

Resource Management Group

Managing the Operational Risks of Outsourcing

November 21, 2003

Agenda

- External IT Sourcing: Risk Complexity
- Morgan Stanley Background
- Risk Framework
 - Country Risk
 - Vendor Risk
 - Consultant Risk
- Review
- Discussion

External IT Sourcing: Operational Risk Complexity

- Power & Communication Outages
 - East Coast power outages
 - Undersea cable outages in India
- Terrorist Threats
 - Car bombings in Mumbai
 - Kidnappings in the Philippines
- Geo-political Tension
 - India and Pakistan political posturing

Morgan Stanley Background

- Business / Corporate Culture
- Component of overall resource management portfolio
- Co-sourcing vs. Outsourcing Model
- Multi-year, phased approach
- Resource Management Group
 - Client Coverage
 - Vendor Coverage
 - Legal / Risk Management
 - Operations / Administration

Risk Framework

- Focus on Operational Risks
- Review Individual Risks
 - Risk Definition
 - Examples
 - Mitigation Factors
- Rank Probability & Severity

Country Risk: Regional/Geo-political Concerns

- **Definition:** Risks associated with working outside the US, such as terrorism, border disputes, regulatory requirements, and political bureaucracy
- **Examples:** Philippine terrorists, India/Pakistan tensions, travel restrictions
- Mitigating Factors
 - Encourage vendors to have multiple location diversity
 - Choose a globally diversified vendor portfolio: offsite, offshore, nearshore
 - Construct an application-by-region risk assessment matrix
 - Define client “back sourcing” program
 - Create a network of regional information sources

Vendor Risk: Vendor Viability

- **Definition:** The risks/uncertainty associated with working with vendors. Are they properly managed? Are they properly funded?
- **Examples:** PSI Net / Metamor bankruptcy filing
- Mitigating Factors
 - Give proper weighting to public companies when selecting partners
 - Define client “back sourcing” program
 - Perform annual vendor financial audit w/ quarterly updates
 - Document, communicate, and test vendor BCP plans

Vendor Risk: Infrastructure

- **Definition:** Few countries have infrastructure capabilities comparable to those of the US and Western Europe. Major components of such an infrastructure include: power, telecommunications, water, HVAC, and transportation
- **Examples:** Undersea cable interruptions for telecommunications in India and frequent power outages in both India and the Philippines.
- Mitigating Factors
 - Establish fully redundant data communications network
 - Maintain multiple-day water supply
 - Separate grid and entry point for electrical supply
 - Ensure full backup power generation, with fuel storage capacity and supply contracts
 - Encourage vendors to have multiple location diversity
 - Define client “back sourcing” program

Vendor Risk: Information Security

- **Definition:** Extending your company's network beyond its four walls will increase the risk of sensitive information and/or intellectual property being leaked to the public
- **Examples:** Data and voice networks are quite susceptible to eavesdropping when your network extends to your offsite vendors
- Mitigating Factors
 - Create a secured workspace – a company within the company – to isolate offshore staff
 - Require an encrypted data network – a physically isolated “air gapped” network
 - Document a security policy – drafted with security, internal audit, and the resource management group to define security policy and procedures
 - Conduct annual vendor security audits

Vendor Risk: Business Continuity/Disaster Recovery

- **Definition:** Many organizations overlook their outsourced resources in their official BCP and DR plans. As this population grows, however, it becomes critical to define BCP / DR plans for this group and, if possible, to formally include them in the firm's official plans
- **Examples:** Building collapses, typhoons, power outages, etc.
- Mitigating Factors
 - By vendor, build an infrastructure risk assessment – from this information, construct BCP plans
 - Document, communicate and test vendor BCP plans
 - Formally integrate vendor BCP plans
 - Define client “Back Sourcing” program – human capital is always the most critical asset

Consultant Risk: Information Security

- **Definition:** Protecting corporate information from outsiders is more obvious than protecting it from insiders. From an information security perspective, how does a company protect itself from its consultants?
- **Examples:** The leaking of inside information regarding mergers and acquisitions or internal compensation could damage a firm's reputation and/or carry severe financial penalties. This type of information must be adequately protected
- Mitigating Factors
 - Establish background checks/drug testing for consultants
 - Have consultants review and sign:
 - Vendor code of conduct
 - Stock trading policy
 - Sensitive information policy
 - Web & email usage policy
 - Scramble sensitive data

Consultant Risk: Human Capital

- **Definition:** Especially in a co-sourcing model, people are the most critical component for success. Constant switching of staff will almost certainly spell failure for the initiative
- **Examples:** In both the Philippines and in India, many look forward to the opportunity to work overseas. The trend has been to get several years of experience locally and then leave for better opportunities abroad
- Mitigating Factors
 - Pay close attention to vendors' turnover rates; compare with industry benchmarks
 - Understand the vendors' incentive structures and match to your sourcing model
 - Ensure access to and ownership of proper systems documentation at all times
 - Define client "Back Sourcing" program


Managing Offshore Risk: Review

- Every sourcing strategy has limitations
- Risk Management needs to be an iterative process
- Hold everyone to the same standards
- Offshore outsourcing will bring a new set of challenges to your organization
- Do not abdicate your role in managing outsourcing risk
- Human Capital is always the most critical asset – and the most difficult to replace
- Create the necessary feedback loops to be able to make the difficult decisions

Managing Offshore Risk: Next Steps

- Build globally diversified vendor portfolio
- Create the necessary documentation
 - Project “back sourcing” plans
 - Application-by-region matrix
 - Security requirements & policies
 - Infrastructure risk assessment
 - BCP / DR plans
 - Vendor code of conduct
- Conduct Security & Financial Audits
- Integrate vendor BCP & DR plans and test regularly

Discussion

- 
- 9:15-9:40 – Case discussion breakout groups
- 9:40-9:50 - Break
- 9:50-10:00 – Breakout group presentations
- 10:00-10:30- Open Discussion and Comments