Risk Management@SAP

Michael Collet

28th January 2005,
Frankfurt, GI -Fachgruppe SECMGT
If business has no risk, don’t do it! (frei nach Tom DeMarco & Timothy Lister)
Establish Best-Practice orientated uniform Risk Management methodologies, processes and tools for all of SAP’s LoB’s; Responsibility for SAP’s ongoing external and internal risk reporting

Roll-out of effective Internal Controls documentation and assessment processes mandated by Sarbanes-Oxley Act as a core process risk response strategy

Ongoing Shaping of corporate wide risk aligned insurance programs as a core risk response strategy

Scope of Corporate Risk Management

Risk Management Framework

Documentation & Assessment of Internal Controls

Insurance Strategy

© SAP GRM project 2003
The implementation of SAP’s Corporate Risk Management Model (scope, covered activities, LoB-specific adaptations, responsibilities) has been agreed with SAP’s Lines of Business.
SAP’s Operational Risk Management (ORM) Application

- Structure Setup
- Execution
- Analysis
- Process Support

- Views and Worksets for Risk Owners, Risk Validators, Accountable Executives, Project Managers, Administrators
- Organization, Process, Project and Object Structures, Risk Assessments, Risk Responses, Business Intelligence, Info Cubes, Reports
- Process-to-Process Integration, Offline Transactions, Notifications and Workflow

SAP Web Application Server

- HR (Organization)
- SOA-MIC (Processes)
- PS, CRM, cProjects (Projects)
- BW (Reporting)
- CO (aggregation financial comparison data)
- xls upload Interface (Projects)

© SAP GRM project 2003
The 5 key process steps...
The 5 key process steps...

- Risk Planning: Process Integration
- Risk Identification: Brain-storming
- Risk Analysis: Assessment (meeting)
- Risk Response: to ORM / Validation (approval)
- Risk Monitoring: Reporting / Re-Assessments
Risk Planning

For on-going business operations:

- Usually occurs as part of annual planning
- Involves deciding how business risks are identified, assessed and monitored

For projects:

- Involves deciding how risk management will fit into the project plan

Determining how to approach risk management in your business area or project
Risk Identification

Uncovering risks to your business or project before they turn into problems

Risk Planning → Risk Identification → Risk Analysis → Risk Response → Risk Monitoring

Iterative process. For example:
- At the start of the annual budgeting process
- During the Evaluation phase of the Customer Engagement Lifecycle
- During the Planning phase of a standard or customer-specific development project
- At the end of the Business Blueprint phase of an implementation project

No standard approach to identifying risk. However, some common approaches include questionnaires, interviews, workshops, surveys
Risk Identification

Risk Statement

<table>
<thead>
<tr>
<th>Condition Causing Concern</th>
<th>Potential Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no customer team to support productive system</td>
<td>Go live will be delayed</td>
</tr>
<tr>
<td>The customer is unable to replace the consultants for system support</td>
<td>Customer will be unable to perform system management causing system degradation</td>
</tr>
<tr>
<td>Too much time is needed for SAP to make clear decisions</td>
<td>Confusion and delays</td>
</tr>
</tbody>
</table>
## Risk Brainstorming Template

**Assessment Title:** Facility & Physical Security Assessment
**Assessment Moderator:** John Smith
**Latest date to send results back:** 20th July 2004
**Brainstormer’s Name:** Hans Meier

### Brainstorm Results

<table>
<thead>
<tr>
<th>Risk #</th>
<th>Risk Title</th>
<th>Cause of Risk</th>
<th>Negative Consequence for SAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External Attack</td>
<td>Attack on embassy located in same building as SAP</td>
<td>Disruption of SAP operations</td>
</tr>
<tr>
<td>2</td>
<td>Protected Areas</td>
<td>Areas in the building exist requiring special protection e.g. Utilities in the Basement can be better protected.</td>
<td>Since these are areas where critical functions are being performed, a disruption here would cause disruption of business.</td>
</tr>
<tr>
<td>3</td>
<td>Existence of Contingency Plans</td>
<td>Contingency plans not in place for all critical business processes and supporting infrastructure for Facilities.</td>
<td>No fail back measure in the event of disaster and business could get affected.</td>
</tr>
<tr>
<td>4</td>
<td>Availability of critical resources</td>
<td>Danger of critical services, infrastructure and information being unavailable when needed. In the absence of an alternative site to transfer essential services.</td>
<td>In the event of a disaster like 'Sabotage' / 'Fire' in critical areas, this could lead to a long term disruption to business operations.</td>
</tr>
<tr>
<td>5</td>
<td>Misuse of Passwords</td>
<td>There are known incidents regarding the misuse of (user-) passwords.</td>
<td>Possibility of future intentional or unintentional hacking into key systems, could lead to a disruption of business operations.</td>
</tr>
</tbody>
</table>
Risk Identification

