

# Enterprise Risk Management (ERM) for IT - Projects & Accounts

---

4<sup>th</sup> May'2008

# High Level Overview

---

- Why to adopt the Portfolio Approach for Managing IT Risks
- ERM Framework for IT Risk Management
  - Approach & Framework
  - Risk Profiling by Criteria
  - Risk Quantification - Operational Risk Index
  - ERM Process
- Risk Management
  - Assessment, Reporting, Communication & Mitigation
- Enterprise Risks applicable to IT Projects
  - Contractual
  - Infrastructure
  - Customer
- Gain and Pain of Adopting to ERM Approach
  - Challenges
  - Benefits & Value-Add

# Risk Management - Expectation at a high level ...

---

- Higher Risks to be on radar
- Right and Timely responses to the risks
- Setting up a culture to discuss the risks openly
- Shared Language for Risk Communication
- Set up a process to keep the risks in visibility
- Manage the risks with lower visibility
- Understand the evolving nature of risks
- Portfolio way to Manage the risks

# ERM perspective at Industry

---

- A 2005 McKinsey survey of 1,000 directors indicated that 76% wanted to spend more time on risk management
- A recent survey of 271 large companies by The Conference Board and Mercer Oliver Wyman indicated that:
  - 90% are building, or planning to build, ERM
  - 11% have completely implemented ERM
- The companies that have fully implemented ERM reported a high degree of satisfaction:
  - 86% cite better informed business decisions (vs. 58%)
  - 83% cite greater consensus on key risks (vs. 36%)
  - 79% cite increased management accountability (vs. 34%)

## Some questions to be asked at the beginning ...

---

- What are the company's top five IT risks?
- Do we have relevant data on exposures and trends related to these risks?
- Have we defined IT risk at organizational level?
- Are risk policies and risk tolerance limits (applicable to IT Projects and Operations) defined and in place?
- Have the majority of our actual losses and incidents (project failures, application crashes, downtime) been identified?
- Are we managing our business on a risk-adjusted profitability basis?

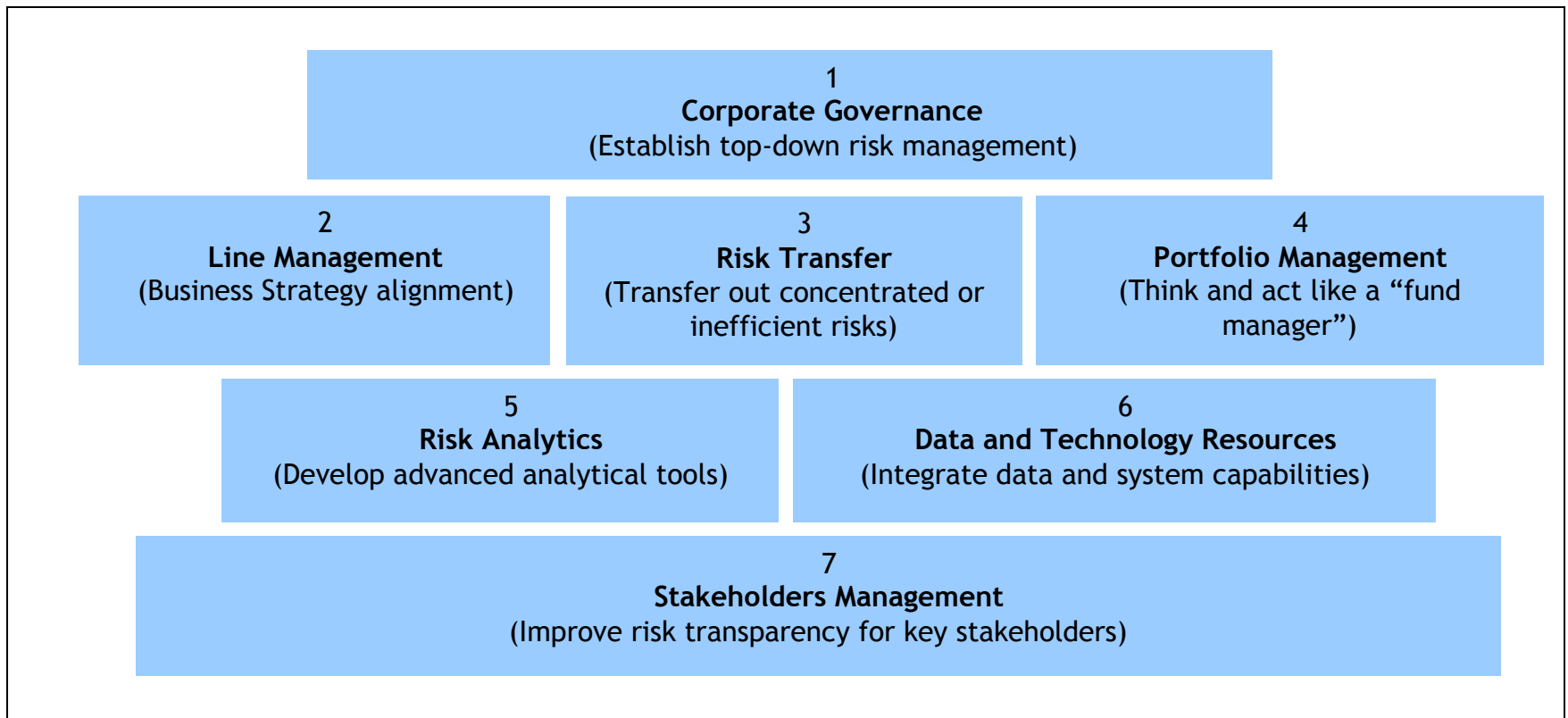
# Why adopt ERM approach for IT Risk Management?

