A Framework of Using Captive Insurance to Streamline IT Control and Compliance Management

Xia Zhao, University of North Carolina at Greensboro, 
x.zhao3@uncg.edu
Ling Xue, University of Scranton  
xuel2@scranton.edu

ABSTRACT

To streamline IT compliance management and reduce the compliance cost, large companies need to address the issues of incentive and information. This article proposes a framework which illustrates how companies can use a risk management approach - captive insurance - to resolve these issues and ultimately achieve cost-efficient IT compliance management.

1. INTRODUCTION

Companies are under regulatory pressure to ensure their IT security. For example, Sarbanes-Oxley Act (SOX) compliance has imperative implications for companies' information security practices, since most modern companies rely heavily on information systems to handle their financial information management. HIPPA (The Health Information Portability and Accountability Act) requires organizations to protect individuals' medical information. Gramm-Leach-Bliley Act requires financial institutions to maintain data privacy of their clients. California Information Practices Act SB1386 requires businesses to inform residents if their unencrypted personal information has been compromised. Regulations outside US include Canadian Privacy Act, which requires the protection of individual information, Basel II, which calls for internal control over information reporting for European companies, and Hong Kong Personal Data Privacy Act, which protects the privacy of living individuals regarding personal data. The compliance with multiple regulations further escalates the IT compliance costs for companies.

Companies are now seeking ways to reduce the cost of IT compliance. However, this task is challenging due to a number of reasons, including:

- The wide scope of IT control. Almost all IT aspects, e.g., hardware, software, storage, network, and even outsourced IT processes, are subject to the control requirements implied by at least some regulations;
- The inherent complexity of companies' IT systems. Different business units (BU) within large organizations often implement diverse IT systems. The identification and implementation of control objects for different IT systems are complex, and it is hard to apply the experience with certain IT systems to other systems;
- The lack of IT control guidance. Most regulations do not specify the effectiveness of IT control. For example, SOX requires companies to maintain the security and
integrity of their IT systems to support the financial reporting. But SOX itself does not define what are IT control objects and control processes. Companies have to rely on other standards, such as COBIT (Control Objectives for Information and related Technology) to configure their IT control. In many cases, companies, especially those small ones, have to configure control solutions based on their specific situations. This procedure inevitably incurs steep learning curve and large expenditures in external consulting services.

- The severe penalties of noncompliance. The penalties ranging from corporate fines, reputation loss to criminal charges for executives often force companies to commit redundant resources to ensure the compliance.

This article proposes a framework which illustrates how companies can use a risk management approach-captive insurance, to streamline their IT compliance management and reduce the compliance cost. The captive is an insurance company that a company or a group of companies establish to insure their business risks. Compared with the conventional insurance market, captive insurance allows companies to reduce overhead expenses in insurance and increase control over the insurance procedure. Using captive insurance, companies can reduce costs in IT control by transferring part of IT risks to the outside reinsurance or capital markets. More importantly, with captive insurance, companies can use insurance techniques to address another two key issues in IT compliance management, i.e., the incentive issue (i.e., how to align incentives of different business units) and the information issues (i.e., how to manage information to facilitate compliance management). The proposed framework illustrates how companies can enhance the efficiency of their IT compliance management by using captive insurance to resolve these issues.

The rest of the article is organized as follows. Section 2 reviews the incentive issue and information issue in IT compliance management, and discusses the importance of addressing these issues. In section 3, we introduce the basic concepts of captive insurance and explain how captive insurance can be used to address the incentive and information issues. Section 4 presents the details of the framework integrating captive insurance with IT compliance management. In section 5, we discuss how this framework can be applied in IT compliance involving outside partners. Section 6 discusses some issues regarding the operation of the captive. In section 7, we introduce some alternative risk transfer mechanisms that can substitute the captive insurance in our framework. Section 8 concludes the article.

