ISG™ imagine your future®

THIRD PARTY SUPPLIER RISK MANAGEMENT

Meeting Emerging Financial Services Regulatory Requirements

ISG

INTRODUCTION

U.S. and Canadian financial services companies face increased regulatory scrutiny of the processes, systems and controls used in monitoring and managing risks associated with third-party suppliers. Across a wide range of agencies, the general guidance and oversight requirements are similar and becoming more of a priority.

While managing and monitoring supplier risk has always been good business practice, the stakes have increased in recent years. More than ever, failing to meet regulatory requirements and expectations can mean potentially significant penalties and remediation costs, as well as serious organizational reputational exposures.

Several recent trends are driving regulators to look at supplier risk more closely. These include:

1. ***Greater Overall Interest in Operational Risk:*** Supplier risk is a type of operational risk, which is taking on more importance to regulators. In May 2012, Thomas Curry, head of the Comptroller of the Currency, said the operational risk is "currently at the top of the list of safety and soundness issues and might have eclipsed credit risk as a safety and soundness challenge."

2. ***Greater Interest in Compliance Risk:*** The Dodd-Frank act requirements are leading to more supervisory focus on compliance risks, which mean greater regulatory scrutiny of suppliers, especially suppliers that interact directly with customers or have customer data.

3. ***Changing Nature of Outsourcing:*** Financial services companies are outsourcing an increasing number of sensitive functions (e.g., customer support centers, social media, mobile banking) which materially increases the need for better vendor management. Additionally, the growth of cloud computing and other technologies presents new challenges as to where sensitive data is stored and what protections of this data exist. The regulators know that suppliers are the soft underbelly for cyber-security and privacy risks.

This ISG white paper describes the four areas of supplier risk regulators look at and the 15 characteristics of good supplier risk management that will meet ever increasing and more rigorous regulatory requirements.

THE REGULATORY LANDSCAPE

Financial services companies in the US and Canada face increased regulatory scrutiny regardless of whether they are a bank, credit union, insurance company, specialty lender, payment services provider, financial information company or other type of financial products provider. The various agencies are increasingly scrutinizing financial services companies' third-party supplier risk management programs.

Existing regulations are taking on new and more rigorous interpretation. Many of these pronouncements and rules are aimed at monitoring and managing the risks of third-party suppliers to financial services companies.

Some requirements are well established and have been of interest to regulators for a while, but agencies are stepping up enforcement of regulations and holding institutions to a higher standard.

Adding to the complexity of the regulatory environment for U.S.-based or foreign owned organizations operating in the U.S. is the Consumer Financial Protection Bureau (CFPB), a new agency created by the Dodd–Frank Wall Street Reform and Consumer Protection Act. The CFPB is bringing a new level of authority, new perspective, and new energy to oversight of financial services companies. The CFPB is independent of current regulatory agencies and adds further complexity to management's efforts at assuring compliance. We expect this trend to continue and extend through the various oversight bodies in North America.

SUPPLIER RISK MANAGEMENT AREAS

The framework for assessing adequacy of supplier risk is remarkably consistent across regulatory agencies. The wording and details may differ among regulators, but the thrust and focus is the same. An example of this focus is summarized by the OCC in Bulletin 2001-47, which states that, an institution:

"Engage in a rigorous analytical process to identify, measure, monitor, and establish controls to manage the risks associated with third-party relationships."

Guidance details vary, but each regulatory agency tends to look at four primary areas to examine adequacy of supplier risk management, as described below.

Inherent Sourcing Risk

Before any third parties are even considered, the company should have a process to assess the risk of sourcing a process, product or function. The types of risks to consider are strategic, reputation and brand, financial, competitive position, data security and integrity, customer impact, employee impact and general operations.

Due Diligence of Potential Suppliers

Once the company has appropriately considered the general risk inherent in sourcing a process, product, or function, the second area is the selection of the supplier.

This type of supplier risk is specific to each individual potential supplier and primarily means the adequacy of the due diligence during the evaluation and selection process. The company is responsible for undertaking the proper research into the supplier's ability to deliver the service and has proper internal controls that meet financial services regulatory standards.

Contract Form and Content

This aspect of supplier risk management involves the completeness and sufficiency of the agreement with the supplier. The regulators consider form and content of contracts to ensure a company's rights and supplier obligations meet regulatory requirements, and good business practices.