Common Risk Catalog:

- Corporate-wide catalog of generic risk categories

- Economic
- Communication and Information
- Market
- Financial
- Strategic Focus
- Product
- Human Capital
- Project
- Organization and Governance
- Other Operational Risks
## Risk Identification

### Economic Risks
- Global Economy: 50000075
- Regional Economy: 50000076
- Legal and Regulatory Environment: 50000077
- Natural Catastrophes: 50000078
- External Attacks: 50000079

### Market Risks
- Competition: 50000080
- Industry Sector: 50000081
- Market Development: 50000082

### Strategic Focus
- Strategic Objective Planning and Setting: 50000103
- Competitive Positioning: 50000104
- Partner Management: 50000105
- Research and Innovation: 50000106
- Customer Focus: 50000107
- Brand and Reputation: 50000108

### Financial Risks
- Financial Reporting
  - Accounting Guidelines: 50000139
  - Financial Market Regulations: 50000140
  - Financial Misstatements: 50000141
- Internal Compliance: 50000142
- Treasury
  - Currency: 50000143
  - Liquidity: 50000144

### Organization and Governance
- Corporate Governance: 50000116
- Corporate Culture and Leadership: 50000117
- Organizational Structure
  - Organizational Structure: 50000119
  - Processes: 50000120
  - Process Execution: 50000122
  - Internal Controls System: 50000124
- Signature Rules: 50000191
- Partner Engagement
  - Quality of the Partner: 50000130
  - Agenda of the Partner: 50000131
  - Segregation of Responsibilities: 50000132
  - Partner Relationship: 50000133

### Project Risks
- Close Out: 50000206
- Project Management
  - Project Sponsorship: 50000209
  - Project Leadership and Qualification: 50000210
  - Project Team: 50000211
- Planning and Risk Identification: 50000213
- Escalation Management: 50000220
- Project Change Management: 50000221
- Initiation and Planning
  - Budgeting and Profitability: 50000233
  - Scope and Deliverables
  - Solution: 50000227
  - Technology: 50000228

### Communication and Information
- Investor Relations: 50000139
- Corporate Communications: 50000110
- Competitive Intelligence: 50000111
- Information Strategy: 50000112
- Knowledge Transfer Strategy: 50000113
- Information Transfer Execution: 50000114
- Idea Management: 50000115

### Other Operational Risks
- Intellectual Property Rights: 50000166
- Procurement
  - Vendor Selection: 50000167
  - Vendor Monitoring: 50000168
  - Vendor Dependency: 50000169
- Policy: 50000170
- Infrastructure Operators
  - Security Governance: 50000171
  - Facilities and Physical Security
  - Planning and Construction: 50000173
  - Loss of Infrastructure: 50000174
  - Unauthorized Access: 50000175
  - Impairment of Personnel: 50000176
  - Facilities and Physical Security: 5021172
  - Information and IT
    - Confidentiality: 50000177
    - Availability: 50000178
    - Technology: 50000180
    - Integrity: 5021170
# Risk Identification - Assessment Template

