Ever-increasing operational complexity in the wake of a financial crisis tied to high-profile financial fraud makes controlling risks a top priority for the financial services industry. Over the years, financial institutions have invested in stringent controls and robust Operational Risk Management (ORM) programs and frameworks, and these programs and frameworks have been implemented broadly within the financial services industry. Recently, however, in light of technological advances, trends in globalization, and new regulatory requirements, financial institutions are reconsidering the effectiveness of current ORM frameworks and programs.
Operational Risk Management (ORM) framework

The 2008 financial crisis substantially increased the level of regulatory scrutiny on firms in the financial services industry. Within the industry, one consequence of this heightened regulatory awareness was widespread usage of third parties to carry out material business activities. In response, regulatory agencies, including the Federal Deposit Insurance Corporation (FDIC), Federal Reserve, Office of the Comptroller of the Currency (OCC) and Consumer Financial Protection Bureau (CFPB), issued guidance on managing what is now commonly called third-party risk, a subcategory of operational risk. Today, regulatory agencies have formally stated that, while an institution can rightfully outsource a business activity to a third party, it cannot outsource its institutional risk or compliance responsibilities for that business activity. In other words, financial institutions are now held accountable for the actions of their providers, including compliance and safety related to products and services delivered. This has led companies to develop, and incorporate into ORM frameworks, a variety of programs, policies, and practices specifically concerned with selecting, managing, monitoring, and terminating third-party relationships. Of the many types of third parties—diverse, too, in the range of their impacts on organizations—joint ventures (JVs), in particular, are liable to introduce systemic third-party operational risk to financial institutions. But incorporating the operational risk inherent within a JV into an ORM framework can be challenging for many reasons, including:

• Lack of binding clauses in contracts that lay responsibilities of JV partners to implement an effective ORM framework
• Upfront costs associated with creating an ORM framework
• Lack of clear guidelines or regulations to drive scope and timeframes for implementation of ORM frameworks for JVs

ORM frameworks for Material Operating Groups and Entities (MOGEs)

Basel guidelines state: “A bank’s Operational Risk Management Function (ORMF) is also expected to apply to all of a bank’s material operating groups and entities, including subsidiaries, joint ventures, and geographic regions.” MOGEs, in this definition, include any entity (or entities) which has (or have) material operational, financial, regulatory, or reputational impact on an organization. Thus, it is imperative for organizations to have robust processes in place to identify MOGEs. Financial institutions should consider the following illustrative factors when identifying material joint venture relationships:

• **Controlling interest** – whether the entity is a consolidating or non-consolidating JV
• **Use of common brand or logo** – poses reputational risk if JV uses same branding
• **Equity investment percentage** – risk is directly proportional to investment percentage
• **Business impact on dollar value** – business P&L impact or revenue reliance on JV may develop additional assessment parameters based on the nature and complexity of the business environment and use of JVs

Identifying MOGEs isn’t always easy. Business and risk leadership in general dedicates significant time to developing the right set of parameters and scales, based upon the organization’s risk appetite. A strong framework for arriving at the MOGE would have a twofold impact:

• Provides a list of JVs to concentrate on with greater focus
• A focused approach on material JVs that includes development of an operating model and structure to determine operational risks, necessary controls, and parent involvement
Prioritizing MOGEs

Each JV is unique in its own way and helps fuel an organization’s growth. Risk should be assessed across different domains as listed below for each MOGE. The following factors should be considered while prioritizing MOGEs:

- **Strategic**: Evaluation of strategic impact relating to the organization’s mission and strategic objectives which are posed by JVs
- **Compliance**: Evaluation of compliance risks considering laws and regulations, policies and procedures, ethics and business conduct associated with the JV
- **Internal audit**: Evaluation of risks related to value drivers of the organization covering strategic, financial, operational and compliance objectives
- **Financial**: Evaluation with respect to materiality impact on organizational financial statement
- **Fraud**: Evaluation of potential instances of fraud at JV that could impact organization’s ethics and compliance standards
- **Credit**: Evaluation of potential that JV would fail to meet its obligations in accordance with agreed terms and the liability would fall on parent organization
- **Customer**: Assessing the risk and impact of a JV as a customer on organization’s revenues and net profits
- **Supply Chain**: Assessing the risk associated with identifying the inputs and logistics needed to support the creation of products and services
- **Security**: Evaluation for potential breaches or data integrity issues regarding the financial institution’s confidential data
- **IT**: Evaluation of potential technology system failures, dependency on the JV, and the organization’s return on information technology investments in the JV

Implementation approach for an ORM program

It’s important to note that prioritization of MOGEs helps in phased implementation of an ORM framework. During implementation, organizations can leverage preexisting operational risk or enterprise risk management frameworks for efficient implementation and shorter turnaround time. Organizations may find it useful to assess and cross-leverage ORM frameworks with the JV.

Where the partnering organization is not regulated, or not a part of the financial services industry, the implementation process is far more complex. In such scenarios, any existing Enterprise Risk Management (ERM) frameworks could be leveraged to develop a customized operational risk program. While the scope of ERM is very large, most global organizations follow COSO’s ERM framework. Key components of an ERM framework that can typically be leveraged are:

- **Risk assessment and identification**: Risk identification provides opportunities, indicators, and information that allow an organization to identify and ensure remediation of major risks before they adversely affect the JV. The partnering organization’s top-down risk assessment can be leveraged to understand its risk profile, and processes directly impacting the JV can be reviewed. Other key sources to assess the risk profile of the partnering organization could be reports/minutes from audit/risk/governance committees and assessments of the organization’s internal controls assurance framework. If significant differences exist between the Inherent and Residual risk of the partnering organization, it should be supported with a comprehensive and robust controls assurance program.

- **Internal loss data**: This data can be based on the risk profile and size of the JV. Two thresholds could be established with a lower
threshold for events directly impacting the JV and its associated processes and a higher threshold for any significant loss event within the organization that could directly or indirectly impact the JV. To avoid double counting of the losses, organizations should only capture losses commensurate with their stake in the joint venture.

- **External loss data**: Organizations should customize their external loss reports to include any events that pertain to their JVs.

- **Scenario analysis**: This can be performed in a workshop setting involving the leadership team and all organizations associated with the JV.

- **Key Risk Indicators (KRI)**: Risk assessments, internal/external loss events, and scenario results can be leveraged to identify KRI s for the JV.

**Key principles for establishing ORM frameworks**

Operational risk is just as important as market risk and credit risk for all MOGEs. Management's involvement is critical when considering embedding operational risk management into the institution's culture. In addition, roles and responsibilities should be clearly defined, and procedures put in place outlining how the ORM program has been customized as well as how it integrates with the ORM framework. ORM also should identify how the program is being monitored and reported to the leadership and its effect on capital calculations. Based on the prioritization of MOGE's, organizations can roll out operational risk management frameworks in a phased manner covering a few program elements at a time, as shown in the illustration below:

![Diagram](image)
A broadened regulatory landscape demands that organizations focus beyond conventional boundaries of risk management and start thinking more critically about ORM frameworks as they relate to third parties. An effective approach for rolling out a revised ORM framework includes:

- Identification and development of a comprehensive list of material entities (including JVs) within the organization’s overall risk profile
- An upfront view of the end state for identified entities in terms of people, processes, products, services, and systems
- A prioritized list of JVs based on their criticality to the organization
- Cross-leveraging existing ORM or ERM frameworks for more effective and efficient implementation

By following this approach, organizations can better manage operational risks that come with the third-party relationships essential to today’s increasingly competitive business environment.