Top-Down Mandates and the Need for Organizational Governance, Risk Management, and Compliance in China: A Discussion

Marc Dupuis, Barbara Endicott-Popovsky, Hank Wang, Ilanko Subramaniam, and Yuejin Du
The Information School / University of Washington, GSB Law, Microsoft, and CNCERT/CC
{marcjd, endicott}@uw.edu, hwang@gsblaw.com, ilankos@microsoft.com, and dyj@cert.org.cn

Abstract

Through the course of this past decade China's unprecedented growth since the 1990s has brought to light some unintended consequences. Specifically, there have been several high profile incidents indicating a lack of sufficient mechanisms in place to ensure regulatory compliance with the rule of law. An additional impediment for Chinese organizations has been the structure within China that imposes top-down mandates in an attempt to achieve compliance.

The implementation of a Deming-cycle Governance, Risk Management, and Compliance (GRC) framework can assist organizations in China in meeting this significant challenge. A GRC framework prototype was previously developed as a graduate research project under the guidance of industry, legal experts, and faculty from the Information School at the University of Washington. This article discusses the unique challenges China has faced, the benefits of GRC frameworks in general, and the specific advantages of implementing the GRC framework prototype in China in particular. It is meant as a starting point to elicit both discussion and further research.

1. Introduction

China is a country with a rich history that has seen unprecedented growth for the past two decades. Along with this growth exists an underdeveloped and fragmented system for ensuring regulatory compliance. The primary impediment for the system is it relies on top-down mandates from the Chinese government that are often ill-conceived for the actual conditions within the organizations they are meant to regulate. The underdeveloped and fragmented system has resulted in significant breaches of product safety. Lead paint has been found on toys manufactured for children, melamine has been used as an additive in both pet food and baby formula to artificially increase the apparent protein content, defective tires have been made, among numerous other incidents (O'Rourke, 2008, p. 40). The consequences have often been fatal ("Secretive," 2008). Thus, there are a number of structural and organizational issues in the current compliance system that must be addressed. This includes the lack of transparency within the system as it is believed it is part of the larger problem with respect to compliance that has resulted in problems with product safety (Strunin, 2008, p. 31).

Frameworks that only address risk management are generally known as Enterprise Risk Management (ERM). As Weidenmier and Ramamoorti (2006) discussed with respect to ERM, "…in today's rapidly changing business environment, the ERM plan requires continuous monitoring that is real-time, dynamic, and embedded in the organization…to ensure that the ERM plan evolves to effectively manage the organization's risk" (p. 208). The features deemed required in ERM are found in Governance, Risk Management, and Compliance (GRC) frameworks. In addition to risk management, both governance and compliance are also encompassed in the framework. A Deming-cycle GRC framework is well-suited to combating the structural and organizational challenges faced in China. It encourages participation by all stakeholders and allows for change—it is not a static process. Transparency is increased while also ensuring greater quality and safety.

In light of concerns over the lack of transparency (e.g. by international companies [MacFadyen, 2008]) and significant problems with consistent compliance to quality and safety standards, the implementation of a GRC framework in organizations in China can aid in the defragmentation of China's regulatory compliance problems. The implementation of a GRC framework in an organization will allow it to address multiple compliance areas under one umbrella. One organization saved 30 percent by combining just two compliance areas (SOX 404 and labor laws) under a GRC framework umbrella (Mitchell, 2007, p. 288). While there are several different types of GRC frameworks, they all generally share some key features.

The key features shared by GRC frameworks can be found in the formal definition of GRC given by the Open Compliance & Ethics Group (OCEG) (2009) in their *GRC Capability Model Version 2.0* publication:

> A system of people, processes, and technology that enables an organization to:
>
> - understand and prioritize stakeholder expectations;
> - set business objectives congruent with values and risks;
> - achieve objectives while optimizing risk profile and protecting value;
> - operate within legal, contractual, internal, social and ethical boundaries;
> - provide relevant, reliable and timely information to appropriate stakeholders; and
> - enable the measurement of the performance and effectiveness of the system. (p. 8)

With this definition in mind, it will become clear during the course of this discussion why the implementation of a GRC framework within organizations in China can prove so valuable to combating the structural and organizational challenges they have faced. Therefore, the purpose of this article is to elicit both discussion and further research as it relates to these challenges; specifically, how the implementation of a GRC framework within organizations in China can aid in this endeavor. We first examine China's structural and organizational challenges as well as recent problems in manufacturing it has encountered over the past decade. Next, we look at GRC frameworks in the context of China and problems it has faced. This is followed by a discussion on the GRC framework prototype that was developed as part of a graduate research project under the guidance of industry, legal experts, and faculty from the Information School at the University of Washington. Afterward, two examples of GRC framework implementations are discussed, including one used by Microsoft. The GRC framework prototype is based on the GRC framework developed and currently used by Microsoft. We then consider some specific issues involving GRC frameworks, including GRC frameworks being viewed as an overhead item, their use in international organizations, and cultural issues that need to be taken into account. Finally, we conclude by discussing the urgent need for GRC framework implementations within organizations in China.

2. Background

A lack of regulatory controls and subsequent enforcement resulted in artificial fertilizer destroying crops and chemical glucose being sold as honey (Kahn, 2007). Those unfortunate events did not happen over the past few years in China, but rather over 100 years ago in the United States. These and similar events brought to light by the pivotal work *The Jungle* (Sinclair, 1906) were the catalyst for the creation of the Food and Drug Administration. While initially weak in its ability to regulate, it eventually obtained the power it needed to regulate effectively 55 years after its creation (Kahn, 2007).

The same problems the United States faced over 100 years ago are now being seen in China and largely for the same reasons. As China seeks to modernize and become prosperous through rapid growth, it has been unable to develop the controls and enforcement necessary to prevent similar problems from occurring. While increasingly prosperous, China's regulatory structure is complicated and has been an impediment with respect to governance, risk management, and compliance. This structure will be explored next.

