RBAC and Financial Risk

Espen Opheim
Manager

25. November, 2010

avanade®
Results Realized

Agenda

- Risk
- COSO ERM
- ”CIA”
- Role-Based Access Control (RBAC)
- Separation of Duty (SoD)
- Suggested approach to implementing SoD
- Limitations and Contraints

Risk

- Operational risk
  - Fraud risk
  - Legal risk
  - Physical risk
  - Environmental risks
- Financial risk
  - Investment risk
  - Business risk
  - Credit risk
  - Market risk
  - Liquidity risk

avanade® Results Realized

COSO ERM Framework

- Efficient and effective operations
- Accurate financial reporting
- Compliance with laws and regulations

Download here http://www.coso.org/ERM-IntegratedFramework.htm

avanade® Results Realized

”CIA”

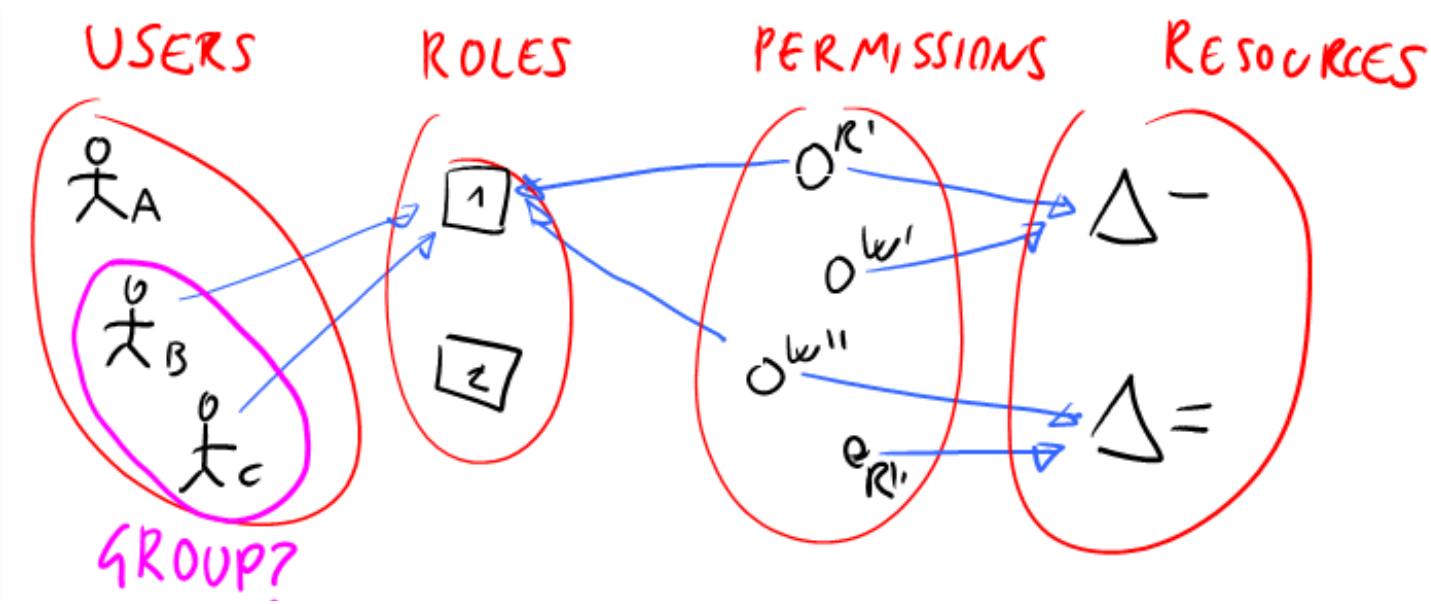
- Data confidentiality
  - Confidentiality refers to limiting information access and disclosure to authorized users -- "the right people" -- and preventing access by or disclosure to unauthorized ones -- "the wrong people."
- Data integrity
  - Integrity refers to the trustworthiness of information resources - that data have not been changed inappropriately, whether by accident or deliberately malign activity
  - requirement that data and processes be modified only in authorized ways by authorized users (Ferraiolo & Kuhn 1992)
- Data availability
  - An information system that is not available when you need it is at least as bad as none at all.

COSO and information security

	Data confidentiality	Data integrity	Data availability
Efficient and effective operations		X	X
Accurate financial reporting		X	X
Compliance with laws and regulations	X	X	X

RBAC

- In computer systems security, role-based access control (RBAC) is an approach to restricting system access to authorized users. (Wikipedia)



Separation of Duty (SoD)

Separation of duty requires that for particular sets of transactions, no single individual be allowed to execute all transactions within the set. The most commonly used examples are the separate transactions needed to initiate a payment and to authorize a payment. No single individual should be capable of executing both transactions.

avanade® Results Realized

Scandals arising from poor SoD

- Societe Generale, $7 billion in losses: Operations expert moved to trading desk, taking some jobs with him.
- Barings Bank, $1 billion in losses: Operations and trading managed by the same individual.
- Lehman Brothers, $0.3 billion in losses: Sales manager took over certain simple operations functions.
- Daiwa, $1.1 billion in losses: Same scenario as Societe Generale.
- Allied Irish Bank, $0.7 billion in losses: Risk limit reporting under control of trader.
- Tyco, $0.3 billion in losses: Three top executives colluded and board of directors exercised ineffective supervision.
- Orange County, $1.6 billion in losses: Trader seen as the unquestioned maestro, while back office was underpowered to understand his trading procedures.

