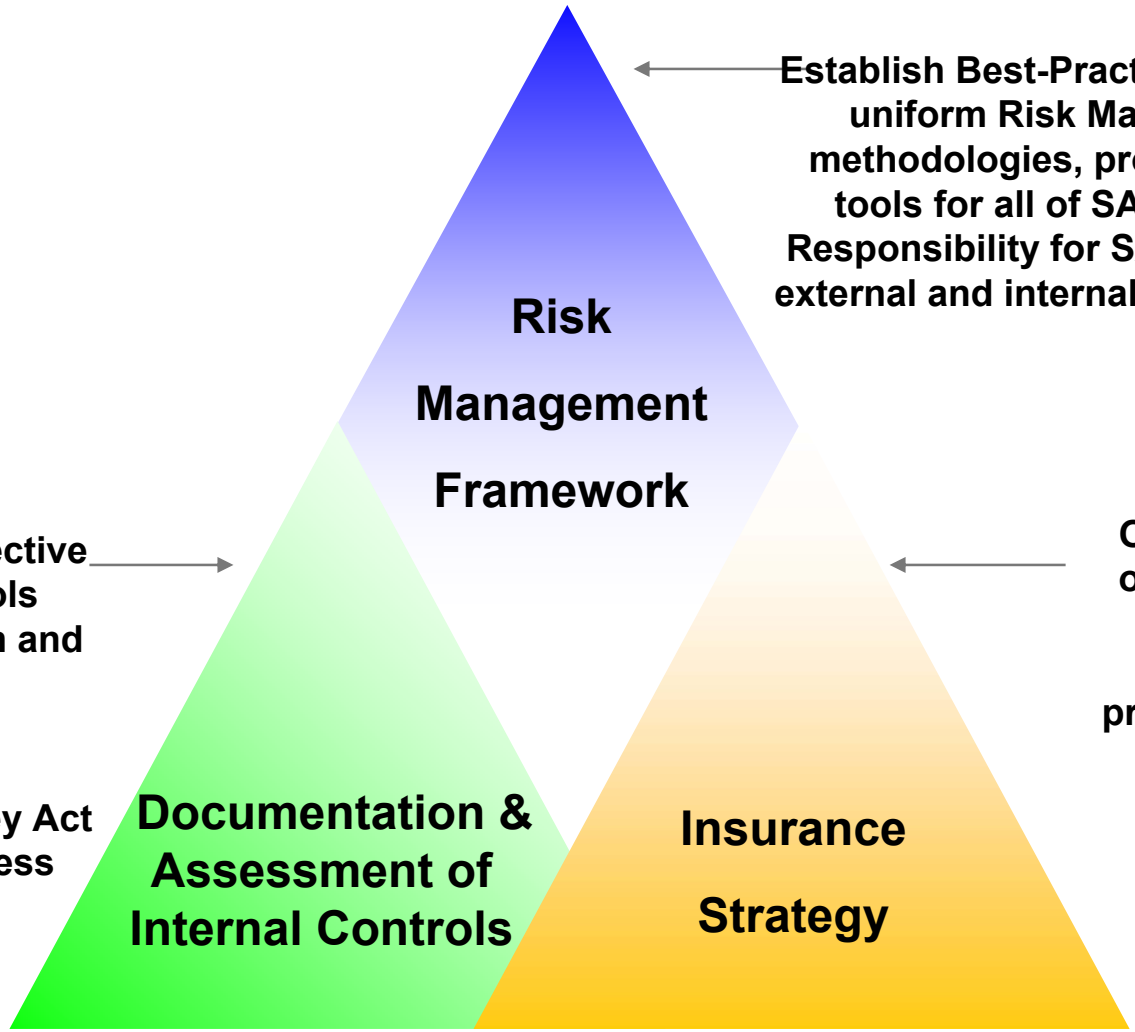
Risk Management@SAP

Michael Collet

28th January 2005,
Frankfurt, GI -Fachgruppe SECMGT

If business has no risk, don't do it! (frei nach Tom DeMarco & Timothy Lister)

