

Risk and Control Self Assessments

Conference on Operational Risk Management
Karachi, 7-8 February 2013



I think self-awareness is probably the most important thing towards being a champion.



*Billie Jean King
US tennis player,
November 1973*

RiskBusiness


© 2013 RiskBusiness International Ltd.

 **Risk Self Assessments**


 

Self-assessment ≠ Self-criticism

 © 2013 RiskBusiness International Ltd.

 **Goals and objectives**

- Raise overall risk awareness
- Create transparency
- Know your institution
- Identify with risk ownership
- Provide comfort to management
- Learn from weaknesses identified
- Take appropriate action if necessary
- Reduce your losses - save money

 © 2013 RiskBusiness International Ltd.

Types of self-assessments




Workshop

Interview

Questionnaire

Identify risk and controls within an operational unit

Assess risk and the status of controls



RiskBusiness

© 2013 RiskBusiness International Ltd.

Designing a self-assessment

- Base your risk assessment on past losses
- Invite those responsible for past losses
- Focus on worst case

Self-assessment is not a blame session !



RiskBusiness

© 2013 RiskBusiness International Ltd.

Designing a self-assessment

- For example: Conduct workshops
- Select the right audience
- Create an atmosphere of trust
- Intervene if it is getting personal
- Discuss potential risks
 - What could go wrong?
 - Catalogue / group events
 - Judge probability
 - Estimate impact
- Agree on further steps



RiskBusiness

© 2013 RiskBusiness International Ltd.

How does it work in practice?

Step 1
Briefing and Knowledge Transfer

Step 2
Develop the Risk Profile

Step 3
Identify Processes, Risks and Controls

Step 4
Complete Detailed Assessments


Step 5
Review and Accept Results

Step 6
Update Risk Profile

Step 7
Distribute Risk Information

RiskBusiness

© 2013 RiskBusiness International Ltd.




Step 1 – Briefing and knowledge transfer

- Exactly stake out the scope and activities of the assessment unit
 - What does the unit do?
 - What is not part of their activities?
 - Whom do they depend on?
 - Who depends on them?
 - What technological support do they need?
 - etc.

© 2013 RiskBusiness International Ltd.

RiskBusiness



Step 1 – Assessing business environment

- The business environment is assessed with a view on understanding
 - **levels of business growth/change**
 - **competitive pressures**
 - **regulatory changes and requirements**
 - **technological complexities and outlook**
 - **staffing outlook**
 and our capability to deal with it
- Consideration of
 - Audit rating
 - Business Continuity rating
 - Compliance rating
 - Historical Loss rating

© 2013 RiskBusiness International Ltd.

RiskBusiness

Step 2 – Risk profiling

- What is risk profiling?
 - A **subjective assessment** of the overall operational risks facing the assessment entity at a point in time
- How do we develop the profile?
 - Pre-defined set of risk categories
 - Pre-defined set of business functions
 - Using business expertise, **assess the impact of each risk category on each business function** in isolation
 - This is known as a risk point

© 2013 RiskBusiness International Ltd. *RiskBusiness*

Step 2 – Risk profiling

Business Function	Risk Categories			Assessment Entity	
	Processing OP&P	Conduct C&W	External E&F	1 Products	2 etc
Originion					
Execution					
Processing & Operations					
Business Continuity					
Technology					
Finance					
Oversight					
Human Resources					
Corporate Services					

© 2013 RiskBusiness International Ltd. *RiskBusiness*

Step 2 – Risk profiling: What could go wrong?

- Nothing ever goes wrong, we have controls.
 - What if controls fail?
 - Which processes are vulnerable?
 - What could happen?
 - Why could it happen?

RiskBusiness

© 2013 RiskBusiness International Ltd.

Step 2 – Risk profiling

RiskBusiness Risk Profile
Current Business Entity: Business Unit One

Home Page Services Maintenance Sign Off

OK Cancel Details

		Internal Damage	Reputational Damage	Legal and Regulatory	Operational Disruption	Financial Impact	Strategic Impact	Compliance	Other
Origination	Product or Service Development and...	2	1	5	6	4	2	3	1
	Customer Relationship Management	4	2	3	4	2	6	6	1
	Credit Review and Approval	1	4	4	4	4	5	6	5
	Models and Methodologies	6	6	6	6	5	4	3	2
	Research	1	5	4	3	3	2	5	6
	Custom or Structured Transaction In...	1	2	2	2	2	2	2	2
	Reference Data Creation and Mainten...	1	1	3	1	1	1	1	1
Execution	Third Party Distribution Channel Ma...	1	3	3	1	3	3	2	2
	Advisory Services	1	1	1	1	1	1	1	1
	Pricing and Quotations	4	3	2	3	4	3	6	3
	Limits and Facility Checking	6	5	2	2	6	2	3	2
	Insulation Management	6	4	6	4	6	4	6	4

© 2005, 2006, 2007 RiskBusiness International Limited

© 2013 RiskBusiness International Ltd. Screenshot from RiskBusiness RCSA Tool

Step 2 – Risk profiling – rating bands

Overall Risk	Granularity	Score	Criteria
High	High	9	Severe risk that could make the product or the business a contributor to major loss
	Medium	8	Severe risk mandating senior management attention
	Low	7	High risk mandating close business management attention
Medium	High	6	Medium risk requiring business management attention
	Medium	5	Medium risk requiring middle management attention
	Low	4	Medium risk requiring ongoing observation by supervisory or senior clerical staff
Low	High	3	Low risk that could be reduced by more efficient controls
	Medium	2	Low risk, generally assumed as cost of doing business
	Low	1	Immaterial every-day risk not worth mitigating
Not Applicable		0	Impossible combination of Risk Category and Business Function, either by default or by absence of business function

RiskBusiness


© 2013 RiskBusiness International Ltd.

Step 3 – Identify processes, risks and controls

- What part of the process is vulnerable?
- Identify the reasons for the vulnerability
 - The more detailed the process step can be identified, the more likely we can identify the vulnerability
- Document existing controls to address the weakness

RiskBusiness



© 2013 RiskBusiness International Ltd.



Step 3 – Overview

- For each identified “high exposure” risk point, perform:
 - **Process** Identification
 - **Risk** Identification
 - **Control** Identification
- For each identified control, complete a **Control Design Strength Assessment**

© 2013 RiskBusiness International Ltd.






Step 3 – Process identification

- The following example illustrates how the **process identification** is performed:

Level 1 (function - profiling)	Origination	} Standard, from Entity Taxonomy
Level 2 (function - profiling)	Customer Relationship Management	
Level 3 (process 1)	Customer Acquisition	
Level 3 (process 2)	Onboard Customer	
Level 3 (process 3)	Perform KYC and AML Checks	

© 2013 RiskBusiness International Ltd.





Step 3 – Risk identification

Purpose

- To **identify specific risks** within selected risk points, allocating them to processes where they are likely to occur

Risk Categorization


- The following example illustrates how the Taxonomy categorizes the risk of an extra zero in an amount:

Level 1	Execution, Delivery & Process Management
Level 2	Human Processing Error
Level 3	Transaction Execution & Data Capture Failures
Level 4	Accounting Data Entry Errors

Standard, from Entity Taxonomy

RiskBusiness

© 2013 RiskBusiness International Ltd.



Step 3 – Control identification

Purpose

- To **identify controls** for each selected risk point

Control Classification

- Example of the Taxonomy classifying control types:

Class of Control	Function
Detective	To discover errors or undesirable circumstances – and reduce impact e.g. <i>End of day reconciliation</i>
Preventative	To prevent errors and undesirable circumstances e.g. <i>Data encryption as a means of preventing access to proprietary data during transmission</i>
Oversight	To monitor circumstances and ongoing operations e.g. <i>A register of all potential or known conflicts of interest is maintained and reviewed to ensure no conflicts of interest occur</i>
Resolution/Response	To assist in resolving circumstances e.g. <i>Business Continuity, Process Recovery or Resiliency Program</i>
Planning/Guidance	To guide management and staff in business execution e.g. <i>Implementation of policies, standards and guidelines to induce correct behavior</i>
Governance	High level controls to provide an appropriate business environment e.g. <i>Audit reviews and reporting, internal</i>

RiskBusiness

© 2013 RiskBusiness International Ltd.



Step 3 – Control design strength assessment

Purpose

- To assess the **inherent strength of control design** and understand which risks are mitigated


Elements of design strength

- What is the degree of automation?
- How comprehensive is coverage of the control?
- Does the control activate when needed?
- How correlated is the control to specific risks?
- Is the control rules-based?
- Is it a “key control”?
- Side consideration: How much does the control cost?



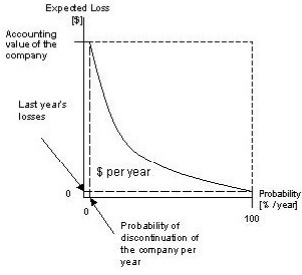
© 2013 RiskBusiness International Ltd.







Step 4 – Detailed assessment


- **Two Part Approach**
 - Control Effectiveness Assessment
 - Risk Assessment








© 2013 RiskBusiness International Ltd.





Step 4 – Control effectiveness assessment


Purpose

- To evaluate the effectiveness of each control as applied to a specific risk within a specific process

Scoring matrix - example

Score	Meaning
Very Low	Totally ineffective
Low	Not that effective in countering risk
Medium	Generally effective in countering risk
High	Highly effective and typically counters risk
Very High	Extremely effective in countering risk

© 2013 RiskBusiness International Ltd. **RiskBusiness**



Step 4 – Overall risk assessment


Purpose

- To **measure the residual exposure**, after the effect of controls, to each identified risk
- Exposure is measured using a combination of
 - direct (financial & efficiency) and
 - indirect risk ratings (reputational, non financial regulatory, other)

Scoring

- Value (\$) based impact** is used to assess direct impact. The same ranking is used for **efficiency impact**.
- Point rating scale** (e.g. 1-5) is used for indirect impact, using a series of statements assessing reputational or other factors

© 2013 RiskBusiness International Ltd. **RiskBusiness**




Step 4 – Impact – Judging Probability

- How often do we expect an incident in which area?

Once a week	Transaction settlement
Once a month	IT outage
Once a quarter	Staff experience
Once a year	Regulatory
Once a decade	Disaster Recovery

RiskBusiness

© 2013 RiskBusiness International Ltd.



Step 4 – Impact – Estimation of Cost

- What could an incident cost?

Once a week		Transaction settlement			
Once a month		IT outage			
Once a quarter		Staff experience			
Once a year			Regulatory		
Once a decade				Disaster Recovery	

up to	\$ 10,000	\$ 100,000	\$ 1,000,000	\$ 10,000,000	> \$ 10,000,000
-------	-----------	------------	--------------	---------------	-----------------

RiskBusiness

© 2013 RiskBusiness International Ltd.

Step 5 – Impact – Tolerance Level

- Where is our financial tolerance level?

Once a week		Transaction settlement			
Once a month	IT outage				
Once a quarter	Staff experience				
Once a year			Regulatory		
Once a decade				Disaster Recovery	
up to	\$ 10,000	\$ 100,000	\$ 1,000,000	\$ 10,000,000	> \$ 10,000,000

© 2013 RiskBusiness International Ltd. **RiskBusiness**

Step 5 – Impact – Reputation

- What impact do events have on our reputation?

Once a week		Transaction settlement			
Once a month	IT outage →				
Once a quarter	Staff experience				
Once a year			Regulatory		
Once a decade			←	Disaster Recovery	
	None / unpleasant	Press notice	Broad public discussion	Bank is under serious pressure	Achievement of objectives made uncertain

© 2013 RiskBusiness International Ltd. **RiskBusiness**

Step 5 – Review and Accepting of Results

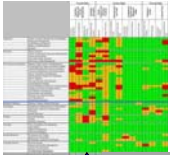
- Review RCSA results within the assessment unit
- Accept and sign-off the RCSA output
 - **Within tolerance:** no action required
 - **At tolerance:** contemplate action if possible
 - **Outside tolerance:** action required

RiskBusiness

© 2013 RiskBusiness International Ltd.

Step 6 – Risk point revaluation as a result

Entity Profile	Risk: Best Execution
Activity: Instruction or Order Management	Risk manifestation: Orders filled by customer preference, not order receipt (first in, first out)



Aggregate to Domain/Country Group profiles


Update Entity Risk Profile

Process Identification	
Control Identification	
Control Design Strength	Satisfactory
Control Effectiveness	Unsatisfactory


Is the risk within risk tolerance acceptance levels?	
Yes / No	

Risk Assessment (residual exposure)	
Anticipated Annual Impact (direct/indirect)	50,000
Expected Frequency of Occurrences	2 per year
Worst Case 1 in 10 years impact (direct/indirect)	500,000

Risk Identification	
---------------------	--





© 2013 RiskBusiness International Ltd.



Step 7 – Distribute risk information

- Publish RCSA results and distribute appropriately
- Aggregate assessment entity output to domain, country and Group level
- Develop and deliver risk reports
- Provide required information to 3rd party constituents e.g. regulators, external auditors, etc.
- Following completion of the RCSA process:
 - Initiate any desired corrective or mitigating action
 - Identify / validate key risk indicators (KRI)
 Outside the Assessment Entity:


© 2013 RiskBusiness International Ltd.

The honesty issue

- Risk denial is a common occurrence
- Important:
 - **Be aware of cultural inhibitions**
 - Establish a no-blame atmosphere
 - Create incentives
- Do not focus on the worst case
- Do your homework, have expectations

© 2013 RiskBusiness International Ltd.






The power of the RCSA




- 360° health check
- Awareness of indirect factors affecting the business
- Evaluation of potential control failures and risks
- Discovery of weak or missing controls → improvements
- Assignment of accountability
- Increased awareness of senior management → support
- Actions following RCSA
- Foundation for KRI selection
- Basis for development of scenarios

© 2013 RiskBusiness International Ltd.

Contact Details



Hansruedi Schütter
Executive Director Europe, Asia and Middle East

Telephone	+41 - 76 - 558 7632
Skype	schuetter
LinkedIn	Hansruedi Schuetter
E-mail	hansruedi.schuetter@riskbusiness.com
URL	www.riskbusiness.com

RiskBusiness is a specialist advisory services firm with focus on operational risk within the broader enterprise risk environment. It comprises exclusively of leading ex-practitioners focused on sharing their experiences with its clients.
The RiskBusiness **RCSA tool** is a web-based application and is offered on a subscription basis.

© 2013 RiskBusiness International Ltd.