Roles and Permissions

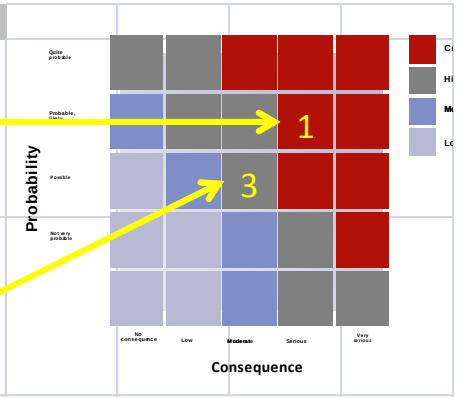
No.	Role	Permissions
1	Vendor Master Maintenance	Create, change or delete vendor master records including payment information such as bank account or routing number
2	Requisition Authorization	Create, change or delete requisitions requests in the system
3	Purchase Order Entry	Create, change or delete transaction records for a purchase order
4	AP Invoice Entry	Create, change or delete transaction records for an invoice in the system

avanade® Results Realized

Conflicting roles

- Individual users need to be able to join more than one Role. This COULD be a risk:

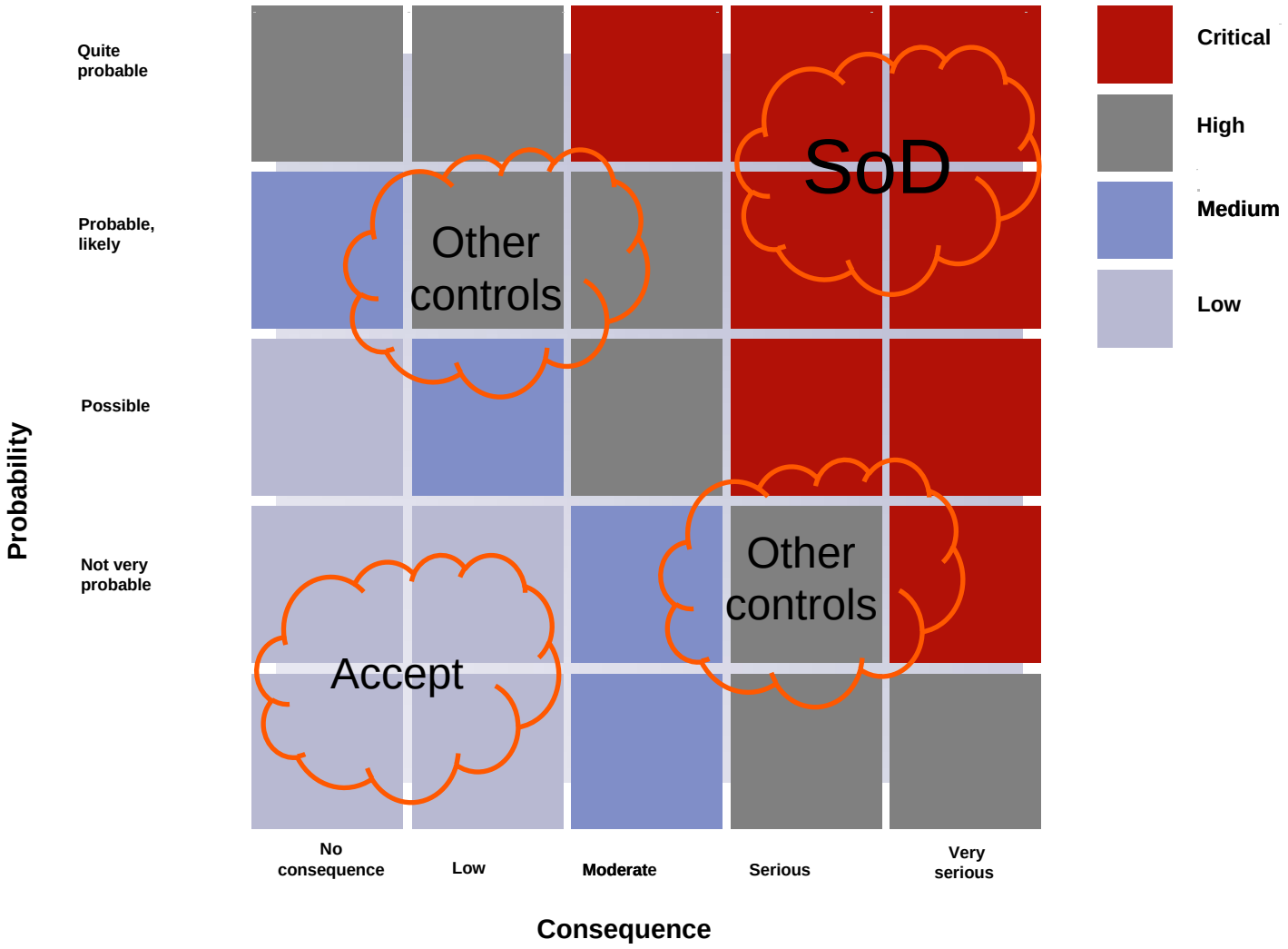
#	Conflicting Functions		Example Risks	Probability	Consequense
1	1. Vendor Master Maintenan	3. Purchase Order Entry	An individual could create fictitious supplier or change existing vendor information (pay to address) and process purchase order against the vendor.	P=4	C=4
2	1. Vendor Master Maintenan	4. Accounts Payable Invoice En	An individual could create nonexistent or unauthorized vendors for payment, as well as change payment information on an existing vender. (I.e. bank routing information)	P=3	C=3



- The example risk defines the risk associated with one user beeing assigned to to to roles
- The probability/consequence assessment ranks the individual risks.
- Some combinations of roles will be incompatible and should be separated by system based SoD or other control mechanisms SoD is not achiavable
- Some risks will be acceptable (below threshold for acceptable risk)

avanade® Results Realized

Risk assessment



Sample SoD Matrix

Task Group Description	Grp	1 AP Voucher Entry	2 AP Payments	3 AP Release Blocked Inv	4 AP Clear Vendor Acct.	5 Vendor Mast. Maint. FI	6 Vendor Mast. Maint. MM	7 Vendor Mast. Maint. CEN	8 Bank Reconciliation	9 AR Cash Application	10 AR Clear Customer Acct.	11 Material Master Maint.	12 Service Master Maint.	13 Requisitioning	14 Release Requisition	14A Process Requisition	15 Purchase Order Entry	16 Purchasing Agreements	17 Goods Receipt on PO	18 Service Receipts Entry	19 Physical Inventory	20 Sales Agrmts/Contracts	21 Customer Master Maint.	22 Customer Master (Credit)	23 Sales Invoicing	24 Sales Invoice Release	25 Sales Order Entry	26 Sales Order Release	27 Sales Pricing Maint.	28 Sales Rebates	29 Maintain Security
AP Voucher Entry	1		X	X	X	X	X	X									X	X	X	X											X
AP Payments	2	X				X	X	X	X								X	X													X
AP Release Blocked Inv	3	X															X	X	X	X											X
AP Clear Vendor Acct.	4	X															X														X
Vendor Mast. Maint. FI	5	X	X				X										X	X													X
Vendor Mast. Maint. MM	6	X	X			X											X	X													X
Vendor Mast. Maint. CEN	7	X	X														X	X													X
Bank Reconciliation	8		X							X																					X
AR Cash Application	9								X													X	X	X	X		X			X	X
AR Clear Customer Acct.	10																					X			X		X			X	X
Material Master Maint.	11													X			X	X													X
Service Master Maint.	12													X			X	X													X
Requisitioning	13											X	X		X		X	X													X
Release Requisition	14													X			X	X													X
Process Requisition	14A													X			X	X													
Purchase Order Entry	15	X	X	X	X	X	X	X				X	X	X	X				X	X											X
Purchasing Agreements	16	X	X	X		X	X	X				X	X	X	X				X	X											X
Goods Receipt on PO	17	X		X													X	X			X										X
Service Receipts Entry	18	X		X													X	X													X
Physical Inventory	19																		X												X
Sales Agrmts/Contracts	20									X	X												X	X							X
Customer Master Maint.	21									X												X					X				X
Customer Master (Credit)	22									X												X					X				X
Sales Invoicing	23									X	X															X			X		X
Sales Invoice Release	24																								X						X
Sales Order Entry	25									X	X												X	X				X	X	X	X
Sales Order Release	26																										X				X
Sales Pricing Maint.	27																								X		X				X
Sales Rebates	28									X	X																X				X
Maintain Security	29	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	

Limitations of the model

- Separation of Duty does not prevent a deliberate fraud when perpetrated in a collusion of two or more persons

Constraints

- Cost of implementing and training
- Additional staff required
- Transaction processing time
- Efficiency loss
- Small department sizes makes SoD impossible to achieve:

"Issue related segregation of duty has been discussed with [client] during the design phase. One specific issue discussed, is possibility for users to both change Vendor account number, and generate / send payments to the same Vendor. [client] don`t consider the risk related to this as a problem. With a small finance department, segregation of duty is hard to implement, and could have negative effect on the department efficiency. By this, segregation of duty is not seen as a issue to be considered."