Scope of Corporate Risk Management



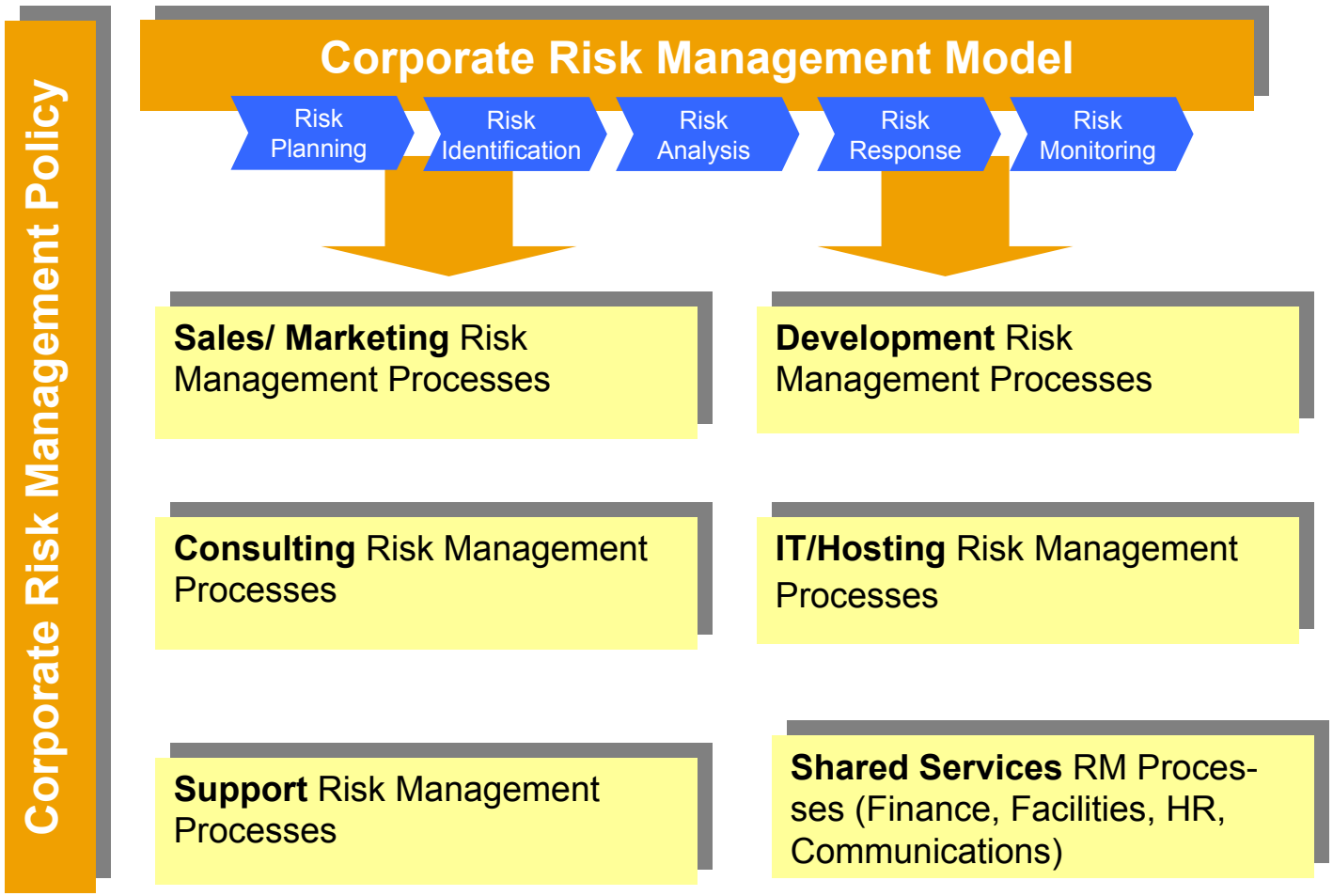
Establish Best-Practice orientated uniform Risk Management methodologies, processes and tools for all of SAP´s LoB´s; Responsibility for SAP´s ongoing external and internal risk reporting