Additionally, regulators evaluate the use of contract templates, especially the internal processes to deviate from standard contract language.

Ongoing Supplier Governance

This area is the post-contract, ongoing oversight of the supplier's delivery of the process, product, or function that has been contracted. Ongoing governance of the relationship is important for regulatory demands, as well as good business practices as the post-contract period can run three, five, and sometimes as long as 10 years.

The regulators expect the financial services company to have proper and adequate controls in place for ensuring data security and compliance with laws (especially related to dealings with consumers and customer data).

FIFTEEN FACTORS REGULATORS LOOK FOR

During exams, regulators look for a control environment that includes organization, technology, processes and policies sufficient to manage adequately the risks of third-party relationships. This control environment will incorporate the attributes and characteristics in 15 specific areas as described below.

1. **Strong Risk Management Environment**

   The regulators will look for evidence of strong risk management and audit functions within the company. The characteristics of "strong" culture, as well as strong risk and audit functions are shown in Attachment 1. These functions need to be well integrated into an overall control environment.

2. **Risk Management Infrastructure**

   Regulators will assess the level of maturity of the various tools and technologies the company has to perform supplier risk management processes. They will also consider how the tools are used and the level of training of staff to use the tools for effective supplier risk management.

3. **Overall Risk Management Documentation**

   The regulators expect to see adequate written program documentation (e.g., policies, procedures, checklists, templates, forms, etc.) that conveys program requirements to staff, with procedures for periodically updating that program documentation.

4. **Staffing Resources**

   The regulators expect to see staffing levels and skills necessary for proper supplier risk management. This includes adequate resourcing, workloads and training on regulatory and compliance topics.

   Additionally, the regulators will look for clear organizational ownership of the risk functions. They are interested in ensuring accountability and responsibility for supplier risk management.

5. **Supplier Risk Management Recordkeeping**

   Regulators expect to see records of supplier risk management activities, as well as an organized mechanism for updating and archiving these records.

6. **Reporting to Executive Management**

   Supplier risk results should be reported to executive management as a regular routine process, and special reporting for adverse changes with a supplier's ability to perform services or other material changes.

7. **Pre-Supplier Selection Risk Assessment**

   Skills and processes are in place to assess inherent risks of outsourcing a process, product or function even before specific suppliers are considered.

8. **Due Diligence Proceadqss and Documentation**

   The regulators want to know that the company properly vetted the supplier before selection through proper due diligence, and has adequately documented findings and selection criteria.

The evidence can include, for example:

1. Site visits to a supplier's office and processing locations.
2. Visits to a supplier's customers.
3. Review of supplier capabilities by subject matter experts in or out of the company.
4. Well-executed RFP process with multiple qualified suppliers during selection.
5. Results of public information reviews, e.g., financial condition, past and pending litigation, bad press, customer complaints, etc.
6. Results of more detailed review of the supplier, e.g., staff skills and training, internal control environment (especially data security controls), business continuity plans, reliance on subcontractors, insurance coverage, etc.

9. **Contracts**

   Regulators will look at three aspects of contracts:

   - ***Contract Forms:*** Ensuring the right form is used with suppliers appropriate to the type of relationship.

- ***Contracting Process:*** The process the company uses for finalizing contracts, including internal and external review, and controls in place to ensure modifications to approved contract forms templates are done only with proper oversight and review by internal and/or external legal counsel.
- ***In-force contracts:*** Regulators will focus on 17 provisions of a contract, mainly for strategically important suppliers (usually defined based on a combination of contract dollar size and criticality of the service to the company's ongoing operations). These 17 areas are summarized in Attachment 2.

10. Data Security

In all aspects of the supplier relationship, data security is one of the most important aspects regulators will examine. The legal and operational control environment must ensure the supplier (and secondary suppliers) are applying the company's own level of data security protection, and are able to adjust to system threats and intrusions. This is particularly important for customer data.

11. Assessment of Internal Controls

Regulators look for evidence that companies review their own processes and controls to ensure that, for example:

- Policies and procedures are actually being followed by operational staff.
- Processes are not "shelfware" (i.e., policy exists but "never comes off the shelf").
- A strong risk management function has not deteriorated into ineffectiveness.
- Clear ownership and accountability for compliance exists throughout the supply chain.