2. Incentive and Information Issues in IT Compliance Management

Companies need to establish a sustainable framework to achieve streamlined IT compliance management. It is important to avoid importing an entire control framework from outside, or handcrafting a complete new control structure. The company needs to incorporate the best external standards and knowledge with their best IT practices developed in-house. Also, in order to maintain a reasonable level of
IT compliance spending, companies need to adopt a risk-based perspective to optimize the scope of their IT controls and focus on critical IT objects rather than all of them.

Companies can apply both top-down and bottom-up approaches in streamlining their IT compliance management and rationalizing the compliance expenditure. The focus in the top-down approach is to determine the IT control objects and policies from a holistic view of the whole corporation. In this process, companies can employ many external standards to formalize the corporate-level policies of control, testing and documentation. For example, general control guidance, such as COSO and PCAOB (Public Company Accounting Oversight Board), and more IT-oriented control standards, such as COBIT and ISO17799, all provide companies a checklist of corporate-wide control objects. In contrast, the bottom-up approach concentrates on discerning gaps between the routine IT systems and the compliance requirements at the process-level. Companies can rely on some existing guidelines, e.g., ITIL (Information Technology Infrastructure Library), to arrange appropriate IT practices at the process-level. However, in many cases, companies need to figure out solutions based upon their specific circumstances.

For large corporations with decentralized organizational structures, BUs and subdivisions are in charge of many process-level activities of control, such as documentation, testing, staff training, deficiencies reporting, remediation implementation, and the coordination with the overall corporate-level policies. Therefore, incentive alignment for individual BUs is imperative for the integration of top-down and bottom-up approaches. However, existing compliance standards and frameworks focus more on the control aspect of compliance management and do not sufficiently address the incentive issues in compliance. For example,

- Are BUs inclined to fully identify and truthfully report the deficiencies and weakness associated with their own IT systems?
- Do different BUs have adequate motivation to implement sufficient IT control of their own budget, especially when IT compliance requires redundant resources?
- Are different BUs willing to voluntarily help each other in IT control?
- What could motivate different BUs to immediately and accurately disclose any security breach, material change or vulnerability incident with their IT systems?

Without successfully resolving these incentive issues, the sustainability and cost-efficiency of IT compliance management is hard to realize.

In addition to incentive issues, the information issue is also imperative. In order to optimize the resource allocation and maintain a cost-efficient framework for IT compliance management, companies need a risk-based perspective to trade off between the effort in control, testing, documentation and the risks of vulnerability and non-compliance. This requires companies to quantify different types of risks and base their investment decisions on scientific cost-benefit analysis. Key resources should be devoted to the critical success factors and residual risks on non-critical factors can be
hedged through other mechanisms, such as the insurance mechanism discussed below. Companies have to continuously collect information on the status quo of their IT control, review the effectiveness and weakness of their control, evaluate the emerging problems and new challenges (especially the rapid technological changes) from the inside and outside, and adjust their control efforts. In shortly, companies need rigorous information collection and analysis to support their smart, adaptive and sustainable compliance management frameworks. The rest of the article illustrates how captive insurance can be used to address these incentive and information issues.

3. Introduction of Captive Insurance

3.1 IT Insurance on Conventional Insurance Market

Starting in 2000, slow steps have been taken by the traditional insurance market to develop cyber-insurance policies to cover IT risks. Existing policies include AIG’s NetAdvantage, Lloyd’s e-Comprehensive, Chubb’s CyberSecurity, Hiscox’s Hacker Insurance, etc. Contemporary first and third-party cyber-insurance policies cover a range of risks including damages in loss/corruption of data, business interruption, liability, cyber extortion, public relations, criminal rewards, cyber-terrorism, and identity theft.