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

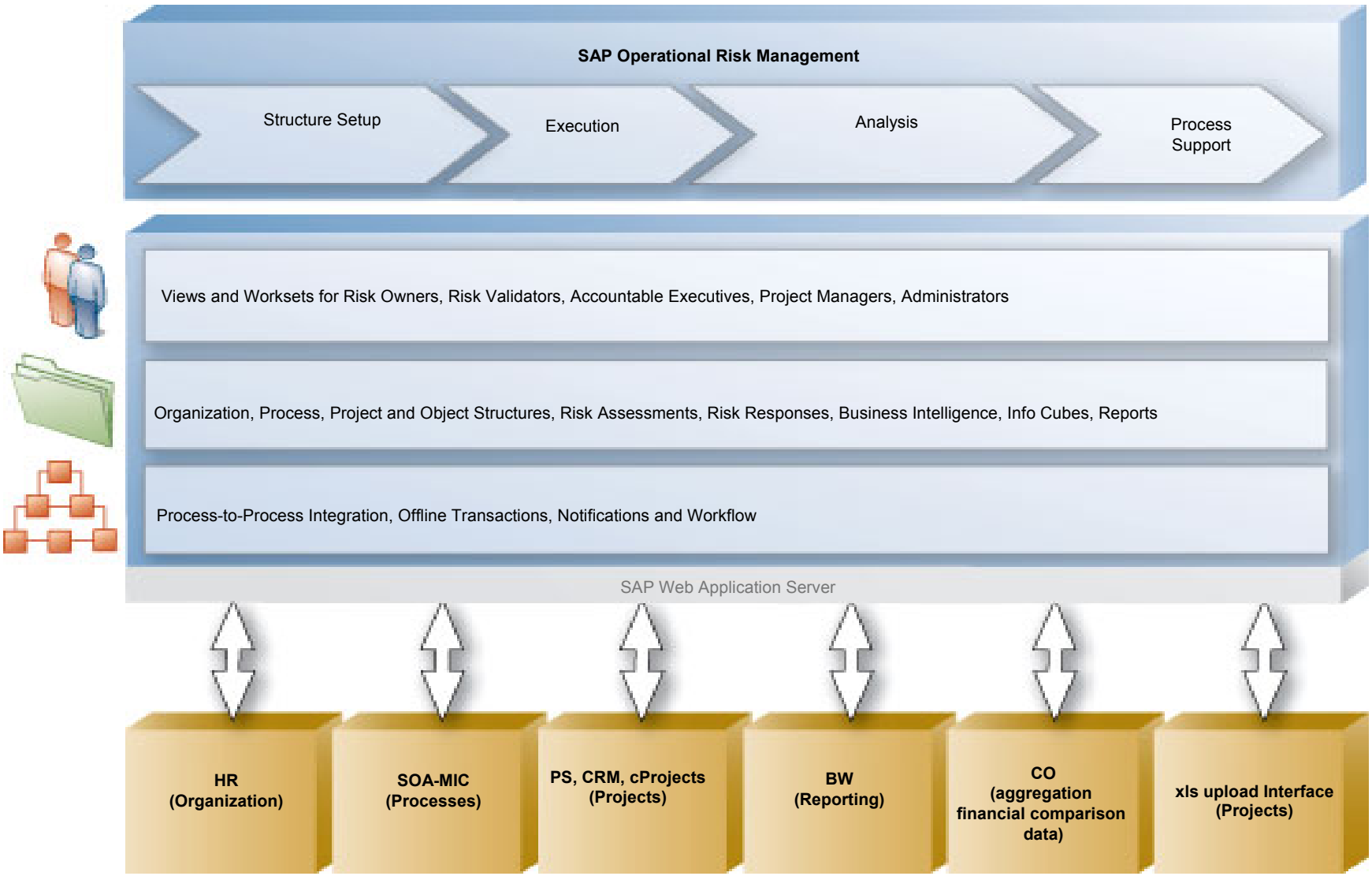
Ongoing Shaping of corporate wide risk aligned insurance programs as a core risk response strategy

