RBAC and SoD

Espen Opheim
Manager

31. March, 2011

avanade®
Results Realized

Agenda

- About Avanade
- Enteprise Resource Planning (ERP)
- ”CIA”
- ERP risks
- Role-Based Access Control (RBAC)
- Separation of Duty (SoD)
- Suggested approach to implementing SoD
- Limitations and Contraints

avanade® Results Realized

The power of three - Accenture and Avanade relationship with Microsoft is strong

In June 2009 Accenture and Avanade was named Microsoft's Enterprise Alliance Partner of the Year

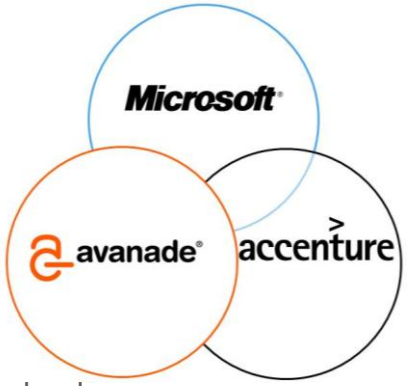
"Avanade is Microsoft's secret weapon in the enterprise"

- Steve Ballmer

Avanade was formed in 2000 as a joint venture company owned by Microsoft and Accenture. Avanade is specialized in complex, enterprise-scale solutions i.e. ERP with 100% focus on Microsoft solutions and applications. The relationship between Microsoft, Accenture and Avanade is strong both locally and globally. Avanade is a Microsoft Gold Partner with certification within Microsoft competence areas such as: Advanced Infrastructure, Security, Networking Infrastructure, Business Process & Integration, Information Worker, Microsoft Dynamics.

Power of Three – a strong alliance

- Specific product expertise
- Technical innovation



- The global technology integrator dedicated to the Microsoft enterprise platform

- Consulting expertise
- Complex program management
- Industry knowledge

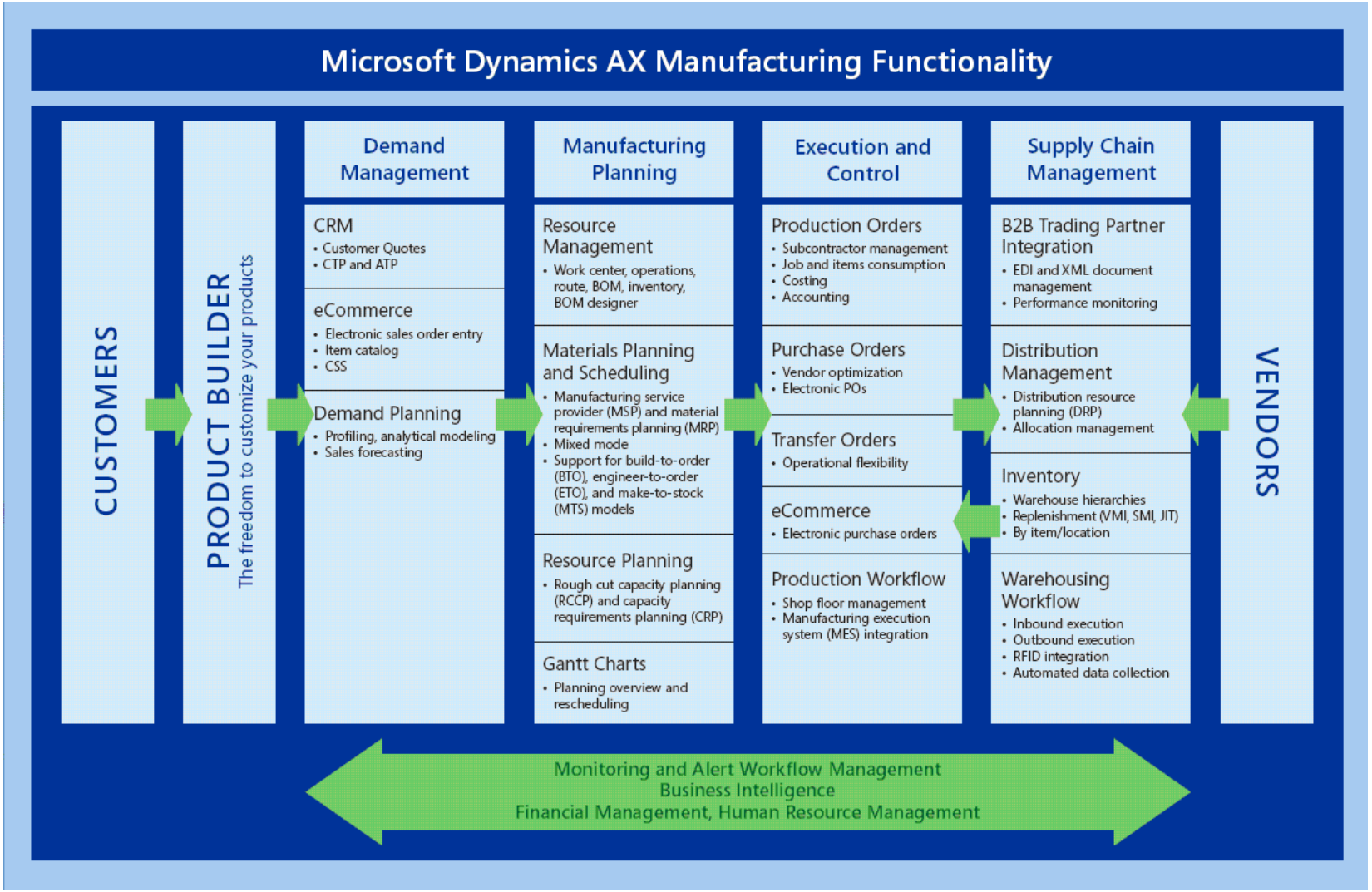
avanade® Results Realized

Enteprise Resource Planning (ERP)

integrates internal and external management information across an entire organization, embracing finance/accounting, manufacturing, sales and service, etc. ERP systems automate this activity with an integrated software application. Its purpose is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders.[1]

(Wikipedia)

ERP – Manufactoring in AX



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.

ERP risks

1. Human error - insiders

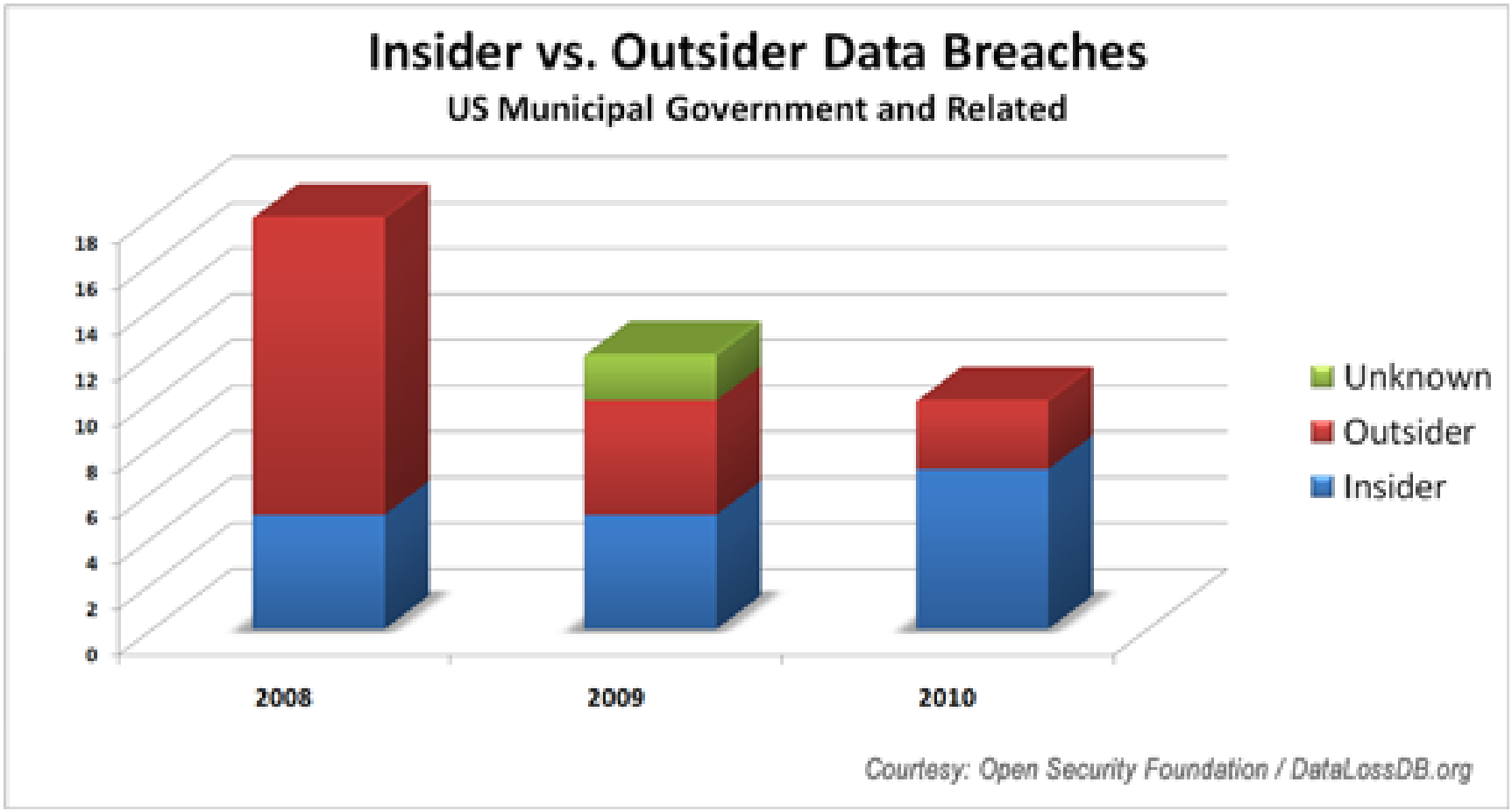
   intentional or accidental misuse of an organization's resource

2. Data theft/destruction/alteration - outsiders

3. ”Malicious code” (modifications/developement)

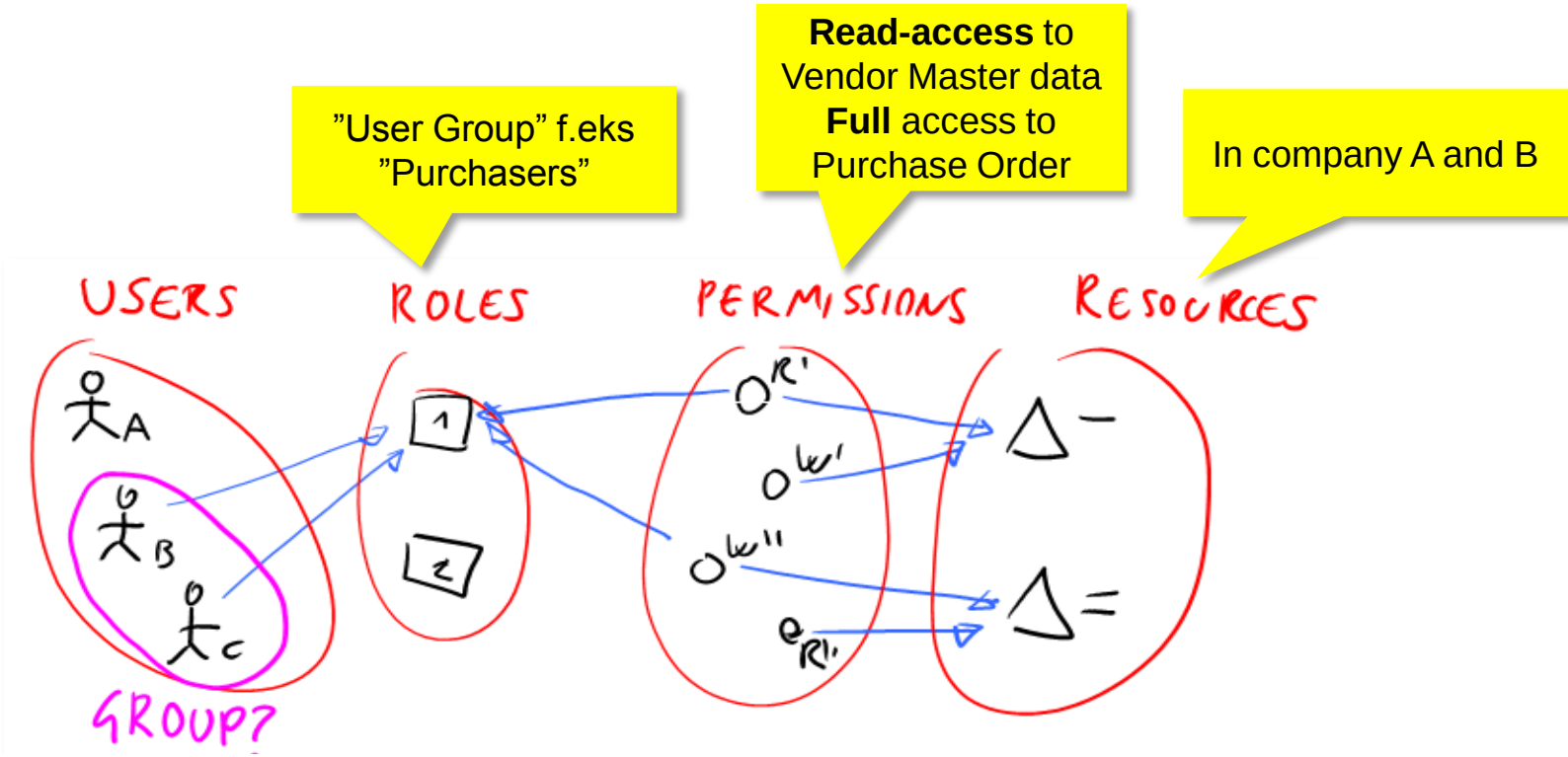
avanade® Results Realized

Insider vs. Outsider Data Breaches



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)

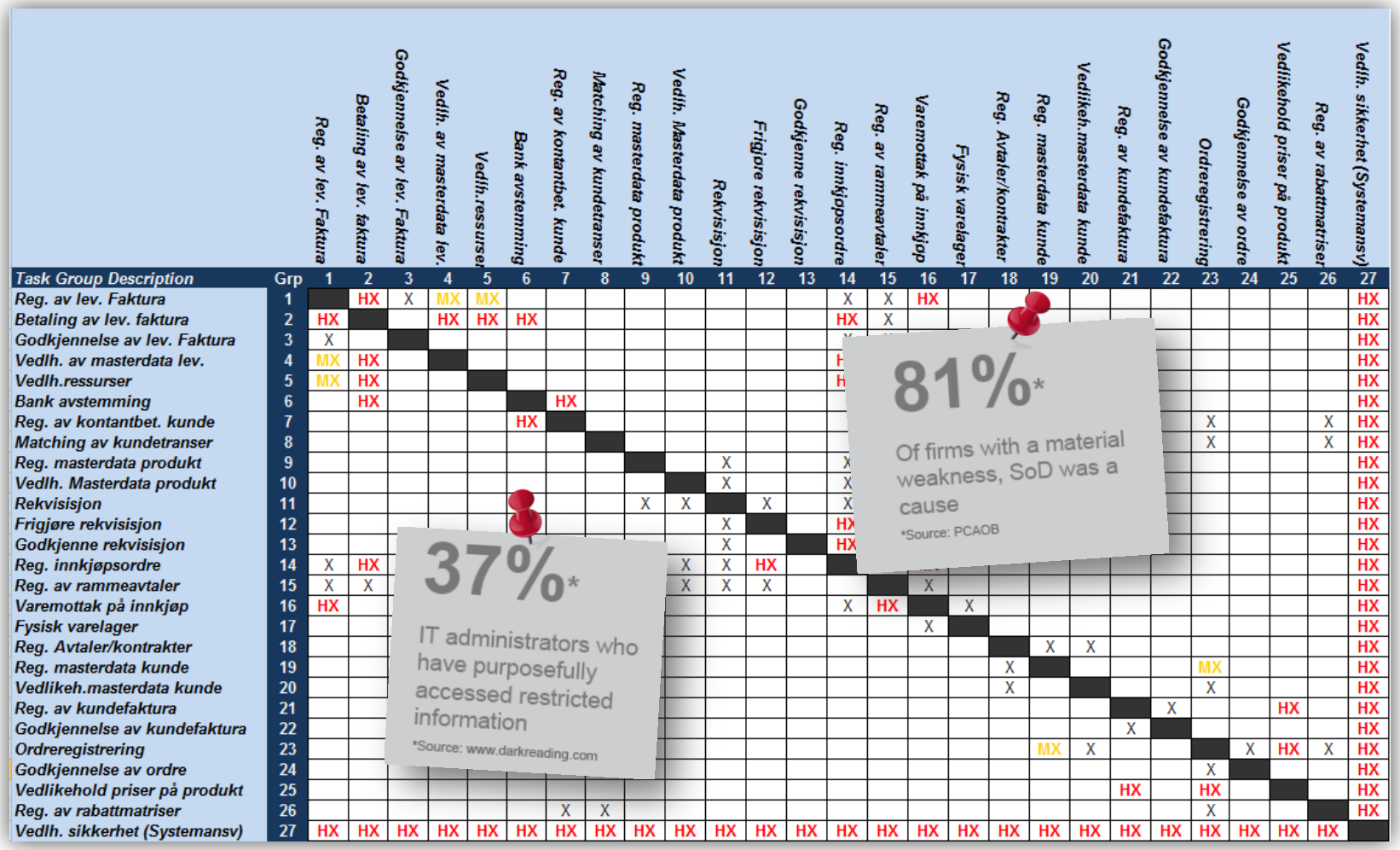
Separation of duty requires that for particular sets of transactions, no single individual be allowed to execute all transactions within the set. The most commonly used examples are the separate transactions needed to initiate a payment and to authorize a payment. No single individual should be capable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

Weak internal control



Roles and Permissions

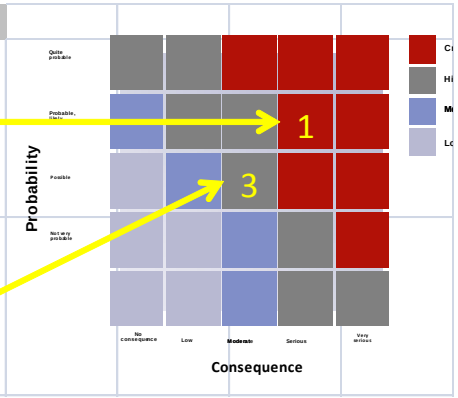
No.	Role	Permissions
1	Vendor Master Maintenance	Create, change or delete vendor master records including payment information such as bank account or routing number
2	Requisition Authorization	Create, change or delete requisitions requests in the system
3	Purchase Order Entry	Create, change or delete 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:

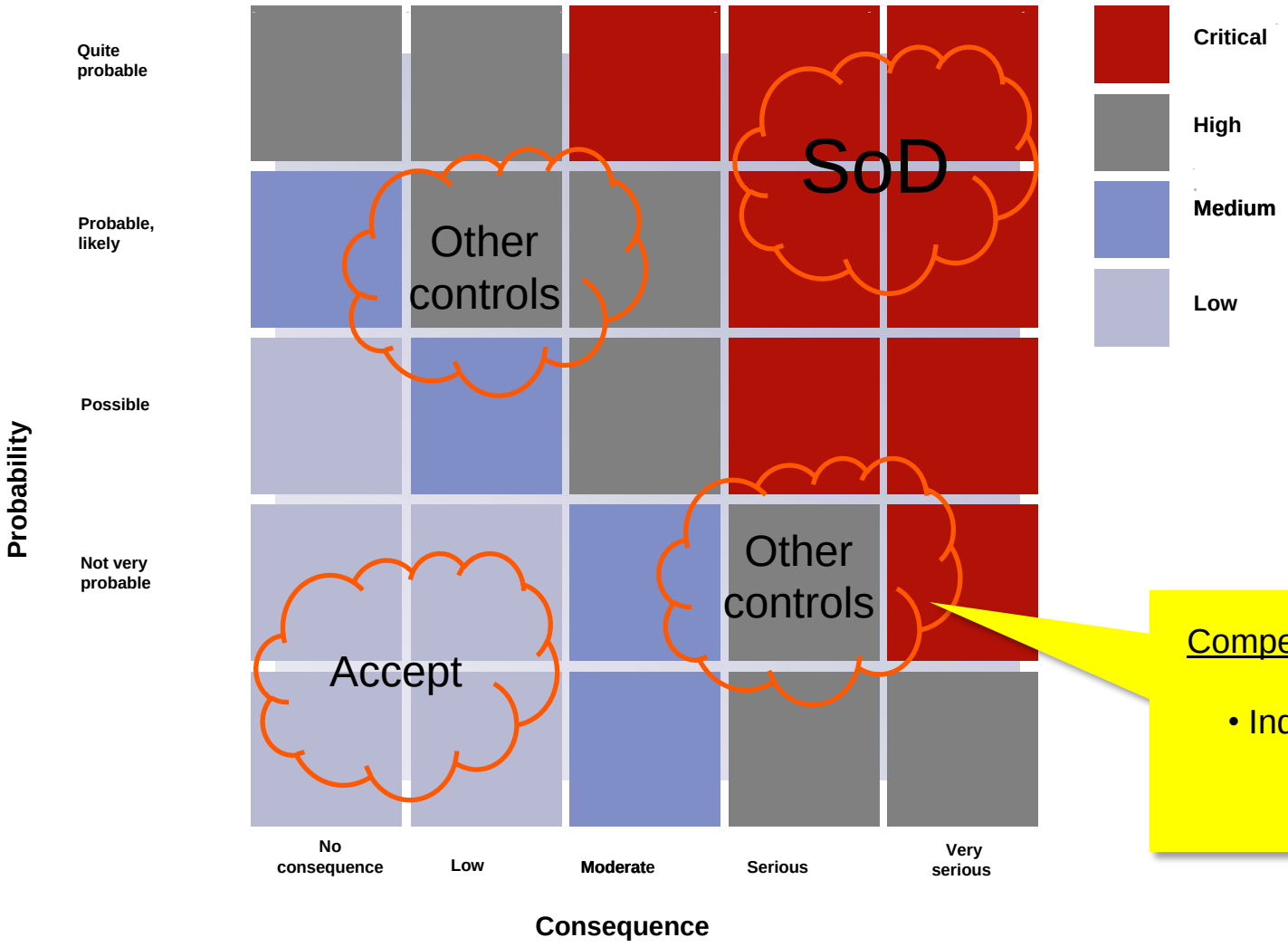
#	Conflicting Functions		Example Risks	Probability	Consequense
1	1. Vendor Master Maintenan	3. Purchase Order Entry	An individual could create fictitious supplier or change existing vendor information (pay to address) and process purchase order against the vendor.	P=4	C=4
2	1. Vendor Master Maintenan	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



Compensating controls:
- Database logs
- Independant review
- Monitoring
- Continous audit

Sample SoD Matrix

- 2 risks with high probability identified
- 7 risks with medium probability identified