---

ERM Approach is the need of the hour for managing IT Projects

- When an IT Project fails, usually management is the last to know
- The project success rate has got better (from 19% in 1994 to 31% in 2006), yet the project success rate for huge / complex projects is just 3%.
- Typically, the organizations go through the cycles of changes. The impact of these changes to risk mitigation capability should be closely watched
  - Adopting to New Business Models
  - Transitioning to New Project Management Practices
  - Change Management due to advancements in Technology, Communication and Collaboration

# Guiding Risk Management Framework\*



\* *Enterprise risk management: from incentives to controls.* / James Lam (Wiley Finance Series, 2003)

# Guiding Risk Management Framework\* - Contd.

---

- Corporate Governance - To ensure that the board of directors and management have established the appropriate organizational processes and corporate controls to measure and manage risk across the company
- Line management to integrate risk management into the revenue generating activities of the company, including business development, product and relationship management, pricing and so on
- Portfolio management to aggregate risk exposures, incorporate diversification effects and monitor risk concentrations against established risk limits
- Risk transfers to mitigate risk exposures that are deemed too high or are more cost-effective to transfer out to a third party than to hold
- Risk Analytics to provide risk measurement, analysis and reporting tools to quantify the company's risk exposures as well as track external drivers
- Data and technology resources to support the analytics and reporting processes
- Stakeholder management to communicate and report the company's risk information to its key stakeholders.



# Approaches to managing IT risk

---

**POLICING:** Business Units can only operate within risk policies established by risk management and their activities are monitored by risk audits and compliance functions

VS

**PARTNERSHIP:** Business Unit and risk management jointly evaluate and resolve risk management issues and share common goals and objectives

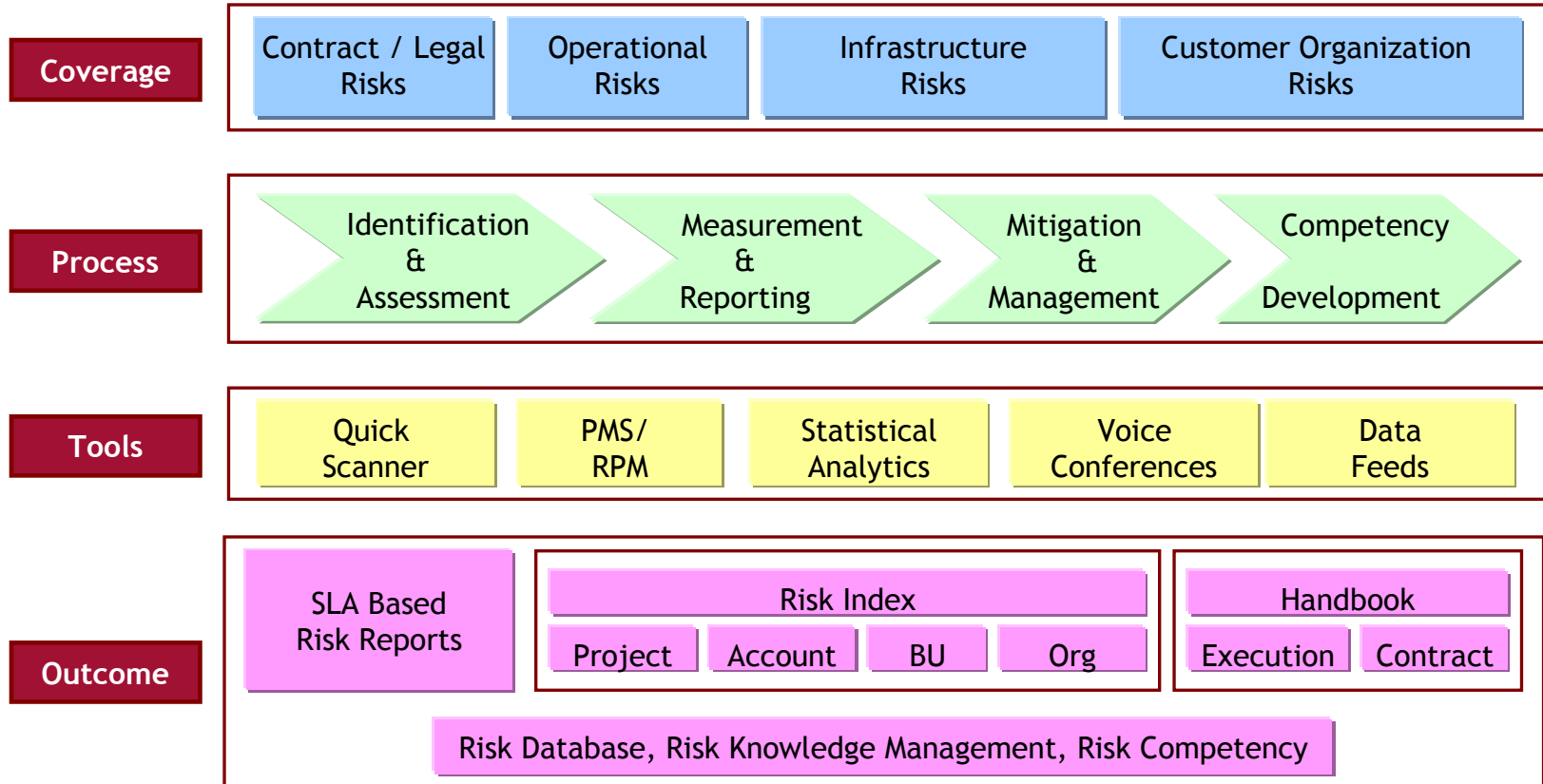
**Partnership ERM model is recommended for initial period**

*“Line Management must recognize the role that risk management plays in supporting long-term performance and stop obsessing over its role in constraining short-term profitability”*

*“Risk Management must recognize the need to understand and respond to line units business needs, not hand down academic, impractical and inflexible policies”*

# Enterprise Risk Management Framework for IT Projects

---



# Selection of Projects for Risk Assessment

---

Organization can focus on select fewer projects for risk assessment based on ...