Corporate Risk Management Model: Breakdown on Line of Business Level

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



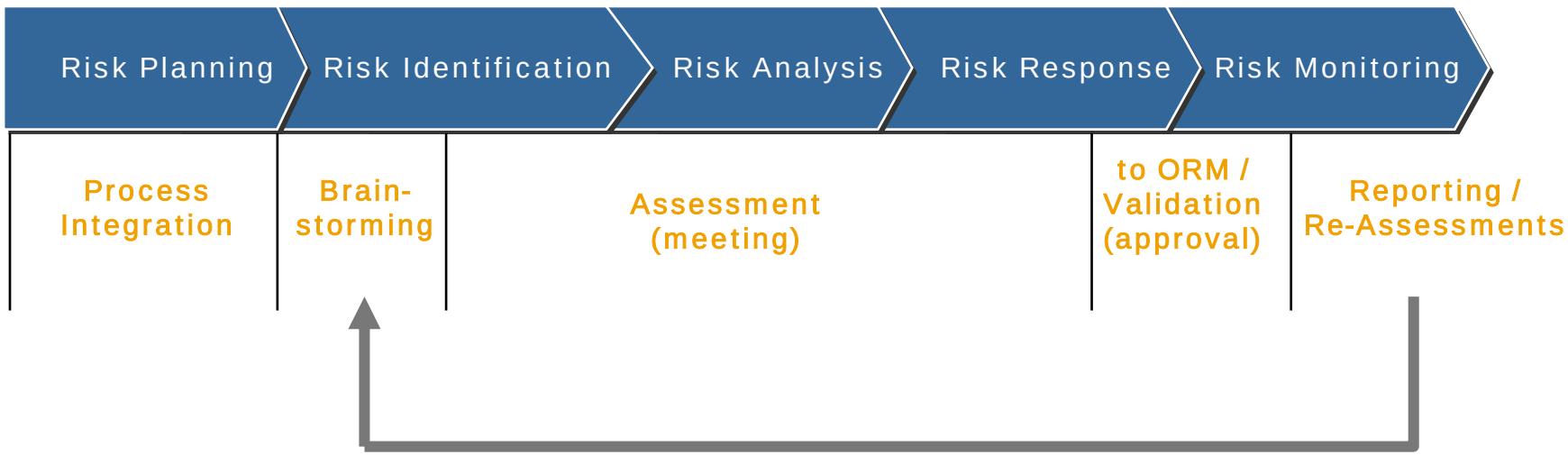
SAP´s Operational Risk Management (ORM) Application



The 5 key process steps…

The Model

The 5 key process steps…



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**

Risk Identification

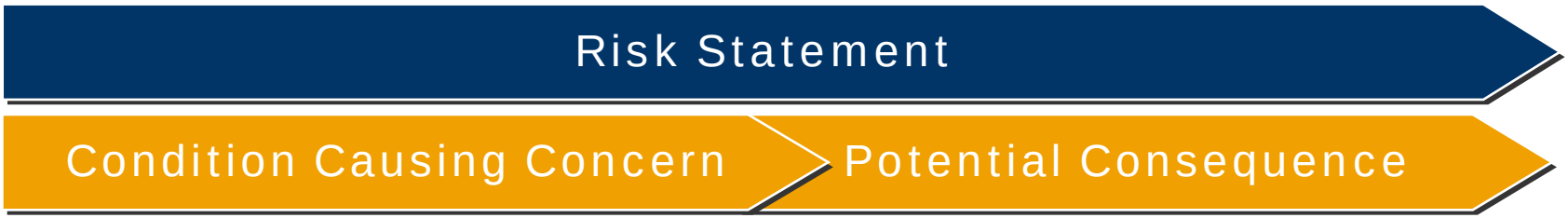
Uncovering risks to your business or project before they turn into problems

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



Condition Causing Concern	Potential Consequence
There is no customer team to support productive system	**Go live will be delayed**
The customer is unable to replace the consultants for system support	**Customer will be unable to perform system management causing system degradation**
Too much time is needed for SAP to make clear decisions	**Confusion and delays**

Risk Identification – Brainstorm Template

GLOBAL RISK MANAGEMENT@SAP

ALIAS: /GRM

Risk Brainstorming Template

Version 1.0

- The Risk Brainstorming is used to prepare a risk assessment.
- Please fill in the 5 most important risks you are aware of. Use English as documentation langauage.
- You can find an example in the "Example" worksheet. In case you want to learn more about the Global Risk Management Model & Policy, use SAPNet Quick Link: /GRM

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

Brainstorm Results

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

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

GLOBAL RISK MANAGEMENT@SAP

ALIAS: /GRM

PROJECT RISK REGISTER

Internal Use Only

> Find the Common Risk that best fits the actual risk, and enter the corresponsing ID number in the Risk Register worksheet.

Common Risk	ID
*This column has **Ecomonmic**, **Market**, **Strategic Focus**, **Financial**, and **Human Capital** Risks...*	
Economic Risks	
Global Economy	50000075
Regional Economy	50000076
Legal and Regulatory Environment	50000077
Natural Catastrophies	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

Common Risk	ID
*This column has **Organization and Governance, Project,** and **Product** Risks...*	
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	50000208
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

Common Risk	ID
*This column has **Communication**, **Other Operational** Risks...*	
Communication and Information	
Investor Relations	50000109
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 Operations	
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	50211172
Information and IT	
Confidentiality	50000177
Availability	50000178
Technology	50000180
Integrity	50211170

Risk Identification – Assessment Template

SAP

GLOBAL RISK MANAGEMENT@SAP

PROJECT RISK REGISTER

Internal Use Only

ALIAS: /GRM

Select the Columns to Display

(•) General ( ) Analysis ( ) Response 1 ( ) Response 2 ( ) All ( ) ORM Selection

> Do not insert rows or columns.

