Supplier Risk Management

Schulmynn Leung
Manager, Supply Chain Strategy & Operations
Supplier Risk Management

Background

What is Supplier Risk Management?
A systematic approach to identify, assess, and mitigate risk in PG&E’s supply base. Today, Supplier Risk Management is an industry best practice that world class organizations have adopted to reduce vulnerability and ensure continuity.

What are examples of situations that left unidentified would negatively impact PG&E’s ability to provide services for our customers?

- A sole source supplier of a key product or service goes out of business (or refuses to supply PG&E) suddenly and without warning due to natural disaster, terrorist act, regulatory shut down, or financial weakness.
- Critically licensed software is suddenly made unavailable for use at PG&E due to contractual terms or failure of the company licensing the software to PG&E.
Supplier Risk Management Process

Step 1: Define Supplier Population
Purpose: Identify population of suppliers in Supplier Risk program

Step 2: Risk Segmentation Model
Purpose: Evaluate each supplier through an initial risk segmentation analysis - providing a consistent and efficient means for PG&E to segment existing or potential suppliers

Step 3: Risk Scoring Model - Inherent Input
Purpose: Identify Supplier risks inherent to the material / service being purchased

Step 4: Control Effectiveness & Residual Subtotal
Purpose: Evaluate effectiveness of supplier (or supplier candidates) to manage inherent risks

Step 5: Residual Risk: Mitigation
Purpose: Ensure that suppliers are appropriately monitored, managed, and reported on throughout the supplier lifecycle

Step 6: Off boarding
Purpose: Ensure that the risk management process off-boards suppliers who are no longer providing services/products to PG&E
**Purpose:** Identify population of suppliers in Supplier Risk program

**Scope:** Any supplier who conducts business with PG&Es can be considered in scope for the program, but emphasis is placed on those considered:

<table>
<thead>
<tr>
<th>Enterprise Strategic</th>
<th>Portfolio Preferred</th>
<th>Valued</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical/Sole Sourced Suppliers.</td>
<td>Suppliers that engage in any high risk activities defined by category management.</td>
<td></td>
</tr>
</tbody>
</table>
Supplier Risk Management Background

Supply Chain Risk - Program Growth - Number of Suppliers

- 2012: 57 suppliers
- 2013: 208 suppliers
- 2014: 576 suppliers
**Purpose:** Evaluate each supplier through an initial risk segmentation analysis - providing a consistent and efficient means for PG&E to segment existing or potential suppliers.

**Scope:** Each supplier rated ‘critical’ or ‘high’ in the Risk Segmentation Model (Step 2) gets a secondary risk segmentation analysis leveraging the Supplier Risk Scoring Model (Step 3), this is conducted annually to validate / update supplier placement, and for each new supplier or service added.
**Purpose**: Identify Supplier risks inherent to the material / service being purchased.

**Scope**: Each supplier rated ‘critical’ or ‘high’ in the Risk Segmentation Model (Step 2) gets a secondary risk segmentation analysis – this provides the supplier’s ‘inherent input’ score. This score assesses each supplier’s risk without taking into consideration any mitigation or controls that are currently in place.

This uncontrolled risk score is referred to as Inherent Risk. The Inherent Risk score is calculated without the input of the supplier and is focused on four major risk categories:

- Financial
- Operational
- Regulatory/Reputational
- Information Security
## Step 3 - Inherent Risk Assessment

<table>
<thead>
<tr>
<th>Category</th>
<th>Supplier risk areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial</strong></td>
<td>Financial impact</td>
</tr>
<tr>
<td></td>
<td>Supplier viability</td>
</tr>
<tr>
<td><strong>Operational</strong></td>
<td>Business continuity</td>
</tr>
<tr>
<td></td>
<td>Supplier market</td>
</tr>
<tr>
<td></td>
<td>Operational risk</td>
</tr>
<tr>
<td><strong>Regulatory/Reputational</strong></td>
<td>Supplier location</td>
</tr>
<tr>
<td></td>
<td>Regulatory exposure / reliance</td>
</tr>
<tr>
<td></td>
<td>Reputational exposure</td>
</tr>
<tr>
<td><strong>Information Security</strong></td>
<td>Confidential data</td>
</tr>
<tr>
<td></td>
<td>Supplier PG&amp;E systems access</td>
</tr>
<tr>
<td></td>
<td>Managing critical PG&amp;E records</td>
</tr>
</tbody>
</table>
**Purpose:** Evaluate effectiveness of supplier (or supplier candidates) to manage inherent risks

**Scope:** How is the Residual Risk score calculated?

Control Effectiveness is assessed based on the status of the supplier in various PG&E internal control programs as well as completion of a risk questionnaire by the Supplier.

Once all of the controls are identified and evaluated, a “Residual Risk” score is calculated based on the strength of the controls in place.
Step 4 – Controls Reviewed

Financial
- Completion of PG&E Credit Risk Review
- Valid Insurance certificates loaded In Exegis

Operational
- Supplier Registration in PICS Auditing system
- Formal risk management program policy
- ISO 9001 certification
- Business Continuity Plan & Test Results
Step 4 – Controls Reviewed

Regulatory/ Compliance
- Compliance manuals and procedures
- Hazardous waste disposal policies
- Compliance and ethics training program policy

Technology/Information Security
- Completion of PG&E’s Third Party Security Review (TSR)
- ISO/IEC 27001 certified
- Information classification policy
Final Residual Risk Scores fall into four risk ratings:
- Critical
- High
- Medium
- Low

This Residual Risk Score along with the Inherent Risk score may be shared with Suppliers during periodic Scorecard reviews.
Now that each supplier has a Residual Score Rating we take the following actions to further mitigate the risks:

- PG&E will collaborate with Suppliers having a Critical or High Residual Score Rating to develop specific action plans to further mitigate the risks and which may require an on-going review and monitoring of the supplier’s risk.
Questions

For future questions or concerns regarding PG&E’s Supplier Risk Program:

Brendan Kearney (415-973-1329) OR
Schulmynn Leung (415-973-7277) OR
PGESupplierRisk@pge.com