- Past History of customer
- Business Potential
- Volume of work
- Team Experience on domain/Technology/methodology
- Contract - MSA and SOW
- SLA Commitments and progress
- Customer Dynamism
- Bill Payment Pattern
- CSS ratings
- Resource and Attrition State
- Requirements grasp and scope creep
- Operational Metrics
- Team Morale
- Patni Internal Dynamics
- Audit Performance

# ERM - IT Project Risk Assessment

---

## Risk Categories Considered

- Project Management
- Engineering State
- Contracts & Compliance
- Fraud
- IT Infrastructure
- Relationship
- Business Potential
- Risk Protection
- Customer Dynamism
- Customer Satisfaction
- Competition
- Leadership
- Volume (Size/Efforts)
- Internal Support
- Business continuity
- Talent Pool

### Rating Criteria

Risk Index : Project, Account, Business Unit, Org

- |           |                            |
|-----------|----------------------------|
| • Static  | Historical Performance     |
| • Dynamic | Current State (Time scale) |

# IT Project Risk Profile - Static & Dynamic Criteria

Static*	Dynamic*
Relationship - History, Immediate Past	Financial Metrics
Business Potential	Customer Dynamics
Volume (Size/Efforts)	Stakeholder Satisfaction State
Execution Methodology	Requirements - Grasp and Scope
Technology Experience	Engineering Metrics
Domain Knowledge	Retention State
Business Units - History and Capability	Internal Support
Geography	Team Dynamics
Contract State	Contract Vis-à-vis Execution State

**Flexible, Transparent, Measurable for most attributes**

(\* Sample attributes)

# Project Risk Index

---

- For each risk category, Project or Account Manager should appraise the state in Project MIS.
- The options provided for each risk category should be Flexible, Transparent and Measurable. For example, the options available to risk category “Team’s Competency” can be
  - Half of the team faces challenge new to project technology OR Half of the team is new to project methodology (e.g. RUP, AGILE)
  - Half of the team is new to Project execution model (e.g. production support for the first time or moving from maintenance to development projects)
  - Working hours of more than 45 Hours per week per person
  - No Issues in team competency
- A weight factor can be assigned to each Risk Category and Project Risk Index can be computed based on the options chosen for the risk categories.

# Project Risk Parameters - Risk Index

Risk Group	Risk Attribute	One Time		Monthly		Quarterly	
		PM	BDO	PM	BDO	PM	BDO
Contract	Agreement State						
	Aggressiveness						
	Acceptance Criteria						
Customer	Relationship						
	Attitude						
	Geography						
	Satisfaction						
	Payment History						
Scope/Requirements	Scope (Definition, grasp, stability)						
Team	Attrition						
	PM Competency						
	OSC Competency						
	Team Competency & Work pressure						
Support	Internal Support						
Size	Volume						

# Account Risk Index - Statistical Model - Factors & Calculations

Factors	Description
Account Budget Range ( R )	Project's contribution towards Account revenue
Number of projects (N)	Number of projects in account
Concentration Factor ( C )	Amount of diversification.
Roll up Recommendation	Roll up strategy based (Rolled up raw score)
Account Risk Index (ARI)	Concentration Factor ( C ) x Rolled up raw score

## Quantitative Bands

Risk Level	Project Score		Account Score	
	Score	Percentile	Score	Percentile
High Risk	$\geq \text{MM}\%$	AA	$\geq \text{GG}\%$	KK (Band 4)
Medium Risk	$> \text{NN}\%$ or $< \text{MM}\%$	BB	$\geq \text{HH}\%$ or $< \text{GG}\%$	LL (Band 3)
Low Risk	$> \text{PP}\%$ or $\leq \text{NN}\%$	CC	$\geq \text{JJ}\%$ or $< \text{HH}\%$	OO (Band 2)
No Risk/Risk Free	$\leq \text{PP}\%$	-	$< \text{JJ}\%$	(Band 1)