> Mandatory fields shaded if required data is missing and "To ORM?" = "Y".

[x] Display headers

Clear Register | Save ORM Data | Press after successful ORM upload > | Upload Successful

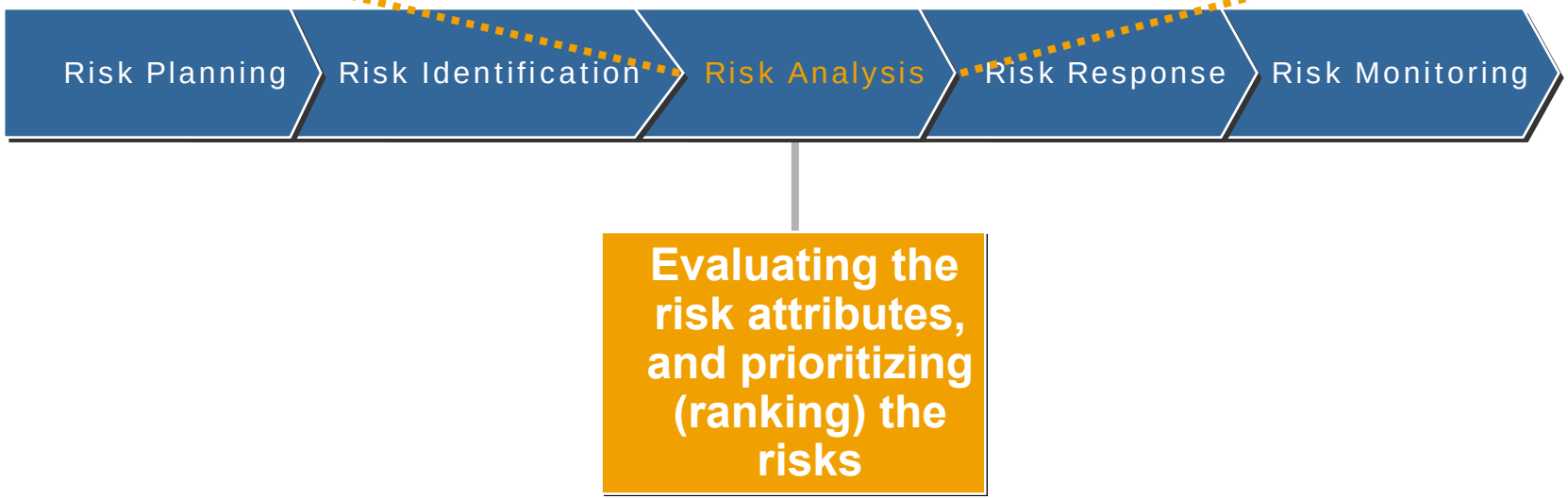
General Risk Information

ID	Identification Date	Common Risk ID	Common Risk Title	Title	Condition	Consequence
1	17.11.2004	50000079	ECONOMIC RISKS: External Attacks	External Attack	Attack on embassy located in same building as SAP	Disruption of SAP operations
2	17.11.2004	50211172	OTHER OPERATIONAL RISKS: Facilities and Physical Security	Protected Areas	Areas in the building exist requiring special protection e.g. Utilities in the Basement can be better protected.	Since these are areas where critical functions are being performed, a disruption here would cause disruption of business
3	17.11.2004	50000120	ORGANIZATION AND GOVERNANCE: Processes	Existence of Contingency Plans	Contingency plans not in place for all critical business processes and supporting infrastructure for Facilities.	No fall back measure in the event of disaster and business could get affected.
4	17.11.2004	50000174	OTHER OPERATIONAL RISKS: Loss of Infrastructure	Availability of critical resources	Danger of critical services, infrastructure and information being unavailable when needed - in the absense of an alternative site to transfer essential services.	In the event of a disaster like 'sabotage' / 'fire' in critical areas, this could lead to a long term disruption to business operations.
5	17.11.2004	50211170	OTHER OPERATIONAL RISKS: Integrity	Misuse of Passwords	There are known incidents regarding the misuse of (user-) passwords.	Possibility of future intentional or unintentional hacking into key systems, could lead to a disruption of

Risk Analysis

Risk attributes ► Probability; Impact; Timeframe

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



Risk Analysis

Probability:

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

81 – 99%		
90%	→	once a year
61 – 80%		
67%	→	once every 1½ years
41 – 60%		
50%	→	once every 2 years
21 – 40%		
33%	→	once every 3 years
25%	→	once every 4 years
1 – 20%		
17%	→	once every 6 years
10%	→	once every 10 years
5%	→	once every 20 years
2%	→	once every 50 years
1%	→	once every 100 years

Based on a one-year assessment horizon !

