

Risk Analysis for Oracle R12 Upgrade Projects

Lisa Laine & Alyssa Johnson
Solution Beacon

ORACLE Platinum
Partner



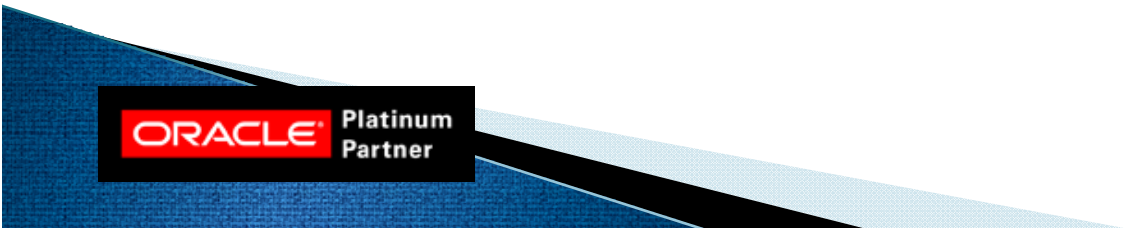
Agenda

- ▶ Introduction to Solution Beacon
- ▶ How to Evaluate Risks
- ▶ R12 Upgrade Risk Example Evaluations
- ▶ Common Upgrade Risks/Mitigation Efforts
- ▶ Risk Prioritization

End-to-End Solutions Provider

Assessments	Implementations
<ul style="list-style-type: none"> • Strategic business assessments & ROI • Functional assessments • Technical assessments • IT roadmap planning • Acquisition integration • Software selection • Upgrade readiness 	<ul style="list-style-type: none"> • ERP upgrades • ERP implementations • ERP migration and consolidation • Oracle Fusion Middleware - SOA • Develop industry specific front-end modules • Custom development • International dependencies and multi-org
Optimizations	Support Services
<ul style="list-style-type: none"> • Business process re-engineering • Functional optimization • Technical optimization • System architecture optimization • Database tuning and optimization 	<ul style="list-style-type: none"> • Functional and technical support • Focused knowledge transfer • Remote DBA support • Oracle instance hosting

Solution Beacon has developed a matrix of upgrade decision points to guide clients toward a well informed R12 decision



Risk Management Definitions

- ▶ What is a risk?
 - The *effect of uncertainty on objectives*, whether positive or negative
- ▶ What is risk management?
 - the identification, assessment, and prioritization of risks
 - followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

Step 1: Identify the Risk

- ▶ A positive or negative effect on the project using a variety of approaches to identify risk
 - Source Analysis*
 - Problem Analysis*
 - Objectives-based risk identification*
 - Common-risk checking*
 - Scenario analysis
 - Risk Charting
- ▶ Evaluating from multiple angles

*Simple methods that pertain to Oracle EBS Projects

Step 2: Assess the Risk

- ▶ Identify the impact
 - Qualitative Scale: High, Med, Low
 - Quantitative Scale: 1 (Low) - 5 (High)
- ▶ Identify the probability
 - Qualitative Scale: High, Med, Low
 - Quantitative Scale: 1 (Low) - 5 (High)
- ▶ Create Risk Index = Impact of Risk Event x Probability of Occurrence

Define Scale

Probability

Impact	High			
	Med			
	Low			
		Low	Med	High

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

Qualitative Approach

Quantitative Approach

Step 3: Risk Management Options

- ▶ Risk Avoidance
 - ▶ Risk Mitigation/Reduction
 - ▶ Risk Sharing (transfer – outsource or insure)
 - ▶ Risk Acceptance
- ▶ Why all the trouble? Not every risk is worth the cost of risk management

Range of Action

Probability

Impact

High			
Med			
Low			
	Low	Med	High



Qualitative Approach

5					
4					
3					
2					
1					
	1	2	3	4	5

Quantitative Approach

Sample Risk Qualitative

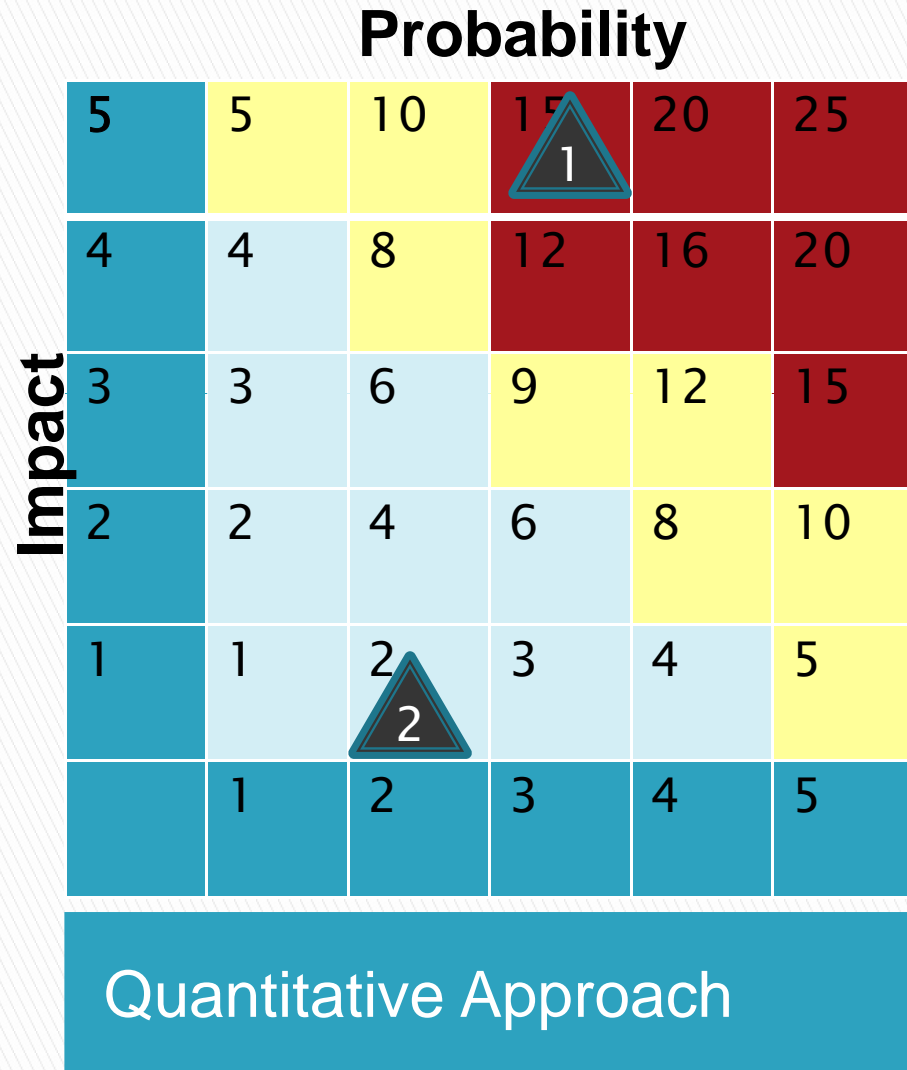
Probability

Impact	High			
	Med			
	Low			
		Low	Med	High
Qualitative Approach				

1. Scope creep threatens go live date and budget
 - Impact: High
 - Probability: Medium
2. Train the trainer approach might not be adequate for the users
 - Impact: Low
 - Probability: Medium

Sample Risk Quantitative

1. Scope creep threatens go live date and budget
 - Impact: 5
 - Probability: 3
 - Risk Index = 15
 2. Train the trainer approach might not be adequate for the users
 - Impact: 1
 - Probability: 2
 - Risk Index = 2
- ▶ Can define quantitative ranges for risk index
- No Action < 5
 - Evaluate >=5 but <12
 - Action required > 15