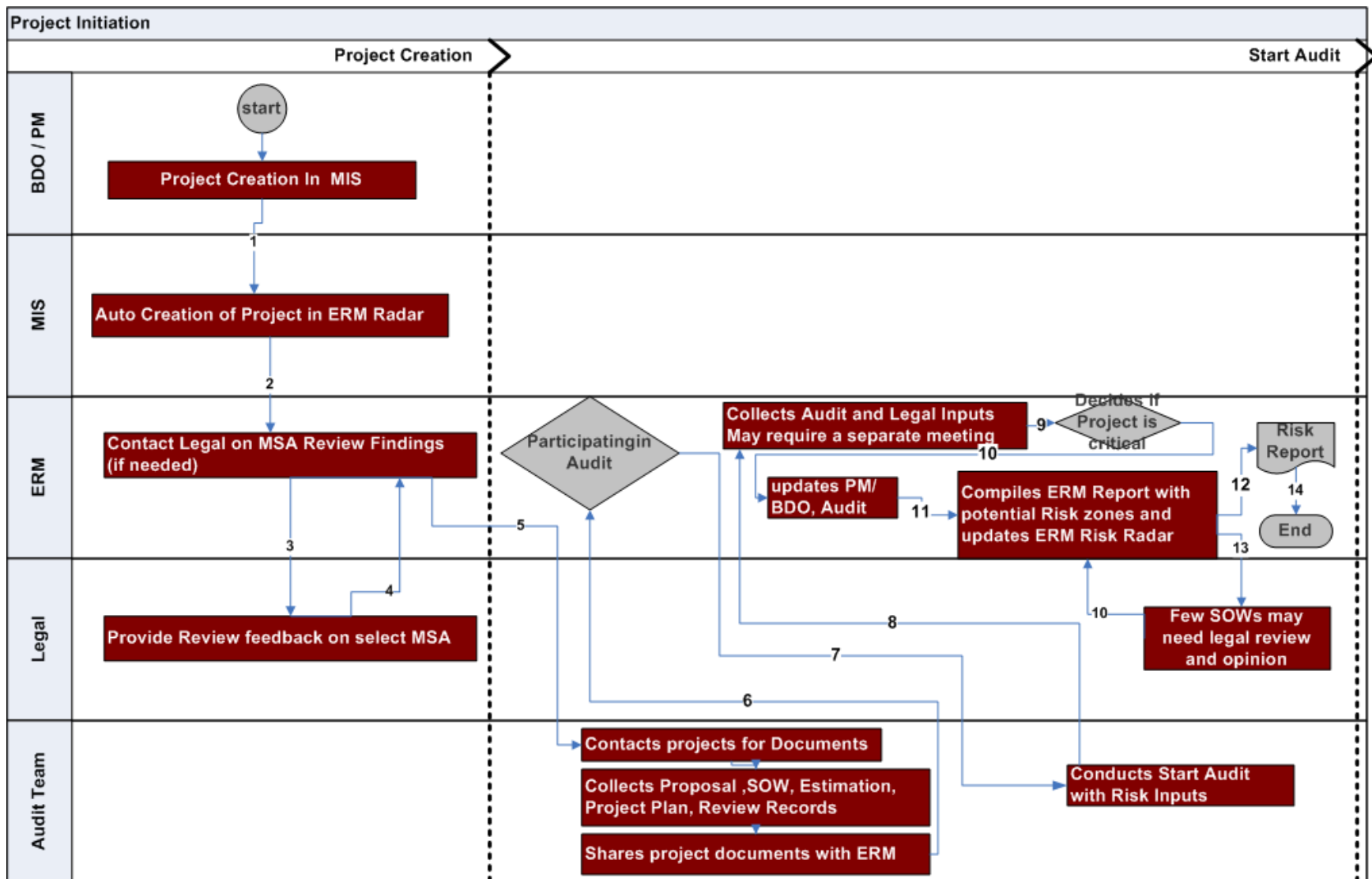


# Project & Account - Operational Risk Indexing

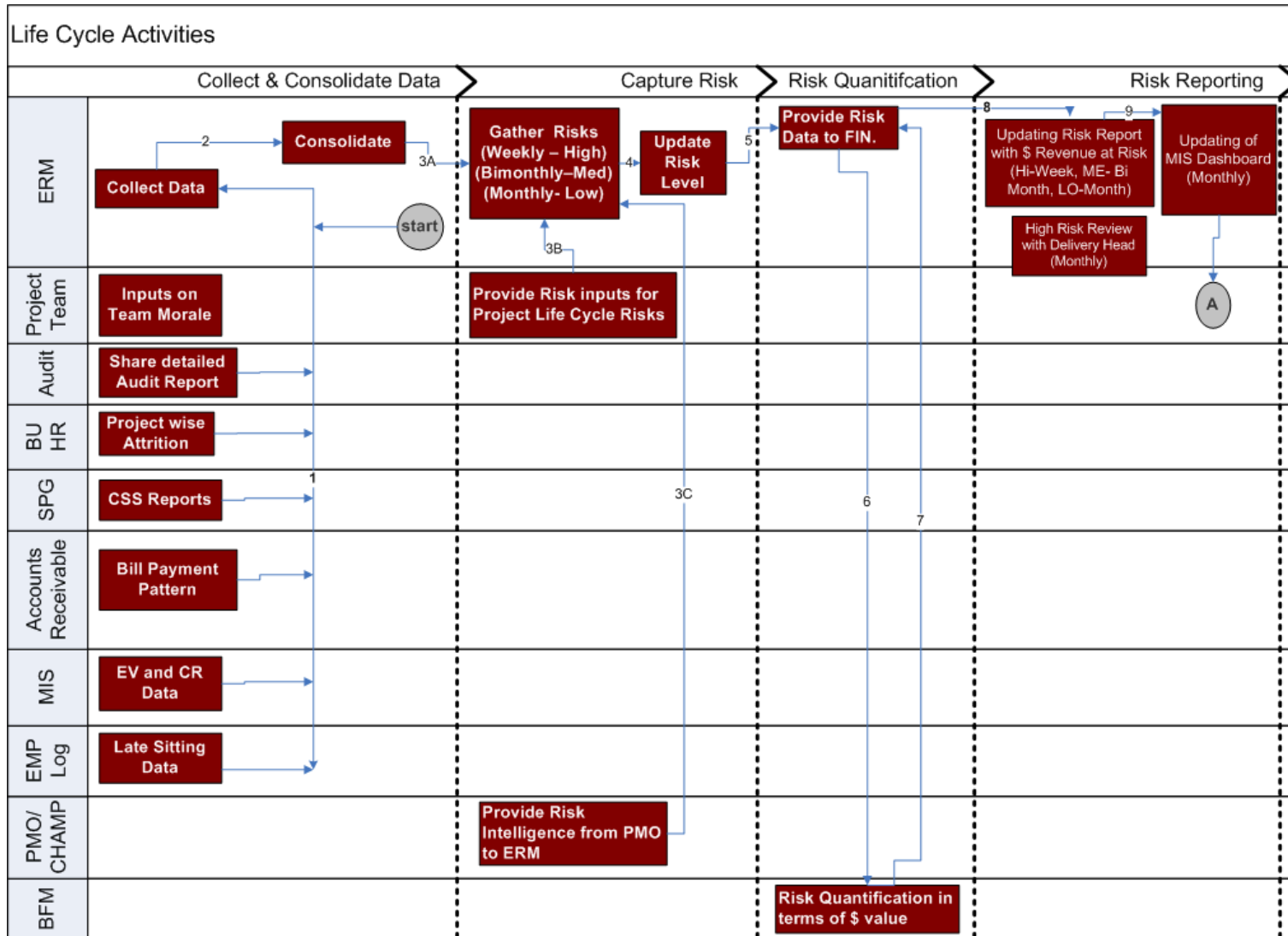
---

- Why Quantify Project / Account Risk?
  - Supplementing Qualitative risk assessment by Quantitative statistical approach
  - Quantitative forewarning to stakeholders based on current operational ecosystem
  - Hierarchical roll up Project -> Account/Program -> Business Unit -> Enterprise
  - Makes it easy to drive the risk model by Statistical Model - blending Qualitative as well as Quantitative inputs
  - Makes it easy to track the risk exposure and risk mitigation capability of the organization.
- Risk Adjusted Revenue Forecast
  - Linear as well as non-linear liability calculations
  - Margin Impact calculators
  - Extending risk framework in business growth space

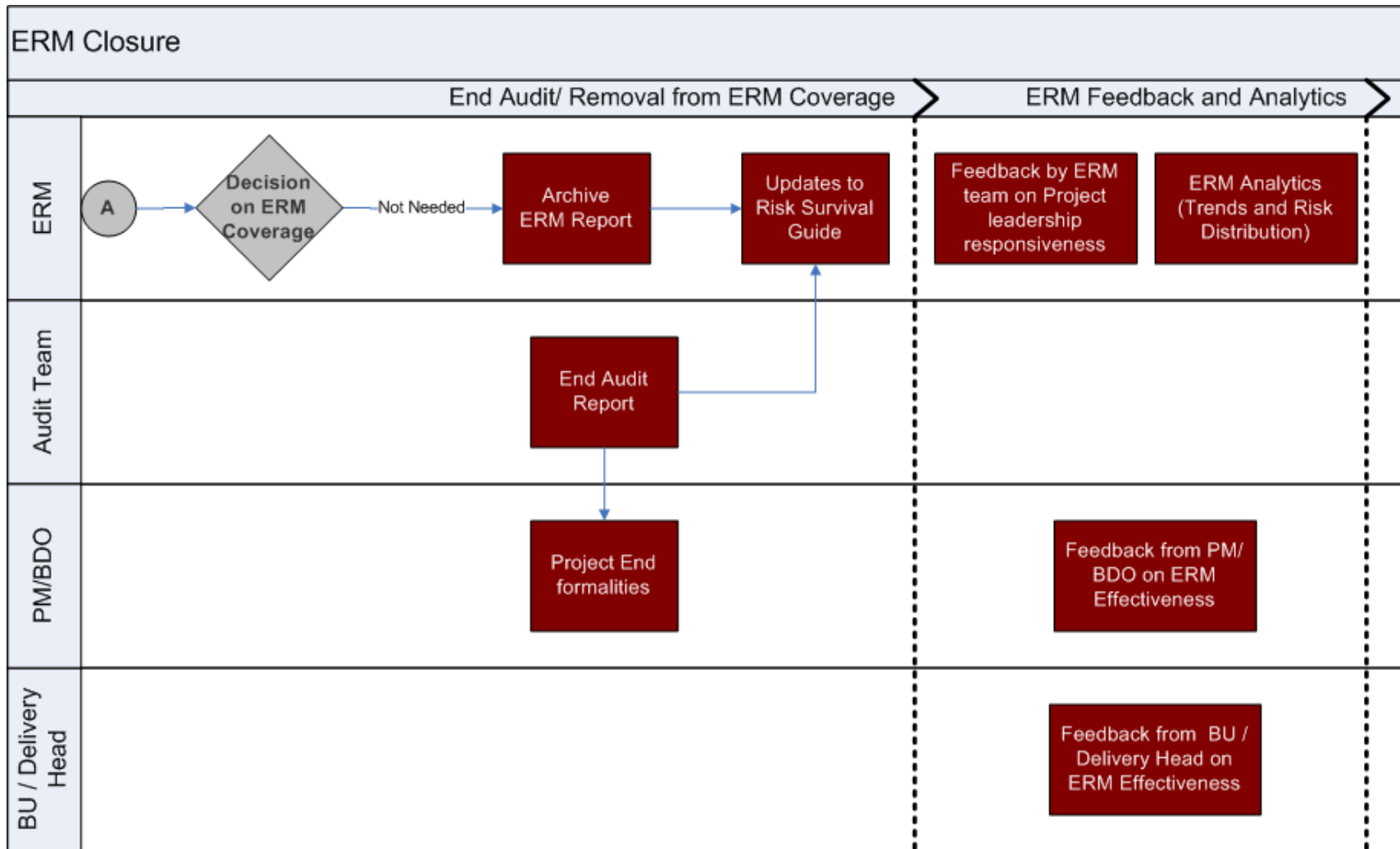
# ERM - Process



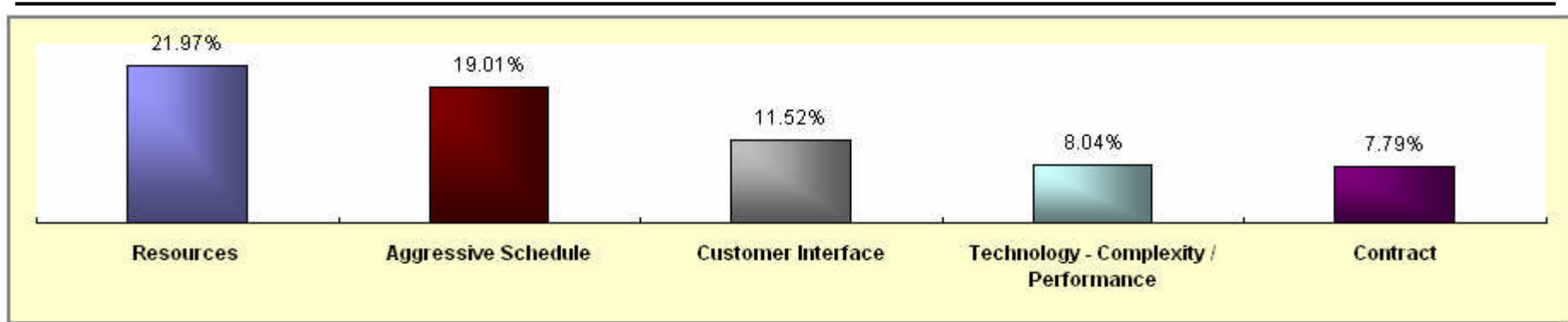
# ERM - Process (contd.)



## ERM - Process (contd.)

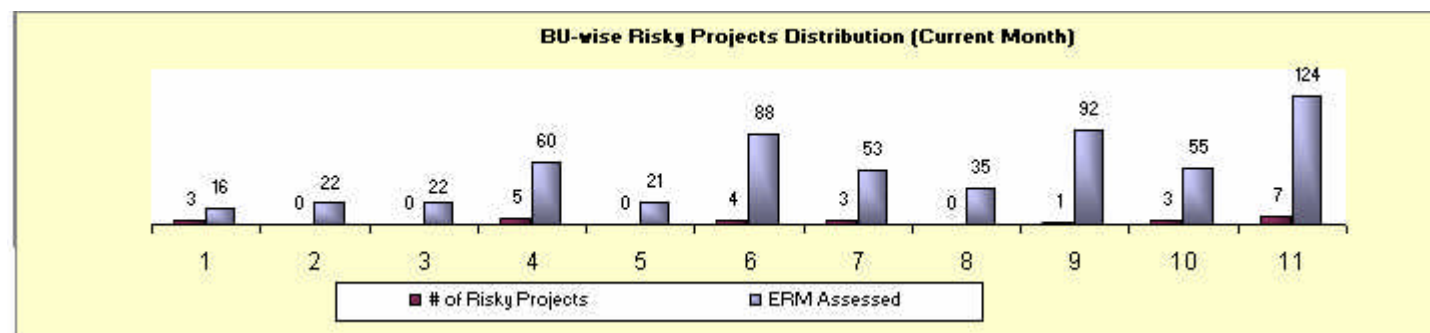
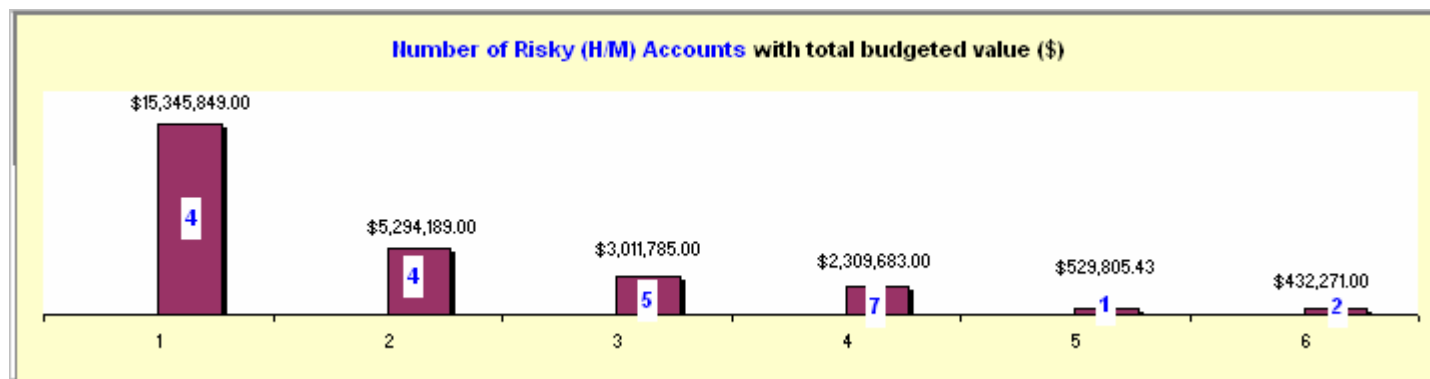
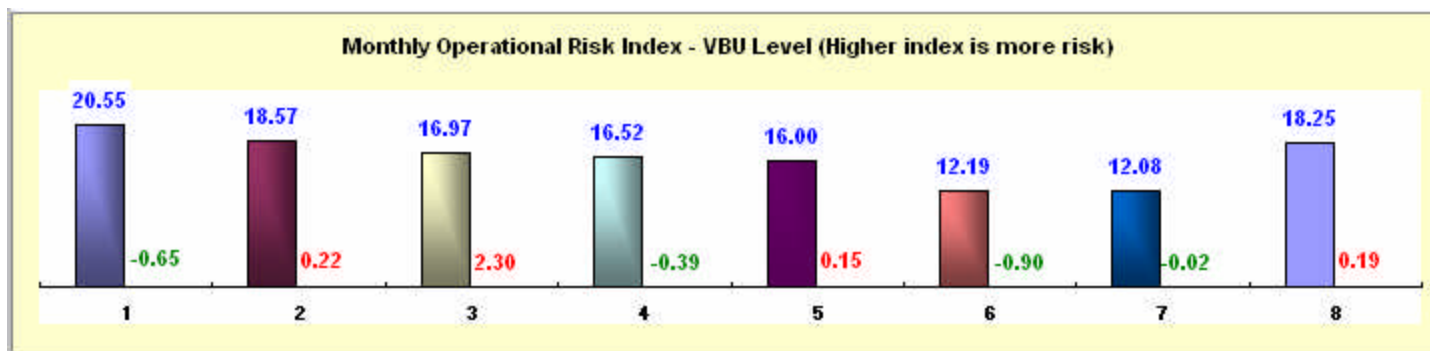