Risk Analysis

Impact (Local/Global):

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

Qualitative Impact		Total Loss (Quantitative)
1 = Insignificant	→	Up to €200,000
2 = Minor	→	€200,000 to €1,000,000
3 = Moderate	→	€1,000,000 to €5,000,000
4 = Major	→	€ 5,000,000 to €25,000,000
5 = Catastrophic	→	Greater than €25,000,000

Local Impact

All costs to re-install normal operation after a risk occurred like.:

- HW costs,
- Customizing costs,
- …

organizations are free to use local Impact according their own definition

Global Impact

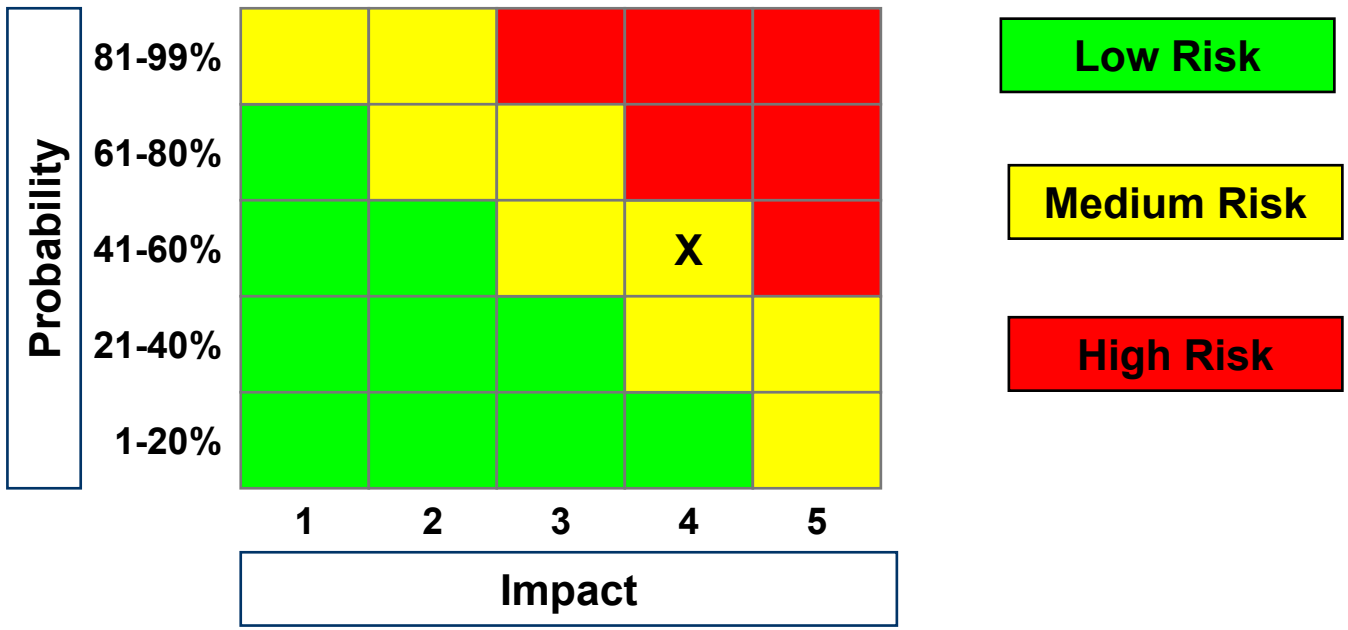
All costs that result out of the risk occurrence like:

- unavailable of services to customers & employees,
- loss of image,
- costs to re-install normal operation (local impact),
- …

Risk Level:

Derived from the probability and impact attributes as follows:

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



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

		Priority		
	Risk Level >	**Low**	**Med**	**High**
Time Frame	Short (0 – 1 month)	**5**	**2**	**1**
	Medium (1 – 6 months)	**7**	**4**	**3**
	Long (> 6 months)	**9**	**8**	**6**

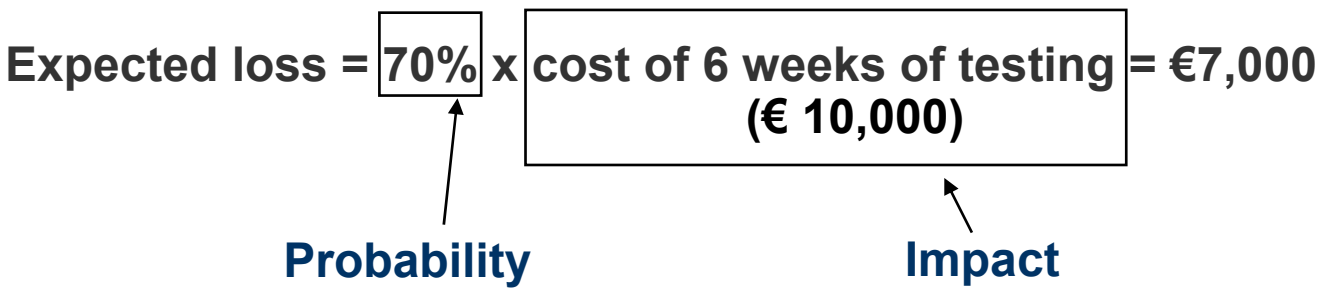
Top priority risks

Financial Exposure ("Expected Loss"):

Probability x Impact

Example:

Highly likely that integration testing will continue for 6 weeks.



Risk Analysis – Assessment Template

GLOBAL RISK MANAGEMENT@SAP

PROJECT REGISTER

Internal Use Only

ALIAS: /GRM

Select the Columns to Display

General | Analysis | Response 1 | Response 2 | All | ORM Selection

> Do not insert rows or columns.

> Mandatory fields shaded. required data is missing and "To ORM?" = "Y".

Display headers

Clear Register | Save ORM Data | Press after successful ORM upload > | Upload Successful

General Risk Information | **is**

ID	Common Risk Title	Title	Condition	Consequence	Total Loss	P	Time-frame	Global Impact Before Response	Local Impact Before Response	Expected Loss	Risk Level	Risk Prior-ity
1	ECONOMIC RISKS: External Attacks	External Attack	Attack on embassy located in same building as SAP	Disruption of SAP operations	6.000.000	2%	2		5	120.000	Med	
2	OTHER OPERATIONAL RISKS: Facilities and Physical Security	Protected Areas	Areas in the building exist requiring special protection e.g. Utilities in the Basement can be better protected.	Since these are areas where critical functions are being performed, a disruption here would cause disruption of business	3.000.000	20%	2		4	600.000	Med	
3	ORGANIZATION AND GOVERNANCE: Processes	Existence of Contingency Plans	Contingency plans not in place for all critical business processes and supporting infrastructure for Facilities.	No fall back measure in the event of disaster and business could get affected.	3.000.000	10%	2		5	300.000	Med	
4	OTHER OPERATIONAL RISKS: Loss of Infrastructure	Availability of critical resources	Danger of critical services, infrastructure and information being unavailable when needed - in the absense of an alternative site to transfer essential services.	In the event of a disaster like 'sabotage' / 'fire' in critical areas, this could lead to a long term disruption to business operations.	6.000.000	2%	1		5	120.000	Med	
5	OTHER OPERATIONAL RISKS: Integrity	Misuse of Passwords	There are known incidents regarding the misuse of (user-) passwords.	Possibility of future intentional or unintentional hacking into key systems, could lead to a disruption of business operations.		90%	3	3	4		High	1

Risk Response

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

GLOBAL RISK MANAGEMENT@SAP

ALIAS: /GRM

PROJECT RISK REGISTER

Internal Use Only

Response
The action(s) to be taken to respond to the risk

Select the Columns to Display

○ General ○ Analysis ◉ Response 1 ○ Response 2 ○ All ○ ORM Selection

> Do not insert rows or columns.

> Mandatory fields shaded [redacted] quired data is missing and "To ORM?" = "Y".