2.1 China and its Structure

The tumultuous changes that China has experienced in the last 50+ years, culminating in the unprecedented growth of the last two decades, have resulted in a fragmented system of regulatory control, dominated by top-down mandates from the government that are often divorced from the practical contexts they are attempting to address. Although the government in Beijing continues to set the agenda for the country, it delegates a large part of the implementation of regulatory policies to local officials (Economy, 2007). This often results in both arbitrary and lax enforcement of policies. At times local government officials will not enforce the policies due to self-interest (Economy, 2007). This interest could be financial or personal, but either way can lead to them ignoring the mandates from Beijing. Ogus (2004) noted in research examining primarily the United Kingdom and the United States:

> Although regulation was predominantly an act of central government, enforcement was a matter for local administration and often ineffective. Legislation was thus as much concerned with the symbolic function of appeasing those aggrieved or responding to political demands as it was with the pursuit of instrumental goals. (p. 6)

While his research was not an examination of China, it does have particular relevance to modern day China and problems it is facing given the role local officials have in enforcement and the increased political attention regulation has garnered over recent years in China.

Additionally, China has been growing not only in one region or one sector, but in many regions and many sectors (MacFadyen, 2008). This has only served to compound the problem of ensuring regulatory compliance with the rule of law as it is inherently difficult for a central government to keep pace with a rapid multi-dimensional expansion. Not only would the central government have to consider the possibility that different sectors have different needs, but that different regions may have different needs as well. Additionally, it is questionable whether a central bureaucracy is best suited at prescribing technical standards for such a vast array of local conditions (Ogus, 2004, p. 11). This is arguably what has led to many of the problems seen in production in China over recent years and will be discussed in the next section.

2.2 Problems with production in China

The results of arbitrary and lax enforcement can have devastating consequences. Over the years, U.S. toy manufacturers have increasingly moved their factories overseas to China in order to save money, primarily on labor costs. Currently, over 90 percent of toys that are sold in the United States are manufactured elsewhere—85 percent in China (Field, 2008, p. 12). In 2007 lead was discovered in several toys amongst many different brands; other defects were also noted. Approximately 25 million toys were recalled as a result of these different problems. While the actual health risks from the exposure to these toys is not yet fully known, there were additional products made in China that year that also posed significant risk to people and animals as well. Defective tires, contaminated toothpaste, and perhaps most well-known was pet food that contained an industrial chemical called melamine were all made in China that year (O'Rourke, 2008, p. 40). Several animals died as a result of the contaminated pet food. The melamine was used to give the appearance of increased protein content in the pet food.

In 2004 around 50 infants died when physicians and parents mistakenly thought their bloated hands and faces were signs of overfeeding when it was really due to protein deficiency (Kahn, 2007). Some small factories in the central part of China produced milk formula for infants that lacked protein. According to Ogus (2004), there is little incentive to disclose information on quality (p. 134). He further noted: "…managers have an incentive to suppress unfavorable information about their firm's 'quality'" (p. 140).

In 2008 it would become evident that the use of melamine in manufacturing continued despite the awareness that was brought to it by its use in pet food and the devastating consequences thereof. The potential rewards were simply too great to pass up with the associated costs minimal given the arbitrary and lax enforcement of regulatory policies. However, the 2008 tainted milk scandal was different from that in 2004 as it involved a top 500 enterprise in China with 18 percent of the milk powder market in 2007 ("World," 2008, p. 45). Other producers were also implicated and panic ensued. At least 4 babies died and approximately 94,000 others were sickened ("Secretive," 2008). While there are differences between intentional criminal activity for increased profit and 'simple' neglect to limit overhead, these differences are minimal from a conceptual standpoint and the end results are often indistinguishable from one another.

2.3 The Response of the Chinese Government

The reaction from the Chinese government to the 2008 melamine milk scandal was mixed. An I-class response was instituted, which consisted of leaders from the Ministry of Health, as well as the functional departments of national and local governments ("World," 2008, p. 45). Additionally, any "famous-brand" product guilty of putting melamine in their milk would be stripped of its brand status (p. 46). Nonetheless, the World Health Organization (WHO) was noted to have difficulties in obtaining up to date information on the number of children sickened by the crisis ("Secretive," 2008). Lawsuits are heavily discouraged by the Chinese government as they are seen as a political threat, which eliminates one additional avenue for recourse ("News," 2008, p. 27). Lawyers in some of the melamine lawsuits were pressured to pull out by Chinese officials ("Tainted," 2008, p. 31). Media have also been banned from reporting bad news at either the local or national levels (p. 31).

Top-down mandates will continue to result in arbitrary and lax enforcement in the current cultural, business, and regulatory environment in China. As Masters (2008) noted, "…there are always weak points in the security of any supply chain, as well as potential weaknesses in any system of checking" (p. 25). Weidenmier and Ramamoorti (2006) also noted that supply-chain is one of two enterprise resource planning (ERP) subsystems with the greatest

security and control risks (p. 209). The problem is that the system in China is primarily reactionary and therefore largely ill-equipped to proactively encourage quality control measures within organizations. In one instance the Chinese government may try to cover-up a scandal, but in another such as when the former head of the State Food and Drug Administration was convicted of taking bribes in order to approve different drugs it may overreact by sentencing him to death (MacFadyen, 2008). According to Ogus (2004):

> Law, as the primary instrument of control, was part of the contradiction: to be consistent with the rule of law, regulatory measures had to assume a level of generality and yet that very generality rendered them incapable, without the *ad hoc* exercise of discretion, of dealing with rapidly fluctuating conditions and events. (p. 57)

In other words, reactionary systems do not work and ultimately lead to failure. A framework that is dynamic, that recognizes the rapid change in conditions that takes place, and that is structured to act in a proactive way is much more likely to be successful and prevent catastrophic events from occurring in the first place.

While such events may not always lead to death, there remains a high likelihood that they will be costly to many stakeholders (e.g. organizations). The latest such event to come to light is defective drywall made in China and sold in the United States during the housing boom. The drywall is believed to be omitting toxic chemicals which are causing damage to products in their homes in addition to posing potentially significant health risks for inhabitants (Corkery, 2009, p. A3). Some builders have had to replace all of the drywall in these homes at significant cost.

The rich history of China, its unprecedented growth, problems in production, and its political structure provide a great opportunity for a GRC framework implementation that can be beneficial for many stakeholders. A discussion on some of the benefits of a GRC framework implementation in China follows.

3. GRC Framework and China

In this section we begin by providing some brief examples of prior uses of the Plan-Do-Check-Act (P-D-C-A) found in GRC frameworks. This is followed by a discussion of some of the benefits a GRC framework implementation within organizations in China can have for various stakeholders. Next, we place into context the tainted milk scandal and toy production problems in China with respect to a GRC framework implementation. Finally, we discuss the implementation of a GRC framework in China.

3.1 Prior Uses of the Plan-Do-Check-Act Approach Found in GRC Frameworks

GRC frameworks are found primarily in the business, legal, and information security sectors. A Deming-cycle learning organization structure implementation of the GRC framework would be most advantageous. Its basic approach of Plan-Do-Check-Act (P-D-C-A) has been recognized as valuable by inclusion in ISO 9000 (process management) and ISO 27000 (information security management), U.S. Federal HIPAA medical record information security rules, the U.S. Federal Gramm-Leach-Bliley information security rules, and the Federal Trade Commission's (FTC) ongoing program of requiring Internet merchants to implement appropriate security under its power to police unfair and deceptive trade practices. GRC frameworks and one of its core approaches (P-D-C-A) has been used repeatedly over the years because of the many benefits it provides to organizations as well as a multitude of stakeholders.

3.2 GRC Benefits and Stakeholders

The implementation of a Governance, Risk Management, and Compliance (GRC) framework within organizations in China can be beneficial on multiple levels and to many stakeholders. Specifically, it can:

- Establish protocols that measure internal compliance with policy
- Collect compliance data
- Increase transparency
- Increase efficiencies
- Increase quality
- Increase security
- Provide continuous feedback

These benefits are not limited to a single stakeholder. Rather, it is quite conceivable that all stakeholders will benefit from the successful implementation of a GRC framework. This includes the Chinese government, primary

organizations, local governments, local, national, and regional regulating bureaus, businesses outsourcing work to organizations (including international firms), and end consumers. The number of benefits a successful GRC framework implementation can have for various stakeholders is quite astounding. When placed in the context of the tainted milk scandal and toy production in China, it helps to further illustrate how a GRC framework implementation within organization in China could have helped mitigate some of the problems faced over recent years.

3.3 The Tainted Milk Scandal and Toy Production in China

With the recent tainted milk scandal, transparency has garnered new interest as it relates to maintaining the quality and safety of products. According to Strunin (2008), "To maintain product quality and safety, brand owners must maintain transparency and traceability throughout the supply chain" (p. 31). MacFadyen noted that China has made some progress towards increased transparency, which is why businesses continue to find China an attractive market to enter when comparing the risks against the benefits (MacFadyen, 2008). However, increased transparency is also needed at the organizational level. The GRC framework would create an environment in which increased transparency could thrive at the organizational level as well.

The tainted milk scandal was likely not profitable for the businesses implicated. The Mengniu joint venture shut down production for approximately a month (MacFadyen, 2008). The Chinese government is supporting a takeover bid by Sanyuan of Sanlu, the company at the forefront of the scandal (Lu, 2009, p. 29). Once word was received that Sanyuan was melamine free its stock price rose by 64.4 percent in six days and overnight demand skyrocketed to eight times production capacity (p. 28). Thus, the business that did not use melamine was *rewarded* financially.

Implementation of the GRC framework at these organizations could have mitigated the damage done by the corrupt leaders or even possibly prevented any milk from becoming tainted in the first place. According to Ogus (2004), "'Compliance' implies conforming to the law as a result of persuasion and negotiation before the event; 'deterrence', on the other hand, depends on penalizing offenders for offences already committed and thus deterring further violations" (p. 95). Compliance can provide ample benefits for an organization and is part of being proactive.

Nestlé also had products made in China that were said to test positive for melamine (Roberts, 2008). In response to the tainted milk scandal, they opened a new research and development center in Beijing that includes advanced product testing machines. It is Nestlé's second research and development facility in China ("World," 2008).

Reputation is important and maintaining a brand's image is essential in a competitive environment. Mattel, Inc. took some of the responsibility with respect to design flaws for small magnets that would easily become dislodged (Brandt, 2008, p. 26). These toys were made in China and were recalled. Other toys Mattel, Inc. recalled were due to problems in the supply chain with unsafe levels of lead used in the paint. One of the main problems these examples illustrate is how organizations have to be proactive instead of reactive.

3.4 Implementing a GRC Framework in China and Past Implementations

The implementation of a Deming-cycle GRC framework in an organization would create a much more dynamic learning organization that is proactive instead of reactive. While the Chinese government has taken some responsibility for the tainted milk scandal to the surprise of many (Raghupathi, 2007, p. 31), supporting GRC framework implementations within organizations in China can go a long way to preventing the problems from occurring in the first place. It is believed that over time as the GRC framework is implemented in various types of organizations the culture around compliance will begin to shift towards proactive dynamic learning organizations with an environment that is welcoming to continuous feedback from all stakeholders. As a result of that feedback adjustments can be made to internal policies.

This dynamic iterative process is in stark contrast to the traditional *democratic* policy making process used in the United States to makes laws and policy. The more traditional process involves notice and comment on draft rules, hearings, litigation to contest enforcement decisions, etc. A traditional approach such as this does not work in the information security field or in any area in which innovation is occurring rapidly as it has been in China. The more technology develops the more difficult it will be to monitor organizations that use these technologies (Ogus, 2004, p. 95). As Ogus (2004) noted, "Nor should it be forgotten that American-style procedures generate substantial administrative costs and delays" (p. 114). Interestingly, many organizations that have a significant history of

working with governmental contracts in the United States also have a considerable amount of experience with successful GRC framework implementations of their own.

There have been some implementations of GRC type frameworks within organizations in China over the past 30 years; most notably, the system known as lean production (LP) (Chen & Meng, 2010, p. 54). Some organizations have benefited greatly from it, while most have not met the goals they had set for themselves (p. 54). Chassis Branch of FAW was able to reduce its "work-in-process" by 70 percent through the implementation of LP (p. 54). Chen and Meng (2010) noted that while there are some success stories, the number of organizations disappointed with their results through LP implementations significantly outnumbers these success stories (p. 54). The authors noted four main causes for the organizations that failed to meet their full potential with LP. First, these organizations would often focus only on the LP tools without realizing that business strategy and buy-in from both management and employees are essential. Second, these organizations have often hoped for quick results when this is not the norm. Toyota developed TBP over a period of decades for the specifics of their company, circumstances, and culture. While it will not take decades for organizations in China to achieve results, it will generally require more than a couple of months. Next, some of the organizations were enthralled with the successes of the LP implementations by other organizations and would do what they could do emulate them in every way possible. This was problematic since cultural considerations must be taken into account at all levels; this includes management philosophy (p. 54). Finally, many of the TP "experts" within the organizations only understood LP at a superficial level. In other words, they may have known much of the "what", but lacked the essence behind LP and thus failed to see the big picture. In order for any GRC framework to be successful in China or elsewhere, these potential roadblocks to success must be considered at every step of implementation. In the next section we discuss a GRC framework prototype that has its roots in one such organization, Microsoft.

4. GRC Framework Prototype

During 2008 the Governance, Risk Management and Compliance (GRC) framework prototype was developed as a graduate research project under the guidance of industry, legal experts, and faculty from the Information School at the University of Washington. When properly implemented this framework and associated set of protocols and training programs will permanently change a chaotic organization culture into one aligned with internally developed governance policies driven by externally mandated laws and regulatory regimes. The purpose is to leave behind a sustainable infrastructure that reflects the rule of law.

External to an organization are the legal and regulatory regimes, which influence the development of the organization's policies designed to reflect compliance to these regimes. The internal policies implemented through the GRC framework result in organizational alignment to mandates from the regulatory regimes, thus embedding compliance. If a GRC framework is not used then the controls, feedback, and audits that would otherwise be institutionalized cannot be and permanent alignment is not assured. As a result the rule of law remains a concept outside of the organization, without the participation and involvement of all those within the organization.

According to Weidenmier and Ramamoorti (2006), IT governance was not made a high priority in the past and instead an incremental approach was taken with respect to compliance; an integral approach is more effective (p. 211). They noted, "Embedded controls ensure compliance at the time of the business process entry, making employees systematically follow governance directives, ultimately changing the organizational culture" (p. 211). Mitchell (2007) also noted the importance of not treating GRC as an afterthought, but rather beginning the entire process with GRC in mind at the forefront (p. 281).

An outline for the GRC framework prototype is found in Appendix II. While it has not yet had the benefit of being tested itself, the GRC framework prototype was developed in consultation with experts at Microsoft and it is based on their GRC framework that has been tested both in the United States and internationally over multiple years, including China. This includes new acquisitions of various size companies with differing cultural, regulatory, and economic compositions. As will be discussed in the next section, the results have been promising.

5. GRC Implementation Examples

GRC frameworks have been implemented in various types and sizes of organizations throughout the world since the last half of the twentieth century. The importance they have had for some of these organizations would be difficult to overstate. In this section we briefly discuss two examples of GRC framework implementations. The first one, Toyota, is in many respects the pivotal example as it ushered in a new era of manufacturing with some of

the most significant changes made since the assembly line was first introduced. The GRC framework Toyota developed is used in organizations throughout the world with proven success. Thun et al (2010) studied 188 manufacturing organizations and found that as they implemented a greater number of Toyota's processes to a larger degree they showed a higher level of performance with respect to key indicators, i.e., quality, time, and cost. The second example is Microsoft. The GRC framework prototype has its roots in the GRC framework developed and currently used by Microsoft. While developed during different time periods and for different types of organizations, both have shown promising results.

5.1 Toyota and Deming

Toyota neared bankruptcy in the 1950's (Takeuchi, Osono, & Shimizu, 2008, p. 99). During the same time period Deming, a statistician, was sent by the U.S. government to Japan to help them with their census (Luchansky, 2008). The belief early on with Japanese products was that they were cheap and of poor quality (Luchansky, 2008). Deming gave a series of lectures to industry leaders that were considered particularly relevant and timely. There were a couple of key takeaways from these lectures. According to Luchansky (2008), "…if you focus on quality, over time, quality will tend to increase and costs will fall; if you focus on costs, over time, quality will tend to decrease, causing costs to rise." The other one involved a culture of continual improvement: plan, do, check, act, and continuously repeat.

Toyota took both of these major concepts to heart and implemented them. They used the Plan-Do-Check-Act (P-D-C-A) and refined it into the Toyota Business Practices (TBP) process (Takeuchi, Osono, & Shimizu, 2008, p. 101). This is quite interesting and appropriate that a process for continual improvement led to a better process (for them and their particular circumstances) for continual improvement. The eight step TBP process is a path that gives employees the ability to challenge the status quo. The eight steps are: "clarify the problem; break down the problem; set a target; analyze the root cause; develop countermeasures; set countermeasures through; monitor both results and processes; and standardize successful processes" (p. 101).

Toyota makes some of the best automobiles at the lowest costs in the world (Takeuchi, Osono, & Shimizu, 2008, p. 96). Thus, their implementation of such a system is worth exploring as are the other reasons behind their successes. They invest heavily in their people and seek ideas from everywhere and everyone (p. 98). Constructive criticism is not only allowed, but it is encouraged (p. 99). It makes the company and its products better. Communication is also essential. This is more than simple top-down communication. According to Takeuchi, Osono, & Shimizu (2008), "Toyota fosters a complex web of social networks because it wants 'everybody to know everything'" (p. 99). Along with this open communication, goals are kept broad—both of these working together help ensure employee creativity (p. 100).

In addition to goals being kept broad, employees are given guidelines to follow instead of strict rules (Takeuchi, Osono, & Shimizu, 2008, p. 102). This flexibility allows for employees to comply with the intent behind a specific guideline while not being bogged down by the detailed specifications of certain mandates that may not pertain to the particular conditions under which they operate. The outcome is greater overall efficiency, improved morale, and greater compliance.

Although Toyota has a long track record of success in building quality vehicles in an efficient manner, recent history shows they are not immune to problems in manufacturing. In early 2010, evidence began to surface in the public sphere that there were problems with the accelerator pedals in several of Toyota's models. Several deaths have even been attributed to the defective parts (Maynard, 2010). Their reputation has been impacted negatively, which can be difficult to quantify (D. Katz, 2010, p. 31). Several industry experts have suggested the problem that led to the defective parts was not with TBP, but rather with an incomplete and haphazard implementation of it within certain business components of the company (J. Katz, 2010, p. 20). Specifically, parts were standardized across several different models and the implementation of TBP was focused primarily on the manufacturing side. The standardization led to one defect being carried over into several different models instead of being limited to a single model. Ironically, part of the basis for the development of TBP in the first place was to allow for a variety of models in low volumes (Nambiar, 2010). Additionally, with implementation being focused primarily on the manufacturing side, the engineers who designed the parts were left out of the process to a large extent. The result is a flawed design that may be manufactured quite well, but with a detrimental outcome. Therefore, a full implementation is essential to ensuring success.

While Toyota has been utilizing a GRC framework in one form or another for over 50 years with by and large great success, Microsoft has shown that signs of success can appear in a relatively short time period.

5.2 Microsoft and Trustworthy Computing

In 2002 Microsoft announced an initiative known as Trustworthy Computing (TwC) (Ashford, 2009). A large part of the aim was to transform the organization to one in which risk management was at the forefront of everything they do, most notably writing software code. No longer would it take a backseat to the features desired in the software, or get pushed aside as a result of marketing deadlines.

Increased transparency is also a large part of the initiative. According to George Stathakopoulos, general manager for TwC, the results thus far have been promising (Ashford, 2009). The number of infections per thousand computers decreased from 35 to eight from Windows XP to XP SP2. There was a further reduction from Vista to Vista SP1 from four to one (Ashford, 2009). As early as three years into the TwC initiative, security experts began to notice improvements in Microsoft products (Foley, 2005). Thus, the GRC framework implementation at Microsoft has shown promise in its first decade of implementation. Although GRC frameworks have the capacity to improve an organization in a multitude of ways as these two examples illustrate, there are special considerations that should be taken into account.

6. GRC Considerations

Various types of GRC frameworks have been employed by organizations throughout the world to different degrees for several years now. Their experiences show why a GRC framework implementation can prove beneficial for organizations in China. They also provide some helpful lessons that can guide such an implementation. In this section we discuss how GRC framework implementations have historically been viewed as an overhead item, but how this has begun to shift over recent years as evidence continues to mount that its benefits outweigh its costs. Next, we discuss GRC frameworks in the context of international organizations and the unique opportunities and challenges posed as a result. Finally, there are cultural issues to consider when implementing a GRC framework. This is explored in the context of a specific example.

6.1 GRC Viewed as an Overhead Item

Early on GRC in practice was viewed more as an "overhead item" than something worthy of primary attention or resources (Raghupathi, 2007, p. 95). The prevailing concern was return on investment (ROI) for money spent on information technology, which eventually is what led to the financial and legal collapse of such entities as WorldCom and Enron (p. 94). The approach was neither holistic nor comprehensive. Some organizations do not even create "risk committees" until after there has been a compliance issue significant enough to warrant one ("A Systematic," 2008, p. 66). Some of the difficulty may be that in general it is more difficult to quantify benefits compared to costs (Ogus, 2004, p. 160).

The view that GRC is simply an overhead item has begun to shift in recent years with proven benefits for organizations and those they have an effect on, either directly or indirectly. The costs associated with one company to comply with Sarbanes-Oxley Section 404 declined each year between 2004 and 2006 (Hall, 2008, p. 16). The reason cited by an industry expert is the more comprehensive approach taken by this company in approaching GRC. Additionally, organizations are spending more money on GRC as well with an expected increase of 7.4 percent in 2008 (Pessin, 2008, p. B5B). Organizations are adjusting and realizing from past experiences that it is more cost efficient to be proactive and comprehensive in their approach to GRC: "'In this economic climate, companies can no longer focus solely on reactive spending to meet each new regulation,' said John Hagerty, vice president and research fellow at AMR Research" (quoted in [Pessin, 2008, p. B5B]). Several organizations for which the Sarbanes-Oxley Act did not even apply to have enacted several of the provisions of the act in order to strengthen their internal controls (Savage, Norman, & Lancaster, 2008, p.75).

One of the concerns over complying with Sarbanes-Oxley and similar regulations has been duplication (Raghavan, 2007, p.182). Nonetheless, a survey of corporate directors found that 70 percent of them felt it improved board governance; 60 percent indicated that it has had a positive impact on their companies (p. 182). This includes such things as improved business processes. Compared to their non-adopting peers, such companies have been rewarded with increased stock prices and reduced compliance costs over time (p. 182). Streamlining enterprise risk management to address various regulations can provide an organization with a competitive advantage (p. 183). Mitchell (2007) noted that integrated GRC will result in: 1) "improved information quality"; 2) "reduced errors", and 3) "reduced costs" (p. 285). One survey found that "…84 per cent of those who have completed integrated

GRC projects realize results that meet or exceed expectations" (p. 285). The GRC framework prototype is designed with these goals in mind.

6.2 GRC and International Organizations

In addition to a comprehensive and holistic approach to GRC, many organizations also operate internationally and thus have to contend with several laws outside the jurisdiction of its headquarters. Most notably, European Union (EU) and United States laws (Walker, 2006, p. 72). However, the GRC framework implementation for the organization does not have to be the same in each country it operates. According to Walker (2006) it can be based on a risk assessment on such factors as the categories of employees specific components would apply to and the particulars of each country (p. 71). It is conceivable that much of the GRC framework implementation for the organization would be the same for all of the countries it operates in while some other components would be more fluid. In addition to the flexibility needed due to varying laws, different countries often have different cultures that can change some of the GRC framework implementation dynamic.

6.3 Cultural Issues

An understanding and respect of cultural issues can be critical in a country such as China. In 2006 there were over 400 Starbucks coffee shops in the country (Han and Zhang, 2009, p. 395). The Forbidden City is a museum that represents the "…Chinese civilization over its long imperial history, and is regarded as the cultural symbol of China" (p. 395). In 2000 the management of the Forbidden City invited Starbucks to open a coffee shop there. A conflict ensued between what epitomized "old" and "new". Starbucks had been flourishing in China, beginning with the upper class and working its way into the middle class markets (p. 397). Eventually, a Web-based campaign led by a well-known news anchor would lead to the removal of Starbuck's Forbidden City coffee shop (p. 395). Starbuck's attempts to appease the Chinese people by doing such things as designing the exterior of its coffee shop to resemble the other Forbidden City buildings did not work (p. 399).

Thus, there are cultural issues in China that have to be taken into account. This includes the political climate, still developing governmental oversight and enforcement, and organizational culture. Some components may be different based on cultural considerations. As Walker (2006) noted, "Cultural differences can be an enormous hindrance to the effective implementation of a global compliance programme" (p. 77). It would therefore be important when crafting GRC policies to have mechanisms in place for receiving input that is sensitive to the culture in which it is meant to be implemented. The GRC framework prototype discussed here has this as an integral mechanism built into it. Feedback from all stakeholders is encouraged, which allows for a very organic way in which cultural differences can enter the fold.

The roots of the GRC framework prototype come from an international corporation that has operated all across the world, including China. It has implemented its GRC framework successfully both in its offices as well as in the offices of companies it has acquired. This has occurred both inside and outside of the United States, including China.

Public Relations literature also acknowledges the importance of taking culture into account. In a discussion of the circuit of culture theory, Curtin and Gaither (2005) noted: "A growing body of literature in the area of international practice, however, stresses the need to address and incorporate local cultural norms and practices to allow for a degree of cultural relativism" (p. 105). However, as the authors also noted this should not be taken to an extreme and in essence is just one part of the overall picture. If cultural indexes or indicators are relied on too much this can lead to stereotyping, which would be going against the primary objective of taking culture into account in the first place. The GRC framework prototype is not designed to enter a situation with preconceived notions; rather, it is structured in such a manner as to listen to various stakeholders and determine what their needs are and what cultural issues may need to be taken into account. As Chen and Meng (2010) noted, failing to take local culture into account (including management philosophy) has been one of the reasons why GRC frameworks have not been more successful in China (p. 54).

7. Conclusion

A lack of institutional and organizational measures necessary for effective governance, risk management, and compliance is not unique to China. However, Chinese organizations and organizations that choose to operate within

China present us with a special opportunity given the history of compliance issues and the complex dynamics involving the regulatory, political, and economic traditions of the Chinese people. The need for the GRC framework as articulated here is significant. It is a dynamic process that respects the cultural values of the Chinese people while allowing for real improvement in governance, risk management, and compliance. These improvements can serve to not only be profitable for the organizations in which they are implemented, but also prove beneficial for the Chinese government, partner organizations and stakeholders, regulatory agencies, and as shown in what the consequences of poor GRC can have—it can inevitably serve to save lives.

8. Appendix I – Glossary

Deming-cycle
W. Edwards Deming is the U.S. industrial engineer who taught Toyota how to do total quality management in the 1950's. The Deming-cycle is known as Plan-Do-Check-Act (P-D-C-A); once completed initially the cycle will be continued indefinitely to ensure a self-sustaining and continuously improving quality program (Beckford, 2002, p. 67). Another variation of P-D-C-A is known as Plan-Do-Study-Act (P-D-S-A) (Landesberg, 1999, p. 61).

Federal Trade Commission (FTC):
The FTC was created in 1914 with an original purpose of preventing competition in commerce that was deemed unfair ("About the Federal," 2009). This included the breaking up of monopolies and similar entities. Congress would later expand the role of the FTC in 1938 with a law broadly precluding what it termed "unfair and deceptive trade practices" ("About the Federal," 2009). Currently, the FTC is responsible for the administration of a variety of consumer protection laws (e.g. Equal Credit Opportunity Act) ("About the Federal," 2009).

Food and Drug Administration (FDA):
The FDA began in 1862 with its roots in the U.S. Department of Agriculture (Swann, 2009). Other than meat and poultry, the FDA's jurisdiction is broad and includes most all other food items, drugs (human and animal), animal feed, medical devices, among other things accounting for 25 percent of all consumer spending (Swann, 2009). In 2001, the FDA had a budget of $1.294 billion and a staff of approximately 9,100 (Swann, 2009).

ISO 9000
ISO (International Standard Office) 9000 is also known as "Quality Management and Quality Assurance Standards" (Imberman, 1999, p. 11). The standard was created in 1987 by the ISO of the European Union with the goal of achieving zero-defect products (p. 11). In addition to OEM's (original equipment manufacturers) having to meet the standards, all suppliers to the OEM's were also required to meet the standards. Some of the key components of ISO 9000 include: "a comprehensive quality manual"; "a detailed procedural manual"; "work instructions," and "records" (p. 12).

ISO 27000
ISO (International Standard Office) 27000 is a series of different standards related to information security and are collectively known as the ISO 27000 series ("An Introduction to ISO," 2009). The numbering for these standards begins with ISO 27001.

Jungle, The
The Jungle is a pivotal work by author Upton Sinclair written in 1906. The intent of the author was to increase awareness of the conditions of workers and ultimately have Americans embrace socialism ("Of meat," 2006, p. 32). While this did not happen, its attack on the meatpacking industry and the conditions thereof prompted Congress to pass the first food-safety laws in the U.S. The attention this work brought to the public along with other notable incidences is ultimately considered to be the catalyst for the creation of the FDA.

Plan – Do – Check – Act (P-D-C-A)
Please see Deming-cycle.

U.S. Federal Gramm-Leach-Bliley
The Gramm-Leach-Bliley Act of 1999 is a federal law that became law on November 12, 1999 (Boehne, 2000, p. 4). It is also known as the Financial Modernization Act. The main component of the act was to repeal the Glass-Steagall, which had established a separation between securities underwriting and commercial banking since 1933 (p. 3). While this was a major move towards the deregulation of the banking industry, the Act also contained specific provisions to protect the privacy of consumers as it recognized the increasing role technology would play in consumer banking (p. 13).

U.S. Federal HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that was passed by Congress in 1996. It was designed to protect the privacy rights of individuals as it relates to their personal health information with health care providers, health plans, and clearing houses (Guthrie, 2003, p. 143). Within the Privacy Regulations there is a "minimum necessary" standard as is relates to disclosure. According to Guthrie (2003), "Covered entities must make 'reasonable efforts' to limit the use, disclosure, or request of protected health information to what is minimally necessary" (p. 147).

World Health Organization (WHO)

WHO is in charge of setting and coordinating health policy matters within the United Nations system ("About WHO," 2009). This includes providing technical support when needed, determining the research agenda, and keeping track of health trends across the world ("About WHO," 2009).

9. Appendix II – GRC Framework

GRC frameworks consist of several steps with varying levels of detail to help ensure success at each step. The GRC framework briefly outlined here is the one developed as part of graduate research project under the guidance of industry, legal experts, and faculty from the Information School at the University of Washington.

In the first part of this section, we discuss the importance of the sponsors engaging with the customers. The sponsors are those assisting the person or people from an organization in the possible implementation of a GRC framework (e.g. University of Washington researchers), while the customers are the individual or a unit that initiates the request for a needs assessment and/or GRC framework implementation. Next, we discuss how the scope of work is determined between the sponsor and stakeholders. Afterward, a risk universe document is developed in collaboration with the stakeholders through various techniques. Once this has been accomplished then risk management planning can ensue. This is discussed in addition to some of the ways in which China can benefit by implementing the GRC framework prototype.

9.1 Engage with Customers and Identify Stakeholders

There is no one size fits all GRC program that will work equally well for all organizations. Thus, one important feature of this GRC framework is that a needs assessment takes place prior to implementation. While the purpose of this initial engagement with the customer is primarily for the sponsor to collect information, it is also important that any questions can be answered as well since it will develop a relationship of trust and collaboration right from the outset.

Some of the information that will inevitably be collected during this process informally is the identification of key stakeholders. This will be further refined later in a more formal setting as it is essential to know both potential allies and those that may pose challenges to the project. Additionally, the partner organization can help identify the stakeholders with particular resources (e.g. technical) important for success. While some stakeholders will appear as more critical, engaging with all stakeholders (on-boarding) is essential since establishing rapport early on will help with overall buy-in to the project concept.

9.2 Determine Scope of Work

Once the stakeholders are identified through the formal process, the sponsor and stakeholders will determine the scope of work to be done. This would include the requirements, deliverables, success measures, team roles, among others. Through this process a Statement of Work (S.O.W.) draft will be created. Since a significant reason behind the implementation of a GRC framework is to address the issue of top-down mandates and the resulting negative effects, inherent within this stage is a review of the scope of work and S.O.W. between the sponsor and stakeholders. This includes an opportunity for questions to be asked and answered. Revisions may be made until a final version of the S.O.W. is agreed upon and signed.

9.3 Develop Risk Universe

In order to develop accurate risk questions, the team needs to take a glimpse of the operational framework of the organization. The questions that are developed may help identify the objectives, changes to the current processes, the extent to which the project is going to add value to the business, among many other similar things. Tools such as surveys, questionnaires, face to face interviews, and team brainstorming can be used to help formulate these questions.

An initial meeting will take place consisting of all the team members, stakeholders, governance committee and other units that will potentially be impacted by the project. With this information and the information previously acquired, a risk universe document will be created. The risk universe document is a list of all the units in the organization that will play a direct role to the project and units that will be impacted by it. The stakeholder(s) will verify the accuracy of the document and may make changes as appropriate.

9.4 Risk Management Planning

After verification of the risk universe document, risk management planning can take place. Similar tools can be used to compile questions here as was noted above with respect to developing risk questions (e.g. surveys). Each response to the questions compiled is a possible risk.[1] The responses themselves are compiled, analyzed, and categorized by risks (events). Likelihood scores of each risk occurring is then given, such as 1-5 in which 1 is least likely the risk is going to happen and 5 as the highest possible chance the risk will happen (low to high scoring can also be used).

In addition to the stakeholder(s) verifying the likelihood scores, they will also assign impact scores and verify those. Impact scores can be based on a number of considerations, but commonly include such things as: monetary impact, loss of reputation, loss of business, disruption of business, and/or legal/compliance.

Based on both the likelihood and impact scores the team is able to organize each risk accordingly. This is called risk stacking and can be represented graphically various ways (e.g. heat map). The current controls that are in place to help mitigate risks should be identified and their characteristics noted (e.g. maturity and procedures). An analysis based on this information will serve to inform whether current controls are enough or if new controls are needed. This information would be presented to management, including the cost associated with new software/hardware, training, disruption of processes, etc. Management may accept the recommendations, keep the status quo, or something in-between.

Upon receiving management response, a detailed list of activities to accomplish the implementation of each controls accepted is needed. The final deliverable for this step is the action plan that is submitted to management for them to assign resources. Each activity with assigned resources will now be treated as separate projects.

9.5 China and the GRC framework

As China continues its rapid growth and fast-paced innovation, it will greatly benefit any organization in China to implement the GRC framework if they perceive the need to: 1) improve their outsourcing partnerships with Western organizations by aligning with the legal and regulatory structures that their partners must adhere to, or 2) improve their alignment with international standards or domestically mandated regulations.

[1] Current controls that may mitigate risks are not considered at this stage. Likelihood and impacts scoring should assume that none of the current controls are in place.

10. References

"A Systematic." (2008). "A Systematic Approach to Risk." *Directorship,* 34(3), 66-67.

"About the Federal." (2009). "About the Federal Trade Commission." FTC. Retrieved: 4/18/09, from http://www.ftc.gov/ftc/about.shtm.

"About WHO." (2009). "About WHO." Retrieved 4/18/09, from http://www.who.int/about/en/.

"An Introduction to ISO." (2009). "An Introduction to ISO 27001, ISO 27002....ISO 27008." Retrieved 4/18/09, from http://www.27000.org/.

Ashford, W. (2009, March 4). "Microsoft labels trustworthy computing a success." *Computer Weekly.*

Beckford, J. (2002). "Part two: The quality gurus: Chapter 6: W. Edwards Deming." *Quality, (Routledge)*, 65-83.

Boehne, E. G. (2000). "Financial Modernization: Vastly Different or Fundamentally the Same?" *Business Review, (Federal Reserve Bank of Philadelphia)*, 3.

Brandt, D. (2008). "DIRECT from the SOURCE." *Industrial Engineer: IE,* 40(2), 26-33.

Chen, L. & Meng, B. (2010). "Why Most Chinese Enterprises Fail in Deploying Lean Production." *Asian Social Science,* 6(3), 52-57.

Corkery, M. (2009, January 12). "Chinese Drywall Cited in Building Woes." *The Wall Street Journal*, A3.

Curtin, P. & Gaither, T. (2005). "Privileging Identity, Difference, and Power: The Circuit of Culture As a Basis for Public Relations Theory." *Journal of Public Relations Research,* 17(2), 91-115.

Economy, E. C. (2007). The Great Leap Backward? *Foreign Affairs,* 86, 38-59.

Field, A. M. (2008). "Tough times for toys." *Shipping Digest*, 85(4439), 12-13.

Foley, J. (2005, February 14). "You Call This Trustworthy Computing?" *Information Week.*

Guthrie, J. (2003). "Time Is Running Out - The Burdens and Challenges of HIPAA Compliance: A Look at Preemption Analysis, the Minimum Necessary Standard, and the Notice of Privacy Practices." *Annals Health Law*, 12, 143-177.

Hall, M. (2008). "Cutting Compliance Costs." *Computerworld*, 42(25), 16-16.

Han, G. & Zhang, A. (2009). "Starbucks is forbidden in the Forbidden City: Blog, circuit of culture and informal public relations campaign in China." *Public Relations Review*, 35(1), 395-401.

Imberman, W. (1999). "The American Quest for Quality." *Business Horizons*, 42(5), 11.

Kahn, J. (2007). In China's safety woes, echoes of U.S. history. *International Herald Tribune*, Paris.

Katz, D. (2010, May 1). "What's a Reputation Worth?" *CFO*, 31-32.

Katz, J. (2010, April 1). "Lean Times for "'The Toyota Way'?" *Facilities and Operations*, 20-21.

Lu, E. (2009). "Radical Shifts in China's Milk Market." *China Today*, 58(1), 27-30.

Landesberg, P. (1999). "In the Beginning, There Were Deming and Juran." *Journal for Quality & Participation*, 22(6), 59.

Luchansky, D. (2008). "Manufacturing Culture." Retrieved 4/18/09, from http://www.articlesbase.com/management-articles/manufacturing-culture-567995.html

MacFadyen, K. (2008). "Reconsidering the 'Made in China' Brand?" *Mergers & Acquisitions: The Dealermaker's Journal*, 43(12), 26-27.

Masters, K. (2008). "Chain reaction." *Dairy Industries International*, 73(12), 25-26.

Maynard, M. (2010, January 28). "U.S. House Committee Plans Hearing on Toyota Recall." *The New York Times*.

Mitchell, S. (2007). "GRC360: A framework to help organizations drive principled performance." *International Journal of Disclosure and Governance*, 4(4), 279-296.

Nambiar, A. (2010, March 17-19). "Modern Manufacturing Paradigms – A Comparison." *Proceedings of the International MultiConference of Engineers and Computer Scientists*, (3).

"News." (2008). "News in Quotes." *Tibetan Review: The Monthly Magazine on all Aspects of Tibet*, 43(11), 27-27.

OCEG. (2009). "GRC Capability Model Version 2.0." *Open Compliance & Ethics Group*, Phoenix, AZ: Mitchell, S. & Switzer, C.

"Of Meat." (2006). "Of meat, Mexicans and social mobility; Immigration and "The Jungle"." *The Economist (US)*, 379(8482), 32US.

Ogus, A. I. (2004). *Regulation: legal form and economic theory*. Oxford; Portland, OR, Hart.

O'Rourke, M. (2008). "MADE IN CHINA." *Risk Management (00355593)*, 55(12), 40-40.

Pessin, J. L. (2008). "Companies Plan to Raise Compliance Expenditures." *Wall Street Journal - Eastern Edition*, 251(77), B5B.

"Premier." (2008). "Premier Wen Makes rare admission of gov't failing." *Tibetan Review: The Monthly Magazine on all Aspects of Tibet*, 43(11), 31-32.

Raghavan, K. (2007). "A survey of corporate governance and overlapping regulations in banking." *International Journal of Disclosure and Governance*, 4(3), 181-194.

Raghupathi, W. R. (2007). "CORPORATE GOVERNANCE OF IT: A FRAMEWORK FOR DEVELOPMENT." *Communications of the ACM*, 50(8), 94-99.

Roberts, D. (2008). "Nestle Combats China Food Scandals." *Business Week Online*, 25-25.

Savage, A., Norman, C. & Lancaster, K. (2008). "Using a Movie to Study the COSO Internal Control Framework: An Instructional Case." *Journal of Information Systems*, 22(1), 63-76.

"Secretive." (2008). "Secretive China refuses to cite nearly 94,000 tainted-milk victims." *Tibetan Review: The Monthly Magazine on all Aspects of Tibet*, 43(11), 31-32.

Sinclair, U. (1906). *The Jungle*. New York, Doubleday, Page & company.

Strunin, R. (2008). "Managing Brands through Supply Chain Visibility." *China Business Review*, 35(5), 30-33.

Swann, J. (2009). “History of the FDA.” FDA. Retrieved: 4/18/09, from http://www.fda.gov/oc/history/historyoffda/default.htm

"Tainted." (2008). "Tainted Milk Scandal." *Tibetan Review: The Monthly Magazine on all Aspects of Tibet*, 43(11), 31-32.

Takeuchi, H., Osono, E. & Shimizu, N. (2008). The Contradictions That Drive Toyota's Success. *Harvard Business Review*, Harvard Business School Publication Corp. 86, 96-104.

Thun, J., Drüke, M., & Grübner, A. (2010, January 26). “Empowering Kanban through TPS-principles—an empirical analysis of the Toyota Production System.” *International Journal of Production Research*.

Walker, R. (2006). "International corporate compliance programmes." *International Journal of Disclosure & Governance*, 3(1), 70-81.

Weidenmier, M. & Ramamoorti, S. (2006). “Research Opportunities in Information Technology and Internal Auditing.” *Journal of Information Systems*, 20(1), 205-219.

"World." (2008). "World in Brief." *Dairy Industries International*, 73(12), 10-10.