# Sample Enterprise wide - IT Risks

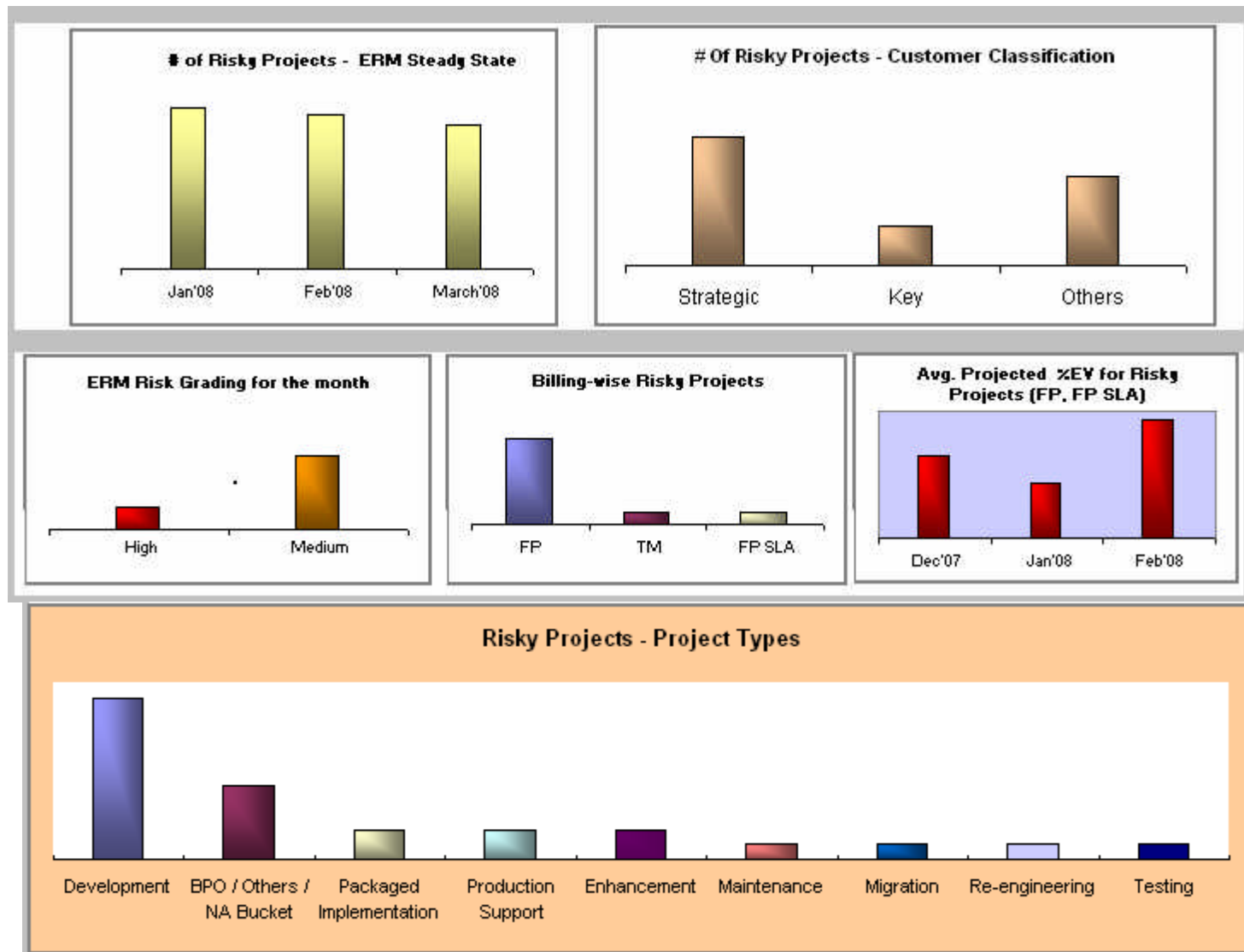


Risk/Concern	Risk Description
Resources	<ul style="list-style-type: none"> <li>• Unavailability of resources with right skills</li> </ul>
Aggressive Schedule	<ul style="list-style-type: none"> <li>• Very aggressive schedule expectations from customer</li> <li>• Moving schedule with no/inadequate development plan to address schedule expectations</li> </ul>
Customer Interface	<ul style="list-style-type: none"> <li>• Sign-offs, Budget/time leakage due to delay in customer decisions</li> <li>• Availability of Hardware/Parts/Licenses/connectivity, test Data, File Formats, Management etc.</li> <li>• Delayed Acceptance</li> </ul>
Technology	<ul style="list-style-type: none"> <li>• Application Performance (Definition/Commitment/Compliance)</li> <li>• Very new or very old technology content, Complex business logic</li> <li>• Requires heavy Third party Integration (not readily available during development)</li> <li>• Tools related challenges</li> </ul>
Contractual Risks	<ul style="list-style-type: none"> <li>• Contract not in place/unsigned, SOW and Proposals do not match</li> <li>• Challenging SLAs in place with penalty provisions, Ambiguous Acceptance criteria, No exit clause</li> <li>• Project Manager unaware on critical contract terms/critical clauses</li> </ul>

# Sample Risk Charts(1/2)
















## Sample Risk Charts (2/2)



# ERM - Risk Communication & Tracking

---

Risk Level (Frequency)	Mgmt	Line Head	Delivery Anchor	Project Owner	Finance	Line Quality Champion	Account Manager
High Risk (Weekly)							
Medium Risk (Fortnightly)							
Low Risk (Monthly)							

**High and Medium Risk Projects Status and Business Unit's Stand on Mitigation & Contingency is presented to the Management**



# Risk Mitigation

---

- Latest Risk Index would define the Project risk Level
- High and Medium risk projects are prioritized for risk mitigation
- Low risk projects mitigation to be exercised based on ROI (ERM Tracking continues in either case)

## Treatment Options

- Retain the risk
- Avoid the risk
- Control the risk
- Transfer the risk

Develop a comprehensive risk containment plan identifying the relevant controls / transformation aspects to mitigate the risks

# IT Projects - Credible Risks Indicators

---

<b>Peripheral</b>	<ul style="list-style-type: none"><li>✓ Historical data points (Evaluation of Optimistic assumptions)</li><li>✓ New Customer Engagements</li><li>✓ Geography – Customer as well as implementing team</li><li>✓ Contract Aggressiveness</li><li>✓ Project Execution Type</li><li>✓ Customer Interface state</li></ul>
<b>Technology</b>	<ul style="list-style-type: none"><li>✓ Application Performance – Commitment, Development, Verification</li><li>✓ Requirements – Grasp &amp; Scope (especially state on implicit requirements)</li><li>✓ Architecture &amp; Designs – Competent Designers, Usage of Design Patterns,</li><li>✓ Automation and Tools (Availability and Competency)</li></ul>
<b>Project Management</b>	<ul style="list-style-type: none"><li>✓ Leadership Capability – Project Manager and Onsite Co-ordinator</li><li>✓ Risk Initiative – Buy in, Transparency, Risk Negativity</li><li>✓ Reporting vs. escalations</li><li>✓ Scheduling (square root theory) and Estimation</li></ul>
<b>Process Strength &amp; Culture</b>	<ul style="list-style-type: none"><li>✓ Strong Methodology backbone – Process</li><li>✓ Process Culture – Controlled vs. in control</li><li>✓ Empowerment vs. Helplessness</li></ul>
<b>Quantitative Tracking</b>	<ul style="list-style-type: none"><li>✓ Risk Indexing is a MUST</li><li>✓ Customer Relationship Index – worth attempting</li><li>✓ \$ Value catches more attention than process content</li></ul>

# Contractual Governance

---

- Risk Gradation process for Contracts
  - Exposure terms
  - Insurance coverage
  - Warranty terms etc.
- Customized Contracts Repository - Early Alerts
- Commitment vis-à-vis Execution State tracking

# Enterprise Infrastructure - Sample Risk coverage chart

Natural Disaster	Defective Defense	Human Initiated Risks	Network & Communication	Legal	Misc.
Fire	Water Leakages	Willful Damages / Inappropriate behavior by Employees	Hacking	Violating Privileges	Collapse of Supply Chain
Floods	Building Collapse	Social Engineering	Transmission Errors	IPR Violation	Denial of Service
Epidemics / Pandemic	Terrorists Attacks	Third-party personnel	Network Congestion Sniffing	Inadequate Licenses	Data Corruption
Humidity	Explosion	Unauthorized movement of Resources	Telecom Failures	Non-Compliance to Statutory Requirements	Operational Errors
Extreme Temperatures	Power Failures	Misuse of resources	Virus Attacks	Use of Unauthorized Software	Obsolete Technology
Lightening	Strikes/Riots	Inappropriate accounting / disposal of assets	Malicious Software		Incompatible Software
	Physical intrusion		IP Spoofing		Non-availability of Key Personnel
	Theft				Attrition
	Dust and airborne Particles				
	Rodent / Pest Attacks				

# Customer - Sample Risk coverage chart

Sr. No.	Attribute	Potential Data Source
1	Customer Industry Assessment	Sales
2	Customer Company Overview (with key numbers)	Sales
3	Customer Competitors	Sales, Program Manager
4	PATNI competitors at customer	Sales, Program Manager, Onsite Manager
5	Customer Credit Details	Finance
6	Top 3 initiatives at the customer organization	Sales, Program Manager, Onsite Manager
7	Movers and Shakers of the company	Sales, Program Manager
8	What influential client managers perceive the Vendor Organization	Sales, Program Manager
9	Outsourcing Trend - (To vendors and to our Organization)	Sales, Program Manager
10	Geography Attributes	Sales, Program Manager
11	Financials - (Annual, Quarterly Results)	Sales, Program Manager
12	Contracting – Preference, Highlights	Legal, Sales

# Challenges in Adopting to ERM Approach

---

## Approach

- Integrating risk assessment into line functions - Building risk-averse culture
- Risk profiling - understanding dependencies between risks
- Setting up Risk Management Framework

## Adoptability

- Risk evolution - business / market / customer / technology changes
- Risk analytics - setting checks and balances. Balancing qualitative and quantitative streams
- Aligning framework by the business domain

## Risk Reporting

- Risk Governance - from strategy to projects
- Compliance - meeting the requirements
- Customizing the economic value-added models
- Integrating line function feeds

## Risk Management

- Handling risk events
- Managing data & technology resources
- Integrating three risk dimensions - operational, market and customer
- Deploying portfolio approach to manage risks

# IT Projects - Risk Officer Attributes

---

- Risk Officer should know ...
  - Risk Management Principles
  - Project / IT / Organization Processes
  - Specifics of the Business Unit and Domain
  - Risk Analytics, Relationship between Quantitative and Qualitative Risk Ratings
- Risk Officer should do ...
  - Networking with Business Units and Line Management
  - Communicating the risk effectively and timely to all stakeholders
  - Sharing the intelligence gathered from BU with Risk Management function
  - Identifying the early indicators for project failures
  - Expert in Non-intrusive Assessment Style
- Risk Officer should focus on ...
  - Identifying Risks which are unknown to Project or Operations Team
  - Stakeholder Management
  - Understanding the dependencies between the risk categories

# Key Benefits from Adopting ERM Approach to IT Risks

---

- Broad, Deep and Quantified Risk Assessment

- Being closest to the ground zero, project leadership is most well placed to identify project execution risks. Groups like ERM can add value by covering risk angles like Payment age, geography, risk history, prevalent trends, credit/market risks etc. in addition to project execution risks

- Collaboration

- ERM brings value add in risk assessment through collaboration with Contracts/legal, BU PMOs, Finance, Audits, HR, Account Management etc. which would be difficult for project leadership in wake of project responsibilities

- Visibility and Appreciation on Risks

- It has been observed that early identification of risks with right set of leadership helps mitigation. ERM looks forward to make risks visible to leadership and seek their support in mitigating them

- Share Risk Experience

- There would be risks for which prescriptive risk mitigation may not be available. In such cases, experience and sharing on how others are addressing these risks would be useful to know.



# Value Add to the Organization

---

- Developing/Fine Tuning ERM framework
  - Corporate IT Risk definition
  - Data Analytics on past Risks/losses database
  - Risk Policy
  - Risk Model
  - Risk communication model
  - Risk intelligence collaboration model etc.
- Developing Customized Risk Indexing scheme
- Developing Risk Analytics for “intelligent” risk policies