12. Assessment of Critical Suppliers

Proper supplier risk management requires periodic assessments of several aspects of supplier risks:

- The status of the supplier should be regularly updated, looking for changes in financial condition, unfavorable news stories, divestitures of key operating capabilities, mergers and acquisitions, and other key changes in the supplier that may impact their ability to deliver.
- Supplier performance relative to the terms and conditions of the contract (which should be part of any good governance program).
- Understanding of the options, complexity, time required, and costs if it becomes necessary to change suppliers.

This periodic assessment can also include onsite audits for strategically important suppliers. The company should have a policy and plan for regular audits of these third parties.

13. Secondary Supplier Transparency

This involves "suppliers to your suppliers" and the level of risk management that can be applied to these secondary suppliers. For example, regulators will assess contractual rights to audit and have transparency to the supplier's suppliers.

14. Ongoing Governance

Since the vast majority of the time spent with a supplier is after the contract is signed, ongoing governance of supplier is of keen interest to regulators. Governance normally covers the day-to-day oversight of suppliers; some aspects are not necessarily regulatory, but simply good business (e.g., invoice validation).

Regulators will assess how a company is managing a supplier during the term of the agreement relative to resources applied, policies, tools and procedures from four primary perspectives:

- Performance to contract requirements.
- Financial relative to pricing, invoicing, etc.
- Contract compliance, interpretations, etc.
- Relationship with supplier for resolving issues, communication, forecasting demand, etc.

15. Offshore Suppliers of Outsourcing Services

Outsourcing providers that deliver services from offshore locations get special scrutiny from regulators. They want to ensure, for example, that a company:

- Performed and documented adequate due diligence during a supplier's selection.
- Can enforce contract terms outside North America.
- Understands and can manage the effects of political and economic risk that may be inherent in the foreign country on management and operations of the foreign provider.
- Has confirmed the supplier has the ability of the offshore provider company to effectively comply with, for example, the Gramm-Leach-Bliley Act (GLBA) privacy and security provisions, the USA Patriot Act anti-money laundering provisions, and other anti-money laundering legal obligations that apply to a company.
- Has confirmed that surety bond covers losses, including losses from errors and omissions that result from arrangements with the offshore provider.
- Has considered the reputation, operating history and financial strength of the offshore provider.
- Has established a maximum recovery period for specific disruptions to assure minimal disruption to ongoing operations.

SUMMARY

Financial industry regulators are including third-party supplier risk management as a substantive part of the exam process. Examiners are looking deeply into financial services companies' processes, policies, technology and staff to gauge the adequacy of the risk and the risk management capabilities to monitor and control various elements of risk.

This is not just an administrative exercise. Real and significant costs are at stake for inadequate supplier risk management, both in direct penalties, remediation costs and in organizational reputation.

Forward-thinking financial services companies are getting ahead of the regulators by evaluating their supplier risk environment and infrastructure prior to exams. This enables them to identify and take corrective actions to eliminate regulatory and operational deficiencies gaps pro actively and not wait for an examination to surface such issues.

Moreover, supplier risk management is not just a regulatory issue but a good business issue as well. The types, frequency and severity of risks have changed dramatically over the last few years. These new risks conditions along with new scrutiny in the area of supply chain risk by the regulators has created a new sense of urgency amongst most financial services companies.

Supplier risk management, once an annual or semi- annual event, now requires continuous and real time monitoring. Financial services companies must ensure that they had adequately staffed their organizations appropriately to meet this new requirement. They must also implement detailed ongoing monitoring, recovery and communication plans to mitigate any disruptions and/or regulatory exposures.

Those financial services companies that take the lead in this area of supply chain risk management will benefit from fewer business disruptions, improved customer satisfaction and loyalty and improved regulatory relations.

ISG™

ATTACHMENT 1

CHARACTERISTICS OF A STRONG RISK MANAGEMENT CULTURE

Written Policies

1. Clearly articulates board-approved enterprise-wide and LOB risk appetite levels, generally relative to earnings or capital, but also considers reputational risks.
2. Considers all relevant risk categories and key drivers, including concentrations and stress conditions.

