

A Successful Implementation of a User Access Management System at E.ON Global Commodities (EGC)

Dr. Carsten Mielke, 04.11.2014

Head of Service Management

E.ON



Agenda

- E.ON Global Commodities SE
- Motivation/Drivers
- Pre-Requisites
- Vendor Selection process
- Added Value
- Lessons Learned
- Challenges Ahead

E.ON Global Commodities SE



E.ON Global Commodities SE

The energy trading business of E.ON, one of the world's largest investor-owned power and gas companies.

As the expert interface between the E.ON Group and international wholesale energy markets, we create value by managing the commodity price risks faced by E.ON and its customers, while optimizing the Group's broad and diverse power and gas portfolio.

- over **1000 professionals** from more than **40 countries**, based in headquarters in Düsseldorf
- one of the most active traders in the international wholesale energy markets
2011 volumes: **Gas 2480 billion kWh, Power 1967 billion kWh, Carbon 598 million metric tons, Coal 269 million metric tons, Oil 89 million metric tons** (~ 600 million barrels);
- active on more than **20 exchanges** and in over **40 countries**
- executed more than **850,000 trades** in 2011

The drivers for a professional User Access Management

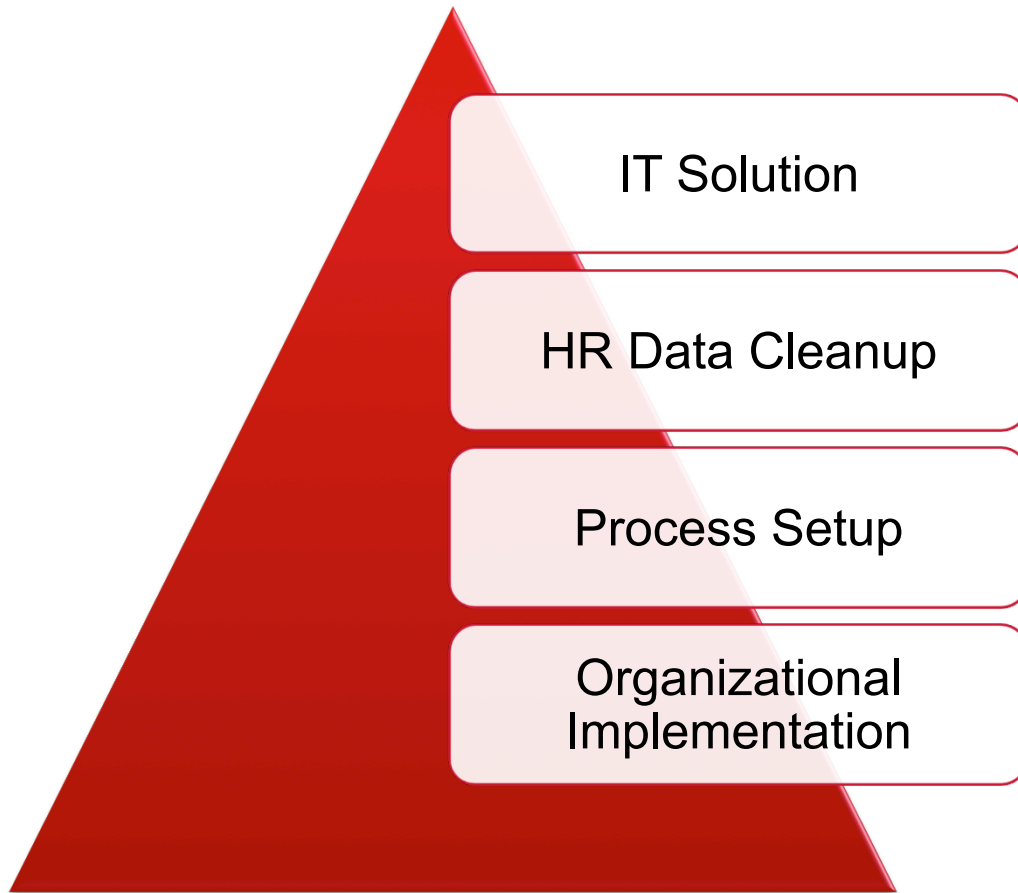
- Audits (according to Audit standards IDW RS FAIT 1, IDW PS330) showed strong need for improvement of evidence for **legal demands on authorization and authentication.**
- Capabilities required
 - record the granting, amending and revoking of access rights to applications in scope of the EET application access processes;
 - enable control on whether internal control process requirements are working effectively at all times

“Nothing is more powerful than an idea whose time has come” – Victor Hugo

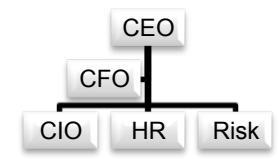
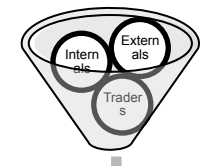
Expected benefits

- **Harmonisation and standardization of user access related processes**
 - From different user application templates down to one, later to a workflow in the Intranet
- **Better control of users, roles and privileges in the target systems**
 - Reducing the risk of abuse of non-intended status
 - Quicker access, changes and termination of accounts in target systems
- **User accounts and licenses can be better controlled**
 - Cost reduction possible
- **Auditing control functions of SoD (Segregation of Duties) and sensitive access rights will be available in a more sophisticated way**
 - Reducing effort in providing audit evidence

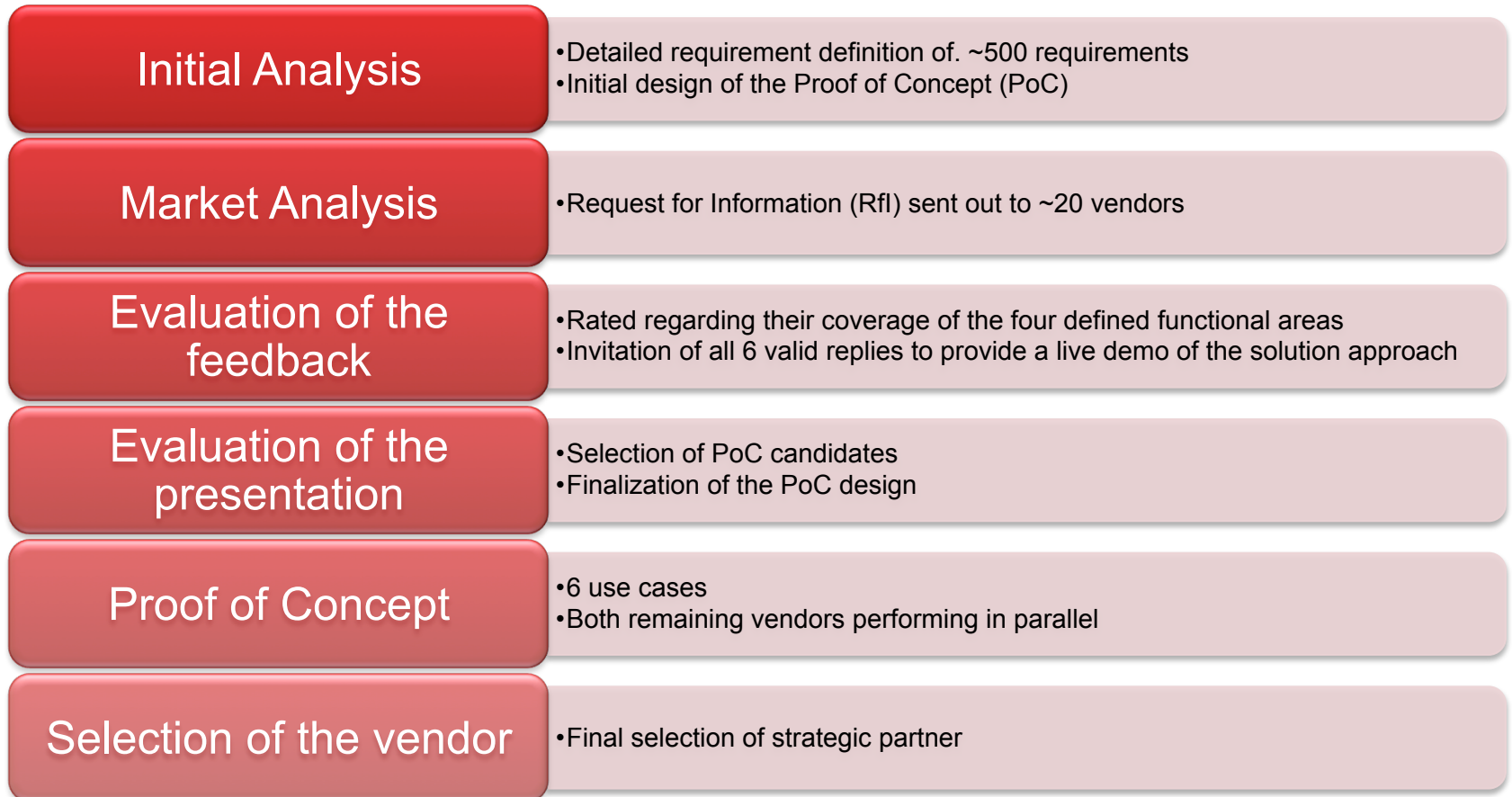
Prerequisites for UAM at E.ON Global Commodities




Market Evaluation	Final selection of the best option based on the market