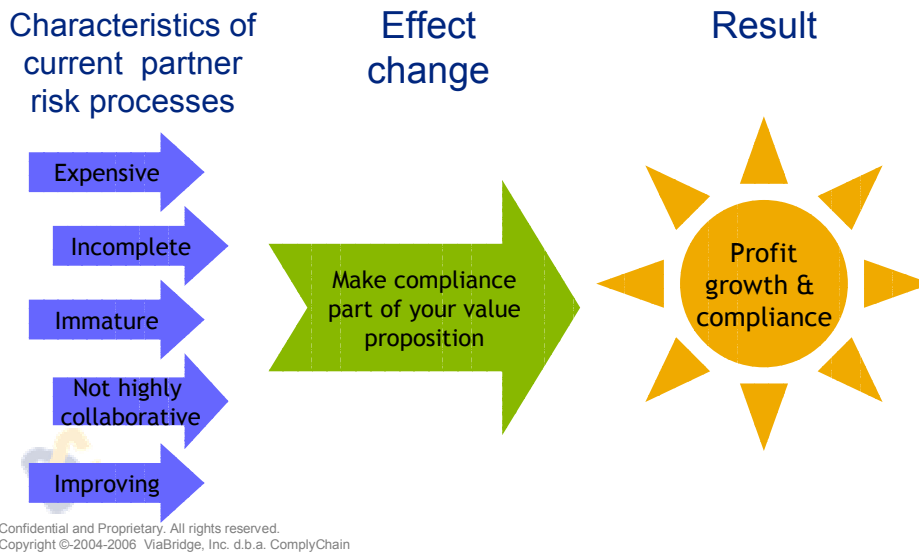
Observations

1. **Current partner compliance efforts are expensive.** One significant cost driver is the number of internal organizations that are impacted by compliance (e.g., audit, risk managers, compliance managers, IT security, and business managers). Additionally, we have seen that many of processes are very manual requiring significant time from professionals with significant knowledge in areas such as IT security, regulation, control practices, etc.
2. **Current partner risk reduction efforts are incomplete.** Most risk reduction activities today seem to be driven by specific initiatives vs. a more comprehensive approach to managing risk between organizations. Data security seems to be the hot topic for most organizations, leaving little thought to the risks of poor performance, data quality or customer service.
3. **Current partner management efforts are immature.** It is common to classify maturity in categories such as: ad hoc, repeatable, defined, managed and optimized. In looking at today's partner management practices, many activities such as contract term management have progressed up the scale to managed or optimized but some activities such as risk reduction efforts have yet to make it that far. Most organizations we have seen have started to put risk reduction terms (e.g., data security requirements, IT performance requirements) into contracts or programs, but only the leading companies are starting to understand how their partners are managing those efforts and changing how they work with those partners based on their risk profiles. We have seen relatively few organizations aligning on risks and establishing effective control practices between partners that can be efficiently managed.
4. **Current risk reduction practices are not highly collaborative.** Typically the dominant organization (i.e., the one with the largest brand value and most to lose) is the organization that initiates compliance programs and leads the way to reducing risks. They typically do this through contracts and programs driven by them, with little input from their partners. Consequently there is typically no mechanism for incorporating some risk reduction needs the partner has for the dominant organization. Moreover, without alignment on risk reduction objectives, there is less than desirable performance in getting partners to comply.
5. **Organizations are becoming aware of the need to manage risks and are making improvements.** Regulations (e.g., Sarbanes – Oxley, GLBA, HIPAA, EU Privacy Directives, state privacy legislation, etc.) have driven a large number of organizations to consider what

they are doing to manage risks with partners. The large companies are taking initiatives and requesting improvements from their smaller partners.

Most experts believe that simply complying with regulation is expensive. The best practice is to find a way to incorporate risk reduction efforts into your business. They suggest that by making it part of your offering you drive more value to the firm and find that compliance is a natural output of the process. The following graphic describes the desired process.

Findings Summary



Summary

There is an increasing need to effectively manage the risks of working with partners, but the practices related to managing risks have significant room for improvement. You may want to consider the following questions:

1. Do you need to have a better understanding of your current risk reduction / compliance management processes and the corresponding opportunities to improve them?
2. Would you like some external input into how you might incorporate risk reduction and compliance processes into the basic value proposition of your organization to help you grow profits?
3. Would you like more innovative ideas on current tactical problems to help you reduce costs of working with partners?
 - a. A more effective and efficient way of communicating policies and training
 - b. A more efficient way to understand you partner's practices
 - c. A faster way to align on risk management objectives internally and with partners
 - d. A more efficient method to plan coordinated risk responses
 - e. An efficient method for real-time notification of events

If you would like additional information on today's best practices for reducing risks of sharing information or on any of the above questions, please call our Information toll free at 877-255-4798 or write us at info@complychain.com