## General Risk Information

<table>
<thead>
<tr>
<th>#</th>
<th>Identification Date</th>
<th>Location</th>
<th>Common Risk Title</th>
<th>Title</th>
<th>Condition</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17.11.2004</td>
<td>ECONOMIC RISKS: External Attacks</td>
<td>External Attack</td>
<td>Attack on embassy located in same building as SAP</td>
<td>Disruption of SAP operations</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>17.11.2004</td>
<td>OTHER OPERATIONAL RISKS: Facilities and Physical Security</td>
<td>Protected Areas</td>
<td>Areas in the building exist requiring special protection e.g. Utilities in the Basement can be better protected.</td>
<td>Since these are areas where critical functions are being performed, a disruptor here would cause disruption of business</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>17.11.2004</td>
<td>ORGANIZATION AND GOVERNANCE: Processes</td>
<td>Existence of Contingency Plans</td>
<td>Contingency plans not in place for all critical business processes and supporting infrastructure for facilities.</td>
<td>No fail back measure in the event of disaster and business could get affected.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>17.11.2004</td>
<td>OTHER OPERATIONAL RISKS: Loss of Infrastructure</td>
<td>Availability of critical resources</td>
<td>Danger of critical services, infrastructure and information being unavailable when needed - in the absence of an alternative site to transfer essential services.</td>
<td>In the event of a disaster like &quot;sabotage&quot; / &quot;fire&quot; in critical areas, this could lead to a long term disruption to business operations.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>17.11.2004</td>
<td>OTHER OPERATIONAL RISKS: Integrity</td>
<td>Misuse of Passwords</td>
<td>There are known incidents regarding the misuse of (user-) passwords.</td>
<td>Possibility of future intentional or unintentional hacking into key systems, could lead to a disruption of</td>
<td></td>
</tr>
</tbody>
</table>

© SAP GRM project 2003

THE BEST-RUN BUSINESSES RUN SAP
Risk attributes ► Probability; Impact; Timeframe

Risk prioritization involves separating out which risks should be dealt with first when allocating resources.

Risk Planning ► Risk Identification ► Risk Analysis ► Risk Response ► Risk Monitoring

Evaluating the risk attributes, and prioritizing (ranking) the risks
## Risk Analysis

### Probability:

Five-level scoring scale to be used by all lines of business:

<table>
<thead>
<tr>
<th>Probability</th>
<th>Percentage</th>
<th>Assessment Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>81 – 99%</td>
<td>90%</td>
<td>once a year</td>
</tr>
<tr>
<td>61 – 80%</td>
<td>67%</td>
<td>once every 1½ years</td>
</tr>
<tr>
<td>41 – 60%</td>
<td>50%</td>
<td>once every 2 years</td>
</tr>
<tr>
<td>21 – 40%</td>
<td>33%</td>
<td>once every 3 years</td>
</tr>
<tr>
<td></td>
<td>25%</td>
<td>once every 4 years</td>
</tr>
<tr>
<td>1 – 20%</td>
<td>17%</td>
<td>once every 6 years</td>
</tr>
<tr>
<td></td>
<td>10%</td>
<td>once every 10 years</td>
</tr>
<tr>
<td></td>
<td>5%</td>
<td>once every 20 years</td>
</tr>
<tr>
<td></td>
<td>2%</td>
<td>once every 50 years</td>
</tr>
<tr>
<td></td>
<td>1%</td>
<td>once every 100 years</td>
</tr>
</tbody>
</table>

Based on a one-year assessment horizon!
Risk Analysis

Impact (Local/Global):

Five-level scoring scale to be used by all lines of business:

<table>
<thead>
<tr>
<th>Qualitative Impact</th>
<th>Total Loss (Quantitative)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = Insignificant</td>
<td>Up to €200,000</td>
</tr>
<tr>
<td>2 = Minor</td>
<td>€200,000 to €1,000,000</td>
</tr>
<tr>
<td>3 = Moderate</td>
<td>€1,000,000 to €5,000,000</td>
</tr>
<tr>
<td>4 = Major</td>
<td>€5,000,000 to €25,000,000</td>
</tr>
<tr>
<td>5 = Catastrophic</td>
<td>Greater than €25,000,000</td>
</tr>
</tbody>
</table>

Local Impact:
All costs to re-install normal operation after a risk occurred like:
- HW costs,
- Customizing costs,
- ...