☑ Display headers

Clear Register | Save ORM Data | Press after successful ORM upload > | Upload Successful

General Risk Information					Risk Response					
ID	Common Risk Title	Title	Condition	Consequence	Response Type	Response	Response Owner	Response Cost	Prob. Reduced By After Resp.	Total Loss Reduced By After Resp.
1	ECONOMIC RISKS: External Attacks	External Attack	Attack on embassy located in same building as SAP	Disruption of SAP operations	Transfer	Ensure sufficient insurance coverage	d033861	10.000		1.000.000
2	OTHER OPERATIONAL RISKS: Facilities and Physical Security	Protected Areas	Areas in the building exist requiring special protection e.g. Utilities in the Basement can be better protected.	Since these are areas where critical functions are being performed, a disruption here would cause disruption of business	Mitigate	Implement security measurements (avoid public access to areas where critical fuctions are performed)	d033861	10.000	15%	
3	ORGANIZATION AND GOVERNANCE: Processes	Existence of Contingency Plans	Contingency plans not in place for all critical business processes and supporting infrastructure for Facilities.	No fall back measure in the event of disaster and business could get affected.	Mitigate	Setup Business Contengency Plans (BCP) for all relevant processes. Contact Corporate Security for support (Christine Trexler-Walde)	d033861	50.000	8%	
4	OTHER OPERATIONAL RISKS: Loss of Infrastructure	Availability of critical resources	Danger of critical services, infrastructure and information being unavailable when needed - in the absense of an alternative site to transfer essential services.	In the event of a disaster like 'sabotage' / 'fire' in critical areas, this could lead to a long term disruption to business operations.	Accept					
5	OTHER OPERATIONAL RISKS: Integrity	Misuse of Passwords	There are known incidents regarding the misuse of (user-) passwords.	Possibility of future intentional or unintentional hacking into key systems, could lead to a disruption of business operations.	Mitigate	- Enforcement in case of misuse - Ensure secure passwords (check regulary)	d033861		50%	

Upload Risks to ORM

GLOBAL RISK MANAGEMENT@SAP
ALIAS: /GRM

Maintenance Analysis Status Workflow
Activity-/Risk Maintenance Validation

Exit
ORT / 001

Activity/Risk Maintenance

Show | Get Organization Unit 30001396 Go | Open Advanced Search | Settings

Save | Page 1 of 1 Personalize

Object abbr.	Name
Root	
CorpSecurity	Corporate Security

Activities

Create | Edit | Cancel | Delete | Propose Risk | Upload Risk | Collaborative Risk | Link Risk | Import | Page 1 of 1 Personalize

Title	ID	Risk Level	Risk Priority	Probability	Expected Loss	Total Loss	Global Impact	Local Impact	Status	Analysis	Currency
Root											
Projects											
Processes											
Objects											
Facility / Security / IT (Location XX)	65	Low			430.000,00	17.000.000,00			Draft		EUR
Misuse of Passwords	136	Low	5	40			Moderate	Major	Draft	16.11.2004	EUR
External Attack	132	Low	7	2	100.000,00	5.000.000,00		Catastrophic	Draft	16.11.2004	EUR
Existence of Contingency Plans	134	Low	7	2	60.000,00	3.000.000,00		Catastrophic	Draft	16.11.2004	EUR
Protected Areas	133	Low	7	5	150.000,00	3.000.000,00		Major	Draft	16.11.2004	EUR
Availability of critical resources	135	Low	9	2	120.000,00	6.000.000,00		Catastrophic	Draft	16.11.2004	EUR

Approval Data

Approval Status* To be validated

Assessment frequency 3 Month

Validation – Approval of Risks & Response Strategy

- **"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)**

Validation – Approval of Risks & Response Strategy

GLOBAL RISK MANAGEMENT@SAP
ALIAS: /GRM

Maintenance Analysis Status Workflow
Workflow Inbox

Exit
ORT / 001

Complete work item | Save | Page 1 of 1 | Filter On | Personalize

WF	Title	Creation Date	Status
	Validation required for activity 65 - Facility / Security / IT (Location XX)	16.11.2004	READY

General Data | Owner Summary | Collaborative Summary | Attributes | Risk Grouping | Risks

Edit | Cancel

Administrative Data

Date	16.11.2004	Changing user/Creating user	D033861 Michael Collet
Activity ID	65	Identification Date	16.11.2004
Common Activity	50211458 FacSecIT	Activity type	Object

General Data

Title	Facility / Security / IT (Location XX)		
Assessment owner	D033861 Michael Collet	Organization Unit	30001396 CorpSecurity
Validator	D033861 Michael Collet	New Org Unit	00000000
Accountable Manager		Currency	EUR
Responsible		Opportunity Value	0,00

Approval Data

Approval Status	Validated
Assessment frequency	3 Month
Approval Comment	Please keep me updated by a bi-monthly reporting about the response implementation

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 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**

Risk Monitoring - Reporting

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)**

Copyright 2005 SAP AG. All Rights Reserved

Copyright 2005 SAP AG. Alle Rechte vorbehalten