Supporting Processes

1. Communicating and reinforcing the firm's risk appetite throughout organization (culture).
2. Aligning the firm's business strategy, risk profile and capital plan with its risk appetite.
3. Identifying and aggregating risks within and across legal entities, business lines, products and services, geographies, etc. (Concentration management) at a frequency commensurate with the risk profile.
4. Establishing enterprise-level concentration and other control parameters (limits, triggers) that tie to capital or earnings and cascade into lines of business; establish sub-limits by business line, product, geography as necessary Performing broad scenario analyses and stress tests which capture applicable risks to complement proactive measurement and monitoring.
5. Communicating identified risks up the line.
6. Escalating and resolving exceptions to control parameters in a timely manner.
7. Establishing and executing contingency plans in the event concentration or other control parameters are breached Re-assessing the firm's risk appetite at least annually, when new business opportunities arise, or when there are changes in risk capacity, operating environment, etc.

Independent and Proactive Risk Management and Audit Functions

1. Ensure timely and accurate production of reports for monitoring and proactive control.
2. Assessments based on observed risk levels and trends.
3. Validate the integrity of risk measurement techniques and information used to monitor the risk profile in relation to risk appetite.
4. Evaluate the alignment of policies, procedures, processes, business performance assessments, compensation plans, and decisions with the firm's risk appetite.

Success Drivers

1. Prudent strategic vision supported by understandable and actionable risk appetite policy.
2. Culture of accountability that encourages robust discussions of risks; no material surprises affecting financials, market perception, or reputation with customers.
3. Risk appetite pro actively used in considering business opportunities and strategic options.
4. Principle-based decision making throughout the firm that considers all relevant risks, aligns with the company's established risk appetite, appropriately balances risk/reward over short and longer term time horizons, and provides for a meaningful analysis and basis upon which the Board and risk management/audit functions can effectively and credibly debate and challenge management recommendations and decisions.
5. Highly developed technology, infrastructure, analytics and accurate MIS to support the comprehensive identification, measurement, and monitoring of risks within and across business lines and legal entities strong risk management and audit functions.

CHARACTERISTICS OF A STRONG RISK MANAGEMENT FUNCTION

Key Elements

1. Ensures an appropriate risk management infrastructure is in place (policies, operating procedures, line of business talent levels and appropriate reporting mechanisms).
2. Reporting structure is independent of LOB.
3. Ensures that risk-taking activities are pro actively controlled so that volatility to earnings, capital and the company's reputation is within risk tolerance levels.

Stature and Competence/Talent

1. Executive management and the Board overtly support risk management functions (e.g., credit, market risk, compliance, operational, etc.) and ensure they are staffed appropriately to perform their roles in appropriate depth and frequency.
2. Risk Management personnel understand the businesses, risks, appropriate controls that should be in place, the fit of units and risks into the overall company, and respond to material risk profile changes.
3. Uses Benchmarking/comparison to industry best practices to improve continually.

Accountability/Effecting Change

1. The credibility and stature of risk management with business units is reflected in timely resolution of issues, rare instances of repeat deficiencies, and the inclusion of risk management leaders and/or their staff in business planning initiatives and processes.
2. Risk assessments, including periodic testing, effectively evaluate the completeness of controls and validate that employees are adhering to processes and operating within established limits.
3. Proactive communication between risk managers and business personnel result in timely, and preferably early, resolution of concerns.
4. Judgmental conclusions by risk managers are typically complemented by objective measures to facilitate context and enable tracking of risk relative to stated appetite.
5. Risk managers able to elevate problems and concerns to senior management and Board.

Fundamental Characteristics

1. Policies clearly define risk tolerance, responsibilities and accountabilities.
2. Policies are effectively communicated.
3. Procedures and processes are defined, well understood and adhered to consistently.
4. Internal control processes are comprehensive and effective.
5. Compensation programs effectively balance revenue generation and risk taking.
6. Accountability for control culture is enforced.
7. Risk measurement and monitoring systems enable proactive responses to changing conditions.
8. Design and supporting technology, including models, assumptions, software logic and data input are validated, tested and documented.
9. Systems are accurate, timely, complete and provide information for sound decisions.
10. Information gathered and analyzed is appropriate for volume/complexity of activity.
11. Portfolio risk is identified and actively controlled, including concentrations.
12. Risk taking personnel possess extensive technical and managerial expertise.

13. Business and risk managers fully understand all relevant aspects of risk taking.

14. Contingency planning provides for continuity of activities and services in times of crisis.

15. Any risk management weaknesses are minor, with nominal potential impact to earnings or capital.

CHARACTERISTICS OF A STRONG AUDIT FUNCTION

Stature

1. LOB and financial functions welcome credible challenge from audit team.

2. Attains highest level of respect and confidence within the organization; continually affirmed by attitudes, actions, and overt support of board and executive management – including CEO and CRO.

3. Role is clear and integrated into corporate risk management, policy development, new product and service deployment, changes in strategy and tactical plans, and organizational and structural changes.

4. Audit Committee is well respected and has the financial acumen to understand the issues and confidence to provide credible challenge.

Competence/Talent

1. Chief Auditor has strong technical/analytical and communication skills; good leadership evidenced by ability to attract and retain quality reports.

2. Sufficient resources for talent development.

3. Depth within audit team enables succession, LOB staff rotations and continuation of quality coverage during times of change and/or adversity; staffing level is appropriate to the level of risk undertaken by the company.

4. Expertise aligns with sophistication and complexity of the company's risk profile and operations, enabling ongoing ability to provide credible challenge.

Accountability/Effecting Change

1. Effectively inspires LOB leaders to acknowledge issues and operate with appropriate sense of urgency, and focus in their timely clearing.

2. Periodic reports succinctly and clearly inform management and Board of major findings, including the root cause of problems, issues that cut across multiple areas, adequacy of policies and procedures, potential or emerging concerns and the status of outstanding issues.

3. Reports also leverage objective measures to identify, measure and monitor risk and control issues relative to prudent standards.

4. Audit reports include comments on the efficacy of business unit self-assessments, emerging issues and appropriateness of risk levels relative to both the quality of control environment and to stated risk appetite.

5. Audit results are considered in performance evaluations and compensation decisions.

Scope and Frequency

1. Audit Committee actively sets expectations, approves overall plan, and evaluates audit's performance.

2. Rank Ordering of auditable entities derived from audit team's own risk assessments cross firm, with subsequent adjustments informed by leveraging business unit self-assessments along with changes in the company's strategy and the external environment.

3. Periodic, continuous, forward-looking monitoring, while lower risk entities are evaluated with reasonable frequency.

4. Audit plan and scope of specific audits consider reputation and strategic risk as well as evaluations of risk management and more traditional risks.

5. Audit work considers traditional validation to determine accuracy of financial records, timely and accurate production of reports (data accuracy, model production, segregation of duties etc.), Adherence to policies and procedures, and compliance with laws and regulations as well as an enterprise view that enables insights to provide assessment of the "sensibility" or prudence of risk levels and trends.

6. The Board of Directors can fully rely on the work and conclusions of the audit function.

ATTACHMENT 2

ASPECTS OF OUTSOURCING CONTRACTS REGULATORS LOOK FOR

1. Clear description of what the supplier is to provide (i.e., deliverables and obligations), service levels required (i.e., SLAs), and remedies for non-performance.

2. Use and management of the contracting company's facilities and/or employees, if any.

3. Rights for termination rights and transition support from the supplier.

4. Supplier obligations for reporting the results of performance and other important measures of operations, as well as episodic reports in the event of material changes to the supplier (e.g., change ion financial condition, changes in capabilities through divesture).
5. Audit rights of the company, including rights to audit secondary and tertiary suppliers.
6. Clear definition of the financials of the relationship (e.g., prices, how billed, invoices disputes).
7. Clear definition of ownership rights for data, IP, software licenses, etc.
8. Confidentiality provisions that protect company data, and clearly states the process in the event of unauthorized access to company data.
9. Requirement for supplier to comply with consumer protection laws (especially for customer-facing suppliers).
10. Supplier's data and information security controls to industry accepted standards, particularly for suppliers with access to customer information on company systems.
11. Rights for company to review the supplier's business continuity plan, and penalties for not complying with that plan in the event of an emergency.
12. Requirement that supplier comply with applicable law and the company's policies and procedures.
13. Supplier requirements for records retention; what they keep and for how long.
14. Indemnification and required insurance with particular attention to protecting the company in the event of supplier negligence.
15. Limits on liability is always a contentious issue with suppliers, but the general principle is to have limits on liability proportionate to the amount of loss the company might experience as a result of the supplier's failure to perform.
16. If the prime supplier is subcontracting and assigning work to other suppliers, the company needs to have assurance that provisions of the primary contract will apply to secondary providers, including rights to audit.
17. Appropriate dispute resolution process and mechanisms.

ABOUT ISG

Information Services Group (ISG) (NASDAQ: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including 75 of the top 100 enterprises in the world, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; technology strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For additional information, visit www.isg-one.com.

Let's connect NOW...

ISG™

imagine your future®