Global Impact:
All costs that result out of the risk occurrence like:
- unavailable of services to customers & employees,
- loss of image,
- costs to re-install normal operation (local impact),
- ...

organizations are free to use local impact according their own definition.
Risk Analysis

Risk Level:

Derived from the probability and impact attributes as follows:

**Example:** Probability = 60%; Impact = €1,000,000 (Level 4)
Risk Analysis

Risk Prioritization:

- Involves separating out which risks should be dealt with first when allocating resources
- Approach: Map the risk level against the time frame for the risk (e.g. how soon action is required to prevent the risk from occurring)
- The following table shows how risk severity incorporates the time frame for action to arrive at a prioritized list of risks

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Priority</th>
<th>Risk Level &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low 2</td>
<td>Med 4</td>
</tr>
<tr>
<td>Short (0 – 1 month)</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Medium (1 – 6 months)</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>Long (&gt; 6 months)</td>
<td>9</td>
<td>8</td>
</tr>
</tbody>
</table>

Top priority risks
Financial Exposure ("Expected Loss"): Probability x Impact

Example:
Highly likely that integration testing will continue for 6 weeks.

Expected loss = \[70\% \times \text{cost of 6 weeks of testing} = €7,000\]

\[(€ 10,000)\]
# Risk Analysis – Assessment Template

<table>
<thead>
<tr>
<th>ID</th>
<th>Common Risk Title</th>
<th>Title</th>
<th>Condition</th>
<th>Consequence</th>
<th>Total Loss</th>
<th>P</th>
<th>Time Frame</th>
<th>Global Impact Before Response</th>
<th>Local Impact Before Response</th>
<th>Expected Loss</th>
<th>Risk Level</th>
<th>Risk Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECONOMIC RISKS: External Attacks</td>
<td>External Attack</td>
<td>Attack on embassy located in same building as SAP</td>
<td>Disruption of SAP operations</td>
<td>6,300,000</td>
<td>2%</td>
<td>2</td>
<td>6</td>
<td>120,000</td>
<td>Med</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>OTHER OPERATIONAL RISKS: Facilities and Physical Security</td>
<td>Protected Area</td>
<td>Areas in the building exist requiring special protection e.g. Utilities in the basement can be better protected</td>
<td>Since these are areas where critical functions are being performed, a disruption here would cause disruption of business</td>
<td>3,300,000</td>
<td>2%</td>
<td>2</td>
<td>4</td>
<td>508,000</td>
<td>Med</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ORGANIZATION AND GOVERNANCE Processes</td>
<td>Existence of Contingency Plans</td>
<td>Contingency plans not in place for all critical business processes and supporting infrastructure for Facilities</td>
<td>No fall back measure in the event of disaster and business could get affected</td>
<td>3,300,000</td>
<td>2%</td>
<td>2</td>
<td>5</td>
<td>300,000</td>
<td>Med</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>OTHER OPERATIONAL RISKS: Loss of Infrastructure</td>
<td>Availability of critical resources</td>
<td>Danger of critical services, infrastructure and information being unavailable when needed - in the absence of an alternative site to transfer essential services</td>
<td>In the event of disaster like ‘sabotage’ or ‘fire’ in critical areas, this could lead to a long term disruption to business operations</td>
<td>6,300,000</td>
<td>2%</td>
<td>1</td>
<td>5</td>
<td>120,000</td>
<td>Med</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>OTHER OPERATIONAL RISKS: Integrity</td>
<td>Misuse of Passwords</td>
<td>There are known incidents regarding the misuse of (user) passwords</td>
<td>Possibility of future intentional or unintentional hacking into key systems; could lead to a disruption of business operations</td>
<td>7,500,000</td>
<td>90%</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>High</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Risk Response answers two key questions:

- Who owns the risk (responsibility), and
- What can/should be done (scope and actions)

Standard response actions: Delegate; Research; Transfer; Accept; Mitigate; Watch
## Risk Response – Assessment Template

