Optimizing an Enterprise Wide Effective Vendor Risk Management Program

Pam Schott
Head and VP
Enterprise Supplier Governance

BMO Financial Group
We’re here to help.

June 1, 2015
Emerging Industry Trends

As Procurement organizations mature; their focus needs to be more than just cost savings; they need to be proactively involved in strategic initiatives and creatively protect their organizations

<table>
<thead>
<tr>
<th>Procurement and Finance Alignment</th>
<th>• Essential partnership between procurement and finance to track and record savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Expansion</td>
<td>• Support strategic initiatives in international expansion, licensing, ecommerce growth</td>
</tr>
<tr>
<td>Innovative Solutions</td>
<td>• Expand supply market research to include new innovative solutions (i.e. cloud computing, social media, etc.)</td>
</tr>
<tr>
<td>Talent Management</td>
<td>• Develop a procurement team aligned to business needs, organization’s strategic priorities and growth areas and focus on building and retaining high-performing teams</td>
</tr>
<tr>
<td>Affect Revenue</td>
<td>• Promote and develop the bank’s customer portfolio within our supplier community and maximize value to the bank by being thoughtful about our customer/supplier relationships</td>
</tr>
<tr>
<td>New Risk Domains</td>
<td>• Extension of the Third Party Risk Management to manage additional risk domains beyond Information Security and Supplier Performance (e.g., Reputation, Compliance, or Geo-political Risk)</td>
</tr>
<tr>
<td>4th Party Risk</td>
<td>• Inclusion of 4th Parties in the Risk Management Program, including inventory, assessment and monitoring of 4th Parties (Supply Chain Management)</td>
</tr>
<tr>
<td>M&amp;A / Divestitures</td>
<td>• Ongoing M&amp;A and Restructuring Activities have created new sourcing leverage and necessitated new supply strategies</td>
</tr>
<tr>
<td>Green Value Chains</td>
<td>• Increasingly, customers and governments are demanding firms have plans to make their operations more sustainable and from a more diverse supplier base</td>
</tr>
</tbody>
</table>
Proactive risk management and oversight is an imperative for most organizations.

Third party risk is not a risk unto itself. Rather, it is a combination of other risks with various degrees of severity based on the nature of the relationship with the third party. The potential risk exposure from doing Business with third parties goes well beyond direct financial loss and includes reputational damage, regulatory scrutiny and customer attrition.

The Third Party Risk Domains listed above also apply to fourth parties as an extension of third party risk.
**Overview: Outsourcing and Supplier Risk Management Function at BMO**

<table>
<thead>
<tr>
<th>Tools &amp; Processes</th>
<th>Oversight &amp; Governance</th>
<th>Analytics &amp; Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have controls for identifying, assessing, monitoring and managing outsourcing and supplier risk through a framework and SEMS management tool;</td>
<td>We have developed the three lines of defense operating model, consistent with BMO’s Enterprise framework and instituted a Governance Oversight Committee for the US;</td>
<td>We have refreshed our risk appetite statement and enhanced our reporting capabilities to monitor our risks;</td>
</tr>
<tr>
<td>a. Established end-to-end Outsourcing and Supplier Risk Management Framework</td>
<td>a. Roles of three lines of defense identified</td>
<td>a. Defined risk appetite statement and associated dashboards and KRIs</td>
</tr>
<tr>
<td>b. Supplier Engagement Management system (SEMS) enables supplier intake and risk assessment</td>
<td>b. Governance committee in place, initial focus on US, currently expanding to enterprise</td>
<td>b. Data Analytics and Consumption in SpotFire for drill-down analytics</td>
</tr>
</tbody>
</table>
Development of controls for identifying, assessing, monitoring and managing outsourcing and supplier risk through a framework and SEMS management tool.

1a End-to-End Outsourcing and Supplier Risk Management Framework

- We have implemented an **Outsourcing and Supplier Risk Management Framework** across the enterprise.
- The framework shows an end-to-end view of the processes, structures, controls and systems that are used to manage outsourcing and supplier risk.
- This framework is leveraged throughout the Supplier Lifecycle as set out in the Outsourcing and Supplier Risk Management Corporate Standard.
- Applies consistent onboarding and management methods for outsourcing and supplier arrangements.

1b Supplier Engagement Management System (SEMS)

- All new, renewing and amending supplier arrangements, in addition to significant changes in current agreements must be entered in to SEMS.
- This centralized tool assesses the associated risks – per risk type and in the aggregate – resulting in a risk rating that is used to inform supplier management and oversight.

Outsourcing and Supplier Risk Management Framework

- Preliminary Assessment Questionnaire (PAQ)
- Workload Planning
- Opportunity Strategy
  - Market Intelligence
  - Customer as a Supplier Assessment
  - Supplier Diversity
  - Supplier Engagement Questionnaire (SEQ)
- Stakeholder Engagement
- Due Diligence
- Contract
- Manage
- Renew / Terminate

Supplier Engagement Management System (SEMS) licensed from Hiperos

SEMS is the enterprise tool to identify, assess, manage and monitor outsourcing and supplier risk throughout the supplier lifecycle.

- **Identification**
- **Measurement**
- **Management & Mitigating**
- **Monitoring & Reporting**

Workflow ● Repository for pre-defined artefacts ● Notifications ● Track open items ● Reporting ● Analysis ● Change Management
Supplier Management Lifecycle Framework

Key objectives of the framework include:
- Identification of Risks
- Measurement of Risk Impact
- Management and Mitigation of Risks
- Monitoring and Reporting of Risks

### Supplier Management Lifecycle

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Supplier Selection</th>
<th>Due Diligence</th>
<th>Contract</th>
<th>Manage</th>
<th>Renew / Terminate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Preliminary Assessment Questionnaire (PAQ)</td>
<td>• Stakeholder and CSA Engagement</td>
<td>• Corporate Support Area Due Diligence Program</td>
<td>• Contract Development</td>
<td>• Residual Risk Assessment</td>
<td>• Termination or Renewal Strategy Assessment</td>
</tr>
<tr>
<td>• Workload Planning</td>
<td>• Sourcing Strategy (e.g. RFX, auction, or sole source)</td>
<td>• Corporate Supplier Area Contract Controls</td>
<td>• Negotiation Execution</td>
<td>• Residual Risk Reassessment</td>
<td>• Assessment of Arrangement, Market and Business Requirements</td>
</tr>
<tr>
<td>• Opportunity Strategy</td>
<td>• Conditional Award of the Business – Deal Summary</td>
<td>• Proof of Concept Execution</td>
<td>• Conduct Negotiation</td>
<td>• Post-Contract Supplier Management Controls</td>
<td>• Termination and/or Transition Plan</td>
</tr>
<tr>
<td>• Market Intelligence</td>
<td></td>
<td>• Deal Summary Finalized</td>
<td>• Key Risk Indicators</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Customer as a Supplier Assessment</td>
<td></td>
<td>• Risk Approval</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Supplier Diversity</td>
<td></td>
<td>• Contract Execution and Registration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Supplier Engagement Questionnaire</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Governance
- Risk Definitions
- First Principles
- Operational Risk Corporate Policy
- Standard and Framework Effective Quality Assurance
- Risk Appetite Statement
- OSR Corporate Standards
- SPSG Operational Procedures
- Effective Challenge
- Quality Assurance

### Supplier Engagement Management System (SEMS)
- The enterprise tool to identify, manage, and monitor outsourcing and supplier risk throughout the supplier lifecycle
- Workflow
- Repository for pre-defined artefacts
- Notifications
- Track open items
- Reporting
- Analysis
- Change Management
Adopt three lines of defense operating model and ensure roles and accountabilities are established across all three lines of defense.

**Three Lines of Defence to Manage Outsourcing & Supplier Risk**

**First Line of Defense:**
LOB Supplier Manager/Accountable Executive
- Own and manage identified Outsourcing and Supplier Risk for their supplier arrangements
- Maintain overall accountability and oversight of the relationship:
  - Set the strategic direction of the supplier relationship
  - Make key decisions pertaining to the supplier relationship
  - Resolve any escalated issues

**Second Line of Defence:**
1. SPSG & Outsourcing and Supplier Risk CSA
   - Provide subject matter expertise, specialist support, and independent risk oversight of Outsourcing and Supplier Risk
   - Quality Assurance and Effective Challenge roles in place
   - Develop and implement the Outsourcing & Supplier Risk Management
   - Managed through our SEMS tool
2. CSAs
   - Provide inherent, residual risk assessment and due diligence for their domain of risks
   - Assess implications of vendor risk to their risk domain

**Third Line of Defence:**
Corporate Audit
- Provide an independent assessment of the effectiveness of the internal control environment in 1st and 2nd lines
- Provide timely independent reporting to senior management that assesses whether key control activities are operating effectively and reliably. For example, determining whether there is:
  - Effective supplier risk identification and due diligence
  - Appropriate contract controls
  - Adherence to applicable regulatory guidance
  - Appropriate ongoing supplier management and oversight
  - An effective challenge to the first line and second line that includes escalation processes
Institute a Vendor Management Risk and Operations Committee to provide oversight on supplier risk across all aspects of the Supplier Lifecycle.

### Key Governance Model Elements

**Vendor Management Risk and Operations Committee**
- The Vendor Management Risk and Operations Committee (“VMROC”) is accountable for providing oversight and governance on supplier risks.

**Operational Oversight**
- The Enterprise Supplier Governance (ESG) team members and corporate support areas conduct regular effective challenges on the validity, quality and integrity of the data uploaded within SEMS.
- Hard challenges are then uploaded in to the tool to ensure we demonstrate where we have satisfied areas of concern.
- ESG developed the Standard Operating Framework that articulates the key components and requirements of effective post-contract governance, oversight, and monitoring of Enterprise Critical Suppliers.
- The Framework outlines high level responsibilities and the interaction model between Supplier Management teams, Enterprise Supplier Governance, and Corporate Support Areas.

**Quality Assurance (QA)**
- Two Quality Assurance roles, were created to monitor and ensure completion of effective challenges by Outsourcing & Supplier Risk CSA to perform risk oversight on outsourcing and supplier risk.
- Their quarterly assessments are in compliance with the OSRM Corporate Standards and annual review of framework controls.
Develop a risk appetite statement and enhanced reporting capabilities to allow for increased oversight and governance of the portfolio.

**Defined Risk Appetite Statement and KRI**

- Strives to adhere to the letter and spirit of all regulatory obligations relating to vendor risk. We seek to have no significant instances of regulatory breach.
- We recognize that there is vendor risk inherent in our businesses. Based on our strategy and business practices, we are targeting a moderate* risk appetite.
- We will mitigate exposures that can adversely impact our critical activities, have a disruption to regular business operations, and negatively impact our customers. We will proactively and continuously improve our vendor / supplier risk framework.

**Data and Analytics**

- We have selected SpotFire, a data visualization program, as our enterprise tool to provide risk reporting across the following dimensions:
  - Portfolio view of risks to identify and monitor high, medium, and low risks.
  - Ability to deep dive into engagement data and KRI to understand risk drivers.
  - Enhanced Risk Portfolio dashboard provides a comprehensive view on the Bank’s current risk exposure across key KRI areas. The dashboards are released to VMROC members monthly and are a key input into the OSR CSA Report.
This dashboard articulates how we measure risk through key performance indicators (KRIs), our risk tolerance as defined by the risk appetite and where each LOB and geography stands in relation.

**Vendor Risk Appetite Statement**

We aim to monitor KRIs across the Enterprise Framework, Engagement and Vendor Management processes to understand and mitigate the disruption that vendors can cause on the Bank’s ability to conduct business.

### OSR KRI Dashboard

**Effectiveness of Control Dimensions**

- How a LOB/geography is doing relative to each of the risk dimensions

**Residual Risk Heat Map**

- What proportion of a LOB’s/geography’s vendors are high, medium or low risk

**Risk Trends**

- How a LOB/geography is trending over time across KRIs
On-going Supplier Management: Evolution of the SRM Playbook to the Standard Operating Framework

Based on input from Supplier Manager Teams during the Pilot in October 2014, ESG distilled the SRM Playbook into a more outcome-focused and user-friendly Standard Operating Framework, which was published in December 2014.

**Guiding Principles**

**SRM Playbook**
- Defined Supplier Management processes, roles and responsibilities, tools and templates for the post-contract management of BMO’s most critical suppliers
- Aggregation of best practices for post-contract supplier management into specific management activities
- Emphasis on prescriptive practices for supplier management

(Published August 2014, Retired and replaced by the Standard Operating Framework December 2014)

**Standard Operating Framework**
- Defined Supplier Management processes, roles and responsibilities, tools and templates for the post-contract management of BMO’s most critical suppliers
- Distillation of best practices for post-contract supplier management into management outcomes
- Emphasis on output / interaction across constituents vs prescriptive process steps

(Published December 2014)