Common R12 Upgrade Risks Impacting Timeline/Budget

- ▶ Aggressive Timeline
- ▶ Resolution of Business Issues
- ▶ Lack of User Availability
- ▶ Migration of WRICEP elements
- ▶ Critical Software Bug
- ▶ Setups not properly applied to subsequent instances
- ▶ Performance issues with new software
- ▶ Late application of patch(es) impact testing

Common R12 Upgrade Risks Impacting Project Success

- ▶ Training Quality
- ▶ Resistance to change
- ▶ Business Interruption at go-live
- ▶ Downtime Minimization

Risk Management

RISK IDENTIFICATION	RISK MITIGATION
Timeline is aggressive	<ul style="list-style-type: none"> • Technical upgrade iterations have begun • Strictly manage scope creep • Ensure everyone is aware of schedule, everyone has a backup • Work during month end to make up any slippages • Work late, Work weekends • Go/No-Go checkpoints throughout project
Resolution of Issues Requiring Business Decisions	<ul style="list-style-type: none"> • Every decision assigned to Business Process owner • Due date and default decision in place • Due dates well-communicated to issue owner and adhered to • Regular steering committee meetings to ensure open communication and issue resolution

Risk Management

RISK IDENTIFICATION	RISK MITIGATION
Availability of Users	<ul style="list-style-type: none">• Project plan scheduled around month-end close• No new initiatives during upgrade - code freeze• Vacation planning
Migration of WRICEP elements	<ul style="list-style-type: none">• Review has begun• Assign resources to accomplish within time period
Critical software bug	<ul style="list-style-type: none">• Setup configuration management with project plan so Oracle aware of critical dates• Work with Oracle rep so Oracle is aware of plan• Daily pinging of Oracle for escalation

Risk Management

RISK IDENTIFICATION	RISK MITIGATION
Setups not properly applied to subsequent instances	<ul style="list-style-type: none">• Document, document, document• Ensure each change communicated to SB/client counterpart so can make sure included in documentation
Performance issues with new software	<ul style="list-style-type: none">• DBA consultant to assist• SR with Oracle – diagnostics• Ensure PCs meet SB recommendations for memory/screen size• Performance testing tools

Risk Management

RISK IDENTIFICATION	RISK MITIGATION
Late application of patch could require extensive testing	<ul style="list-style-type: none">• Ensure MOS notes for 12.1.3 recommended patches are followed• Test, test, test in CRP1• Code freeze after CRP2• Evaluate whether patch is required for go-live
Training – time to create materials, deliver, experience of trainers	<ul style="list-style-type: none">• Use CRPs and test scripts for training• Hire training consultant for modules with high change – Payables/Payments

Risk Management

RISK IDENTIFICATION	RISK MITIGATION
Resistance to change	<ul style="list-style-type: none">• Involvement of everyone in CRPs increases comfort with new screens and processes• Meetings to surface concerns
Business interruption at go-live	<ul style="list-style-type: none">• Strong go-live preparation• Go/No Checkpoints throughout project• Final sign-off by upper management
Minimize Downtime	<ul style="list-style-type: none">• Multiple iterations• Optimization Script• Evaluate projects to be done in advance (OATM/Upgrade DB to 11g/Etc...)

Other Source of Risks to Consider

- ▶ Complexity (new modules/global/major architecture change)
- ▶ Poor Testing Processes
- ▶ QA Processes
- ▶ Governance Levels set too high/too low
- ▶ Third Party Systems
- ▶ Power outage
- ▶ Unknown risks
- ▶ Inadequate planning

Wrap Up

- ▶ Risk Management is pretty intuitive to most users
- ▶ We've presented a framework for prioritizing/managing risks
- ▶ Not all risks are worth mitigating
- ▶ Experience has taught us by going through the analysis we mitigate the risk of unknown risks