### General Risk Information

<table>
<thead>
<tr>
<th>ID</th>
<th>Common Risk</th>
<th>Title</th>
<th>Condition</th>
<th>Consequence</th>
<th>Response Type</th>
<th>Response</th>
<th>Response Owner</th>
<th>Response Cost</th>
<th>Prob. Reduced By After Resp.</th>
<th>Total Loss Reduced By After Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECONOMIC RISKS: External Attacks</td>
<td>External Attack</td>
<td>Attack on embassy located in same building as SAP</td>
<td>Disruption of SAP operations</td>
<td>Transfer</td>
<td>Ensure sufficient insurance coverage</td>
<td>d033961</td>
<td>16,000.00</td>
<td>1,000,000.00</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>OTHER OPERATIONAL RISKS: Facilities and Physical Security</td>
<td>Protected Areas</td>
<td>Areas in the building must requiring special protection e.g. Utilities in the Basement can be better protected.</td>
<td>Since these are areas where critical functions are being performed, a disruption here would cause disruption of business</td>
<td>Mitigate</td>
<td>Implement security measurements (avoid public access to areas where critical functions are performed)</td>
<td>d033961</td>
<td>16,000.00</td>
<td>15%</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ORGANIZATION AND GOVERNANCE: Processes</td>
<td>Existence of Contingency Plans</td>
<td>Contingency plans not in place for all critical business processes and supporting infrastructure for Facilities.</td>
<td>No failback measure in the event of disaster and business could get affected.</td>
<td>Mitigate</td>
<td>Setup Business Contingency Plans (BCP) for all relevant processes Contact Corporate Security for support (Christine Treurer-Walde)</td>
<td>d033961</td>
<td>50,000.00</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>OTHER OPERATIONAL RISKS: Loss of Infrastructure</td>
<td>Availability of critical resources</td>
<td>Danger of critical services, infrastructure and information being unavailable when needed - in the absence of an alternative site to transfer essential services.</td>
<td>In the event of a disaster like 'Sabotage' / 'fire' in critical areas, this could lead to a long term disruption to business operations</td>
<td>Accept</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>OTHER OPERATIONAL RISKS: Integrity</td>
<td>Misuse of Passwords</td>
<td>There are recent incidents regarding the misuse of (user-) passwords.</td>
<td>Possibility of future intentional or unintentional hacking into key systems, could lead to a disruption of business operations</td>
<td>Mitigate</td>
<td>Enforcement in case of misuse Ensure secure passwords (check regularly)</td>
<td>d033961</td>
<td></td>
<td>50%</td>
<td></td>
</tr>
</tbody>
</table>
### Upload Risks to ORM

**GLOBAL RISK MANAGEMENT@SAP**

**Activity/Risk Maintenance**

**Object: Corporate Security**

<table>
<thead>
<tr>
<th>Title</th>
<th>D</th>
<th>Risk Level</th>
<th>Risk Priority</th>
<th>Probability</th>
<th>Expected Loss</th>
<th>Total Loss</th>
<th>Global Impact</th>
<th>Local Impact</th>
<th>Status</th>
<th>Analysis</th>
<th>Currency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mouse of Passwords</td>
<td>136</td>
<td>Low</td>
<td>5</td>
<td>40</td>
<td>430,000,000</td>
<td>17,000,000,000</td>
<td>Moderate</td>
<td>Major</td>
<td>Draft</td>
<td>16.11.2004</td>
<td>EUR</td>
</tr>
<tr>
<td>External Attack</td>
<td>132</td>
<td>Low</td>
<td>7</td>
<td>2</td>
<td>100,000,000</td>
<td>5,000,000,000</td>
<td>Catastrophic</td>
<td>Draft</td>
<td>16.11.2004</td>
<td>EUR</td>
<td></td>
</tr>
<tr>
<td>Existence of Contingency Plans</td>
<td>134</td>
<td>Low</td>
<td>7</td>
<td>2</td>
<td>60,000,000</td>
<td>3,000,000,000</td>
<td>Catastrophic</td>
<td>Draft</td>
<td>16.11.2004</td>
<td>EUR</td>
<td></td>
</tr>
<tr>
<td>Protected Areas</td>
<td>133</td>
<td>Low</td>
<td>7</td>
<td>5</td>
<td>150,000,000</td>
<td>3,000,000,000</td>
<td>Major</td>
<td>Draft</td>
<td>16.11.2004</td>
<td>EUR</td>
<td></td>
</tr>
<tr>
<td>Availability of critical resources</td>
<td>135</td>
<td>Low</td>
<td>9</td>
<td>2</td>
<td>120,000,000</td>
<td>5,000,000,000</td>
<td>Catastrophic</td>
<td>Draft</td>
<td>16.11.2004</td>
<td>EUR</td>
<td></td>
</tr>
</tbody>
</table>

**Approval Data**

- **Approval Status**: To be validated
- **Assessment Frequency**: 3 Month
“Risk Validation” is the process of reviewing and approving the identified risks, the analysis, and the risk response plans.