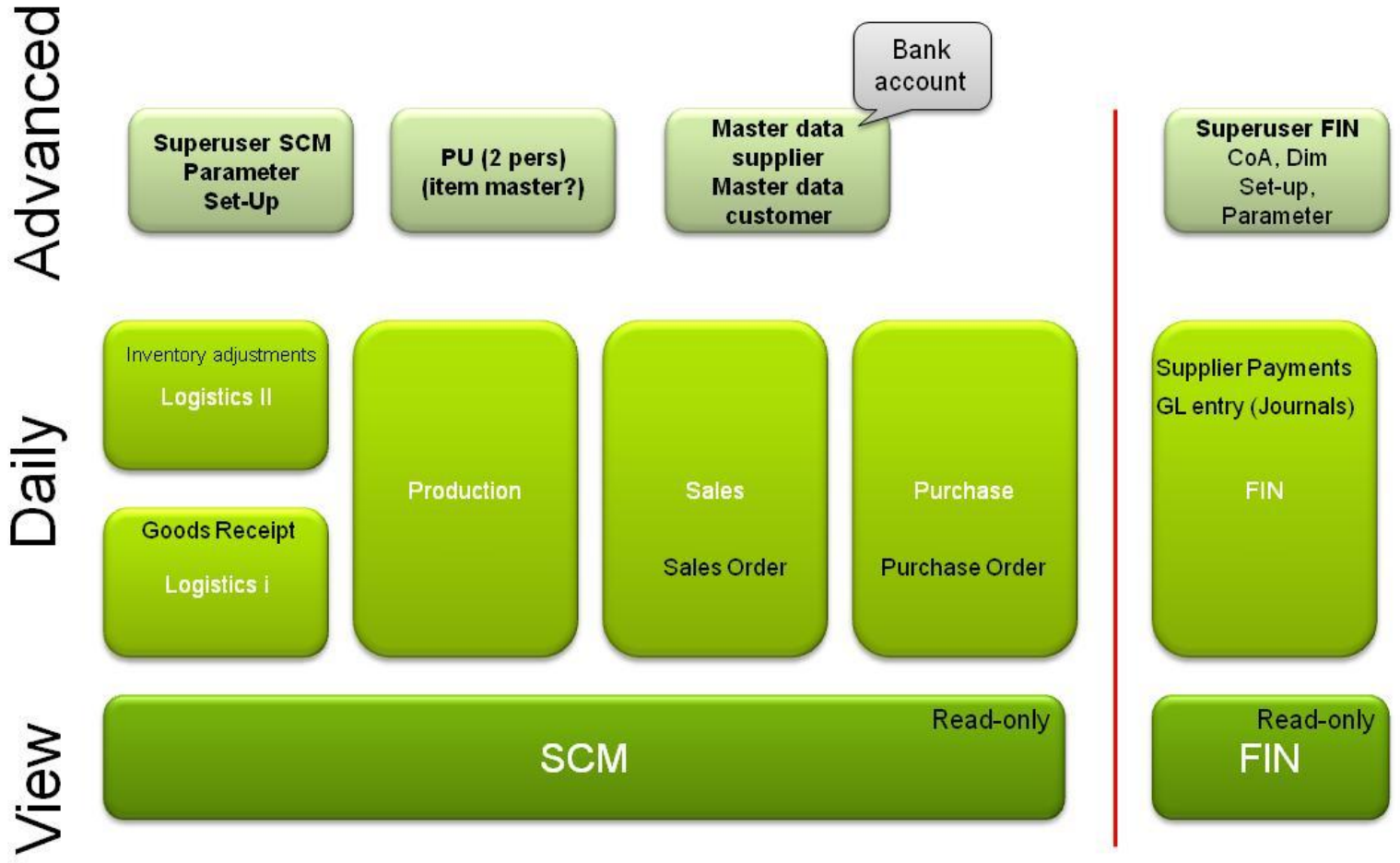
- Master data supplier (bank account #)
- Purchase Order (PO)
- Supplier payments
- Goods Receipt
- Inventory adjustments
- Master data Customer (ship to address)
- Sales Order (SO)
- GL entry (journals Insufficient control of techn. work progress

- ”X” marks conflicting functions that may not be granted to one individual user
- The person responsible for Policy enforcement must perform conflict check prior to providing system access
- When SoD impossible to achieve due to organizational constraints, compensating controls must be implemented and monitored (periodic review or database logging)

	Master data supplier	Purchase Order (PO)	Supplier payments	Goods Receipt	Inventory adjustments	Master data Customer	Sales Order (SO)	GL entry (journals)
Master data supplier		X	X	X				X
Purchase Order (PO)	X		X	X	X			X
Supplier payments	X	X		X	X			X
Goods Receipt	X	X	X		X			X
Inventory adjustments		X	X	X			X	
Master data Customer							X	X
Sales Order (SO)					X	X		
GL entry (journals)	X	X	X	X		X		

avanade® Results Realized

Simple SoD structure (actual case)



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)
- Management ownership (Business vs. IT)
- 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."

espen.opheim@avanade.com

Speakers details

Espen Opheim | Manager
Avanade Norway
Snarøyveien 30, Pb 486,
N-1327 Lysaker, Norway
Switchboard: +47 67 12 85 70
Mobile: +47 468 43 590
E-mail: espen.opheim@avanade.com
www.avanade.com

avanade® Results Realized