Despite the well-identified potential, the development of cyber-insurance policies in traditional insurance market is slow because of many obstacles. The major obstacle for the development of cyber-insurance policies in the traditional insurance market is the inadequate understanding of IT risks. IT-related risks are relatively new to traditional insurance companies. The lack of historical data and experience in building actuarial tables prevents traditional insurance providers from issuing large policies on IT-related incidents and catastrophes. The rapid evolution and proliferation of technology make the accumulation of knowledge even harder. Other obstacles for the development of IT-related insurance policies in the traditional insurance market include (Baer 2003):
• Lack of agreement on basic policy definitions and language
• Lack of underwriting standards or experience
• Possible moral hazards
• Inadequate accountability for IT security flaws and vulnerabilities
• Lack of adequate reinsurance
• No strong collaborative processes or institutions for information sharing
3.2 The Development of the Captive Insurance Market

Captive insurance is an alternative approach that companies can adopt in risk management. A captive is an insurance or reinsurance company owned by a corporation or group of companies who are also insured by the captive. The captive’s primary objective is to insure the risks of its owners and the primary beneficiaries of its underwriting profits are those insured. The number of new captives and the capacity provided through captives has been accelerating worldwide (see Figure 1), fueled by the hardening premium rates and the limited capacity in the conventional commercial insurance market.

The major advantage of using captive insurance over purchasing conventional insurance is the lower cost. By utilizing a captive, companies can retain the underwriting cash-flow. This is beneficial for companies when the cost of cash-flow is lower than external financing. In addition, investment income may be untaxed in certain offshore captive domiciles, increasing the cash-flow advantage to companies.

In addition to financial benefits, the captive has other advantages which make it suitable for insuring the companies’ IT risks. These advantages include:
Writing Captive

- The captive can provide specific insurance products for the subsidiaries of its owners that would not otherwise be available. For many IT-specific insurance policies that are not available in the conventional insurance market, the company's captive can issue them;
- The captive can provide better claim handling experience, e.g., shorter length of time, less negotiation, etc. The loss caused by many IT vulnerabilities such as data corruption is often hard to measure. Therefore, insuring IT risks through the captive can reduce hassles for the company in the claim procedure;
- Companies can use the captive to access the reinsurance market, and then substitute the cost layer of the conventional insurer with the lower costs of the captive;
- The captive owned by a group of members can have larger capacity for large risks. This allows the captive to handle more types of IT risks.

Table 1 illustrates the advantages of captive insurance by comparing it with traditional insurance.

<table>
<thead>
<tr>
<th></th>
<th>Traditional Insurance</th>
<th>Captive Insurance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>High: companies have to pay premiums to the insurance providers.</td>
<td>Low: companies avoid the premium payment to the outside insurers</td>
</tr>
<tr>
<td><strong>Underwriting Flexibility</strong></td>
<td>Low: policies and pricing are controlled by the outsider insurance companies</td>
<td>High: policies and premium rates can be tailored to the specific needs of the insured companies</td>
</tr>
<tr>
<td><strong>Claim Handling</strong></td>
<td>A long and costly procedure of investigation and negotiation;</td>
<td>Shorter time, and better claim experience for the insured companies</td>
</tr>
<tr>
<td><strong>Profit</strong></td>
<td>Earned by the insurance companies</td>
<td>Can be distributed to the insured companies</td>
</tr>
</tbody>
</table>

Table 1: The Key Benefits of Captive Insurance

Currently, many large, multinational companies already have a captive. For example, Fortune 1000 companies have a large fraction of single-parent captives. Single-parent captives represent 70% of captives worldwide. The remaining 30% are written by multi-parent captives, which particularly serve the needs of medium-sized corporations. Another form of captive that can be used by middle sized companies is rent-a-captive. The rent-a-captive is an insurer that provides access to captive facilities for users who do not wish to form their own captive insurance company. The users of the rent-a-captive are liable for their own risks.
3.3 Insurance as an Incentive Tool for Compliance

Insurance companies often confront many incentive issues in their businesses, known as moral hazard and adverse selection issues. Moral hazard refers to the insured’s reluctance to take costly actions that decrease the probability or the magnitude of a loss when it purchases the insurance. For example, a company with data loss insurance may be less careful about protecting its data storage systems than a company without such insurance. Adverse selection refers to the insured’s leveraging of its private information in acquiring insurance policies. Such private information may put the insurer at a disadvantage in insurance underwriting. For example, those companies who are incapable of monitoring network traffic may purchase insurance on the business interruption of its website.

Insurance companies can use several ways to deal with these incentive issues. Monitoring is the most common approach. For example, insurance companies can conduct ex ante audit on eligibility and ex post investigation on claims. However, there are also a variety of monetary approaches that insurance companies can use to influence the insured’s incentives. For example, to address the moral hazard problem, the insurer can use deductibles to expose the insured to some loss when security breaches occur. This motivates the insured to invest more in self-protection. Also, to address the adverse selection problem, the insurer can increase the premiums for certain coverage to prevent the insured from transferring any risks it does not favor.

These insurance techniques can also be used by the company’s captive to deal with incentive issues associated with IT compliance management. For example,

- The captive can use proper insurance benefits to motivate BUs to objectively evaluate their specific IT risks, bear the control responsibilities and accountabilities, and align with the corporate-level IT compliance objectives.
- The captive can use underwriting criteria and claim conditions to resolve both the moral hazard and adverse selection problems in BUs’ own IT control practices. For example, the coverage on loss from virus attack should satisfy the prerequisite that antivirus protection has been adequately deployed; the claim on hacker attack is only acceptable given that effective access control mechanisms such as passwords and encryption are already in place.
- The insurance indemnification on loss ensures the BUs’ incentives in timely and accurately disclosing the security incidents, control failures and system vulnerabilities. Regulations, such as SOX, section 409, normally require companies to report significant change and problems of their IT systems. However, the disclosure of IT incidents may have a negative impact on BUs’ performance evaluation, and therefore, BUs may tend to underestimate the problem or delay the disclosure. Insurance may help resolve this adverse selection problem. The instant and objective claim filing helps BUs receive compensation for their loss. This benefit of reporting mitigates the BUs’ concern over problem disclosure.
3.4 Insurance as an Information Tool for Compliance

It is worth noticing that insurance is an information-intensive business. The captive needs to learn from the past experience in order to improve the actuarial table and underwriting criteria. Therefore, many techniques of information collection and analysis used in insurance can be applied to assist the IT compliance management. For example, the issuing and renewing of insurance policies can provide the company many insightful information on the IT control status of its BUs; The claim data allows the company to detect the weakness of their BUs’ IT control practices; The record systems of insurance can be used to facilitate the documentation in IT control; The stored data from insurance database can also be used to generate required documents for the external audit on IT compliance.

The captive can even take a more proactive role in the company’s cost management. For example, a captive can serve as a central information repository for the analysis on the IT compliance cost. The captive can also leverage its actuarial table to conduct the cost-benefit analysis for IT compliance team to evaluate certain investment plans in IT control. Moreover, the company can learn from its captive’s business about some innovative risk-management products in the outside marketplace.

4. A Framework of Insurance-based IT Compliance Management

In the insurance-based framework of IT control and compliance management, a company’s captive issues insurance policies to other BUs or subdivision sites of the company. The framework is comprised of 7 key blocks, each of which has both the insurance aspects and the compliance aspects. Therefore, each block calls for the cooperation between the IT compliance management team and the captive, which benefits both parties. For the IT compliance management team, the captive insurance helps hedge IT risks and resolve many incentive and information issues associated with IT compliance management. For the captive, the IT compliance group can provide valuable services, such as internal audit and control enforcement, to facilitate insurance processes. The details of each block are discussed as follows.
4.1 Risk recognition and assessment

Both IT compliance and insurance underwriting involve a process of risk assessment. These two processes share many commonalities. For example, the issuing of policy on network security normally requires a security audit on the installation of firewall, virus protection software, network monitoring procedure, etc. Similarly, the compliance with regulations like SOX also involves internal audit on the effectiveness of IT control. Due to the similarity between these two processes, companies can formalize a joint process of risk assessment to serve both purposes of IT compliance and insurance.

The joint process of IT risk assessment involves both the directors from the IT compliance management team and the experts from the captive insurance company. The IT compliance management team may focus more on adopting the top-down perspective to map the regulatory requirements to the corporate-level IT control policies. In contrast, the captive may focus more on adopting the bottom-up perspective to identify specific IT risks for each BU at the process-level. The effective communication between the IT compliance management team and the captive guarantees the success in seamlessly integrating the top-down perspective with the bottom-up perspective.

The company can also adopt a service-oriented perspective regarding the mutual assistant between the IT compliance management team and the captive. For example, in cyber-insurance market, insurance companies often rely on certain standard, such as ISO-17799, as their security audit guidance. ISO-17799 is also a tool that the IT
compliance management team can use to develop IT control policies and test IT controls in BUs. Therefore, the IT compliance management team can act as a service provider for the captive by using ISO-17799 to review BUs’ security practices. This reduces the captive’s reliance on external auditors to conduct the security audit. Similarly, the captive can provide cost-benefit analysis for the IT compliance management team in evaluating specific IT control policies.

<table>
<thead>
<tr>
<th>Risk identification and assessment</th>
<th>Insurance Aspects</th>
<th>Compliance Aspects</th>
<th>Critical Success Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies and their BUs need insurance products to hedge the risks associated with their IT practices</td>
<td>Assess the frequency and severity of IT-related risks to balance risk reduction and risk transfer</td>
<td>Assess the potential threats, vulnerabilities and weakness of IT to comply with regulations</td>
<td>Integrate IT audit to assist both insurance and compliance; adopt a risk-based perspective in IT control</td>
</tr>
<tr>
<td>Underwriting process</td>
<td>Companies and BUs need to rationalize the inputs in compliance management</td>
<td></td>
<td>Provide coverage on BUs’ specific IT risks; save insurance costs; adjust premiums and coverage to motivate BUs to optimize their own risk management;</td>
</tr>
<tr>
<td>Control and risk reduction</td>
<td>Avoid lax practices in self-protection</td>
<td>Comply with the control requirements of the regulations</td>
<td>Combine the two perspectives to enforce the optimal approach.</td>
</tr>
<tr>
<td>Risk transfer</td>
<td>Reduce the loss of the captive itself; stabilize the company’s revenue stream and reduce the capital cost</td>
<td>Reduce the overall costs associated with IT compliance management and IT control</td>
<td>Develop cost-efficient plans of reinsurance and risk securitization</td>
</tr>
<tr>
<td>Claim handling and remediation</td>
<td>Compensate BUs’ loss caused by the vulnerability events</td>
<td>Deficiency management; incident disclosure</td>
<td>Link BUs’ deficiency management and incident disclosure with their claim compensation</td>
</tr>
<tr>
<td>Knowledge building</td>
<td>Historical claim data on vulnerability can be</td>
<td>Meet the disclosure requirements of regulations (e.g.</td>
<td>Use insurance techniques to conduct cost analysis</td>
</tr>
<tr>
<td>Profit Sharing</td>
<td>The retention of the captive’s profit provides the insured incentive in risk reduction</td>
<td>Economic incentives can be used to motivate BUs’ cooperation in compliance management</td>
<td>Link BUs’ IT compliance budget allocation with the performance of the captive</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>

Table 2: The Key Components of Insurance-based IT Compliance Management

Another important part is the BUs’ self-assessment of their IT risks. The availability of insurance motivates BUs’ to objectively evaluate their IT risks and reveal them to the captive. Collaborating with the captive, the IT compliance management team then can acquire more reliable information about the specific IT risks at the process-level. This helps the IT compliance management team to optimize their high-level control policies.

4.2 Underwriting processes

One advantage of captive insurance is that the company can have better control over the insurance policy development and underwriting. Therefore, the IT compliance management team should work closely with the captive to make the IT insurance policies also serve for the purpose of IT compliance.

The insurance policies specify the coverage, the premium (i.e., the price) and the claim compensation. The specification on coverage reflects the characteristics of risks being insured, the premium reflects the insured’s willingness to pay for the risk transfer, and the claim compensation reflects the insurer’s willingness to bear the risks. All of these instruments can be controlled by the company to coordinate BUs with the overall IT compliance objectives. For example, the IT compliance management team can help the captive in deciding what specific IT incidents can be covered by insurance. BUs are motivated to objectively assess and reveal the risks covered by these policies in order to receive the protection from the policy coverage.

Also, since BUs normally absorb some of the compliance-related costs into their own budgets, insurance premiums and claim compensation can be carefully adjusted to control the risk allocation and balance the resource allocation. If the company intends to aggregate the risks from different BUs and achieve more centralized IT control policy, it can issue more policies to BUs with wider coverage ranges and higher
compensation limits. On the other hand, if the company intends to motivate BUs to be more responsible for the control of their local systems, the captive can use lower compensation limits, or impose more strict eligibility criteria for underwriting. In this way, insurance helps combine the top-down approach with the bottom-up approach in IT compliance management.

4.3 Control and risk reduction

The control activities that BUs can undertake to reduce their own IT risks (i.e., self-protection) have been specified in many control standards and guidance. For example, COBIT and ISO 17799 address 10 areas which specify in total 124 control components. Following these standards, BUs can decide what to control and what to monitor.

In addition to self-protection, BUs can also conduct some activities to protect each other. Captive insurance can play an important role in motivating different BUs to engage in peer-protection.

Peer-protection refers to some controls that may not directly benefit individual BUs their own but can mitigate other units’ risks and improve the corporate-level control environment. Due to the interconnectivity of the corporation’s IT infrastructure, the IT systems of different BUs can affect each other. Therefore, from a holistic perspective of IT control, conducting certain peer-protection practices can be more cost-efficient than purely relying on each BU to protect itself. For instance, each unit has more control over its own employees and users. It is operationally easier for each unit to urge its local users to install patches, disconnect malicious users in its domain, discard the malicious traffic originating from its area, filter outbound email spam, and detect and block any attempt of unauthorized access to other systems. Sometimes a small amount of addition input in peer-protection may save a large amount of input in self-protection for other units.

The motivation of peer-protection can be achieved through the profit sharing of the captive. The issue of profit sharing is discussed in detail in section 4.7. The main point is that the profit of the captive can be distributed to its insured units. Therefore, the company can link BUs’ IT budget to the overall performance of the captive. This prevents BUs from considering the company’s general IT security as purely public goods, and thus enhances BUs’ willingness to accept more globally optimal policies.

4.4 Risk transfer

Similar to conventional insurance companies, a variety of ways can be used by the captive to transfer risks and reduce risk retention. For example, the captive can access the reinsurance market. Reinsurance is a contract in which the reinsurance company indemnifies insurance companies against loss under their own insurance policies. Insurance companies can also develop reinsurance policies with each other, limiting
their liability on specific policies, increasing their capacity of policy underwriting, and stabilizing their revenue streams.

The captive can also transfer risks to the capital market through risk securitization. The conventional rationale for risk securitization is to link the insurance market with the capital market, which can absorb much more risk, especially when the catastrophe loss tends not to be highly correlated with capital market returns. Insurance-linked securities include catastrophe (CAT) bonds, CAT options and CAT equity puts. These securities help the issuers raise money in case of a catastrophe, such as hurricane, flood or earthquake. Cyber catastrophes, such as distributed denial of service (DDOS) attack, are also appropriate for securitization.

Risk transfer reduces a company’s IT compliance costs by lowering the loss on control deficiency, security incidents and other IT vulnerabilities. The loss indemnification from the outside reinsurance and capital markets reduces the volatility of a company’s revenue and profit caused by the IT vulnerabilities. The stabilized revenue stream then reduces the company’s capital costs in the financial market. Also, a well-prepared risk transfer policies helps limit the indirect damages associated with vulnerability disclosure, such as reputation damage. The availability of risk transfer policies can signal to the market about the company’s due diligence in internal control and thus moderate the negative impact of disclosing IT accidents.

4.5 Claim handling and remediation plan

With the captive, the company has more control over the procedure of claim handling. Less time and costs will be incurred when the company’s captive handles claims. Moreover, the company can leverage its control capability to facilitate claim handling and generate additional value for IT compliance management.

First, claim handling is an important process of documenting the incidents and weakness of BUs’ security practices and IT control. The insurance indemnification motivates BUs to report security breaches and incidents in a timely and accurate way. The company can immediately detect the occurring problems, and record the remediation processes. A robust claim handling process assists the company in mandated information disclosure. For example, multiple sections of SOX (e.g., section 302, 404, and 409) have strong implications on the capability of a company’s documentation system to deliver incidents and potential weakness of their IT systems. The company can build document generation systems to transfer the claim files into compliance-ready documents. The claim files can also be stored for the use by external audit. The automation of these processes can significantly simplify the documentation management for compliance. The critical success factor here is the effective maintenance of the interface between the claim documents and the compliance documents.
Second, by imposing conditions in claim filing, the company can also force BUs to develop and implement effective solutions of deficiency management and remediation. For example, the captive can specify that BUs can only file claims on loss from network disruption when they already have proper network recovery facilities and solutions in place.

4.6 Knowledge building and sharing

Both the captive insurance and IT compliance management require a continuous process of knowledge building. The captive needs to learn from past experiences in order to improve the actuarial table and underwriting criteria. A captive can serve as a tool for collecting more and better information, for example, a central information repository for the analysis on IT compliance costs to support its cost management efforts.

The initial compliance investment without risk-based consideration often results in redundant coverage. For example, a disproportionate amount of time has been spent on documenting and testing controls that would not cause a material misstatement if they were not operating. Therefore, identifying key risks, assessing impacts, and prioritizing controls are rational practices in reducing the compliance cost.

The risk-based approach enables the company to reduce the redundancy in identifying, controlling and testing IT objects. Many insurance techniques can help construct the risk-based control framework. For example, in building and improving its actuarial table, the captive needs to accumulate past experiences and historical data. The accumulated information assists in estimating the severity and frequency of each type of IT vulnerability. Such rich information on the characteristics of IT vulnerabilities is also valuable for the IT compliance management team to determine the corresponding corporate-level control, testing and documentation policies. For instance, considering the frequency of certain IT vulnerabilities, the IT compliance management team can decide how often the corresponding tests on these vulnerabilities should be conducted.

4.7 Profit sharing

Unlike the typical insurer, which keeps earnings for its own profit, the captive’s retained earnings can be distributed to the insured(s) in the form of profit commission or dividends, or used to reduce premium payments for the participants in future years. A company can establish relations of funding and surplus sharing between its captive and other insured BUs. Insured BUs can make capital investment in the captive, and reap capital returns through the sharing of insurance surplus. Such financial relations align the BUs’ self interests with the corporate-level objectives of IT risk management.
The profit rewards that BUs can receive from the captive also motivate them to help each other and collectively achieve an optimal outcome. The IT compliance management team, the captive, and the senior management of the company need to work together to decide the policies in rewarding BUs through profit sharing. For example, part of BUs’ annual IT budget funding can be based on the overall performance of the captive in insuring IT risks.

5. Partner Control through Captive Insurance

Captive insurance can not only assist internal IT control, but also enable the control over outside partners. In contemporary business environments, firms are increasingly using partnering to achieve their R&D, manufacturing and marketing goals. Partnership and outsourced business processes pose additional problems for IT compliance management, since control over outside partners’ facilities and services is normally constrained by the contracts and the partners’ willingness to cooperate. In this regard, the captive insurance can be used as a strategic tool in partnership management.

Companies can make the insurance coverage available for their various business partners (e.g., suppliers, customers, and outsourcing partners), especially when pricing or terms from the conventional market are not favorable. Through issuing insurance policies covering partners’ IT systems, the captive provides its parent companies a better understanding about not only the threats and vulnerabilities from partners’ IT practices, but also the gaps between partners’ IT controls and their own. Such understanding allows companies to strengthen their own internal IT control as well as develop collaborative control policies and joint risk management processes with their partners.

The captive can also help in the due diligence process of partner selection. There are some guidelines available for companies to regulate their partners’ IT management. For example, SAS 70 is an audit standard for service vendors. The captive can incorporate SAS 70 into its underwriting criteria for service partners.

6. Other Operational Issues of the Captive

Despite the benefits of captive insurance, there are also many operational issues that a company needs to consider when it uses captive insurance. For example,

Legal Issues. Many parts of the business model of captive insurance are subject to regulations. These parts include underwriting constraints (e.g., whether certain forms of captives are eligible to underwrite certain types of policies), solvency ratio (i.e., the maximum level of premium a captive is supposed to write net compared to its capital and surplus position), loss reserve ratio (i.e., the proportion of loss reserves to capital and surplus), the way of profit distribution for the captive, etc. It is expected that as
captive insurance becomes more widely adopted, the regulatory environment will also evolve to help the captive exert more effects in companies’ IT risk management.

Management Issues. Companies may outsource the management of their captives to others, rather than maintain their own employees. For example, companies can use captive management companies to perform the day-to-day operations, and rely on external law firms. Therefore, companies need to maintain a good partnership with those outside parties.

7. Alternative Solutions

It is worth noting that the captive is just one of many alternative risk transfer approaches that companies can use to facilitate their risk-based IT compliance management. There are also other alternative tools. For example,

Finite risk reinsurance. Finite risk reinsurance shifts the main value proposition from traditional risk transfer to risk financing. The customer pays either annual or single premiums to the reinsurer. These funds earn a contractually agreed upon investment return, which is used for eventual loss payments or “flow-back” to the customer. Finite risk reinsurance reduces a company’s capital cost.

Committed capital. Committed capital is based on a contractual commitment to provide capital, in the form of preferred shares, senior debt, or surplus notes, to a company after a specific risk event occurs. Committed capital is a product combining insurance and capital market techniques, and allows the company to obtain less expensive capital during financially stressful events (which can include certain IT risks such as business interruption due to system collapse).

Multi-year/multi-line products (MMP). The recently emerging MMPs allow companies to take advantage of the risk consolidation within their own portfolio of risks. Companies may consolidate their IT risks with other types of operational risks such as credit risks in order to obtain efficient risk transfer and avoid over-insurance.

CONCLUSION

As companies have experienced the initial stage of expenditure, now they are moving toward a more streamlined and cost-efficient manner of IT control and compliance management. In doing so, companies have to align their business units’ incentives in assessing IT risks, maintaining effective and efficient control, and disclosing and documenting control problems. In addition, companies need to rely on intensive information collection and scientific information analysis to optimize and update their control policies.

This article illustrates that the business model of captive insurance can be applied to facilitate the company’s IT control and IT compliance management. Many insurance
techniques can be used to resolve the incentive and information issues in IT compliance management. The framework proposed in this article calls for the cooperation between the businesses’ captive insurance companies and their IT compliance management teams in identifying IT risks and control objects, using insurance mechanisms to motivate BUs’ efficient IT controls and hedge BUs’ IT risks, and managing knowledge for IT compliance. The insurance services provided by the captive can also extend beyond the organizational boundaries and be applied to the areas of external partnering.

REFERENCES


Towers Perrin, Captives 101: Managing Cost and Risk, White Paper

Xia Zhao is an assistant professor at the Bryan School of Business and Economics, the University of North Carolina at Greensboro. She received her Ph.D. degree in Management Science and Information Systems from the University of Texas at Austin. Her research interests are in the areas of information security, electronic commerce and IT governance. She has published papers in Decision Support Systems, IEEE Computer, International Journal of E-Commerce and many conferences.

Ling Xue is an assistant professor at the Kania School of Management, University of Scranton. His research interests are in the areas of IT business value, IT governance, the impact of IT on firm structure, and IT security. He received his Ph.D. in Management Science and Information Systems from the University of Texas at Austin in 2007. He has published in Information Systems Research and International Journal of Electronic Commerce.