Validation transactions take place in ORM.

Responsibility for validation cannot be delegated.

Risk Validator can:

- Approve the assessment
- Reject individual risks (use activity comment field to provide reasons; note that rejected risks can’t be re-activated)
- Set the sensitivity level of a risk (where “sensitivity” means attorney confidential)
<table>
<thead>
<tr>
<th>Administrative Data</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>16.11.2004</td>
<td></td>
<td>Changing user/Creating user</td>
<td>D033861</td>
</tr>
<tr>
<td>Activity ID</td>
<td>65</td>
<td></td>
<td>Identification Date</td>
<td>16.11.2004</td>
</tr>
<tr>
<td>Common Activity</td>
<td>50211458</td>
<td>FacSecIT</td>
<td>Activity type</td>
<td>Object</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General Data</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Facility / Security / IT (Location XX)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment owner</td>
<td>D033861</td>
<td>Michael Collet</td>
<td>Organization Unit</td>
<td>300000000 CorpSecurity</td>
</tr>
<tr>
<td>Validator</td>
<td>D033861</td>
<td>Michael Collet</td>
<td>New Org Unit</td>
<td></td>
</tr>
<tr>
<td>Accountable Manager</td>
<td></td>
<td></td>
<td>Currency</td>
<td>EUR</td>
</tr>
<tr>
<td>Responsible</td>
<td></td>
<td></td>
<td>Opportunity Value</td>
<td>0.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approval Data</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Status</td>
<td>Validated</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment frequency</td>
<td>3 Month</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approval Comment</td>
<td>Please keep me updated by a bi-monthly reporting about the response implementation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Monitoring

Assessing the effectiveness of the response actions
Ongoing activity aimed at ensuring that response plans are working
Activities include collecting information and reporting results

Risk Planning  Risk Identification  Risk Analysis  Risk Response  Risk Monitoring

Keeping track of the risks and evaluating the effectiveness of the response actions
Risk Monitoring – Re-Assessments

Risk Manager / Assessment Owner:

► keep track of existing risks
► Set Assessment Cycle to a reasonable timeframe (e.g. 3 months)
► Require updates from Risk / Response Owners via ORM workflow
► enter new upcoming risks to ORM
Objective:

Provide clear, useful and actionable information about SAP’s risk profile and risk management performance

Target audience:

► Supervisory Board
► Executive Board
► Product Technology Board (PTB)
► Field Management Board (FMB)
Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Die von SAP AG oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten.

Microsoft®, WINDOWS®, NT®, EXCEL®, Word®, PowerPoint® und SQL Server® sind eingetragene Marken der Microsoft Corporation.

IBM®, DB2®, DB2 Universal Database, OS/2®, Parallel Sysplex®, MVS/ESA, AIX®, S/390®, AS/400®, OS/390®, OS/400®, iSeries, pSeries, xSeries, zSeries, z/Os, AFP, Intelligent Miner, WebSphere®, Netfinity®, Tivoli®, Informix und Informix® Dynamic ServerTM sind Marken der IBM Corporation in den USA und/oder anderen Ländern.

ORACLE® ist eine eingetragene Marke der ORACLE Corporation.

UNIX®, X/Open®, OSF/1® und Motif® sind eingetragene Marken der Open Group.

Citrix®, das Citrix-Logo, ICA®, Program Neighborhood®, MetaFrame®, WinFrame®, VideoFrame®, MultiWin® und andere hier erwähnte Namen von Citrix-Produkten sind Marken von Citrix Systems, Inc.


JAVA® ist eine eingetragene Marke der Sun Microsystems, Inc.

JAVASCRIPT® ist eine eingetragene Marke der Sun Microsystems, Inc., verwendet unter der Lizenz der von Netscape entwickelten und implementierten Technologie.

MarketSet und Enterprise Buyer sind gemeinsame Marken von SAP AG und Commerce One.

SAP, SAP Logo, R/2, R/3, mySAP, mySAP.com und weitere im Text erwähnte SAP-Produkte und -Dienst-leistungen sowie die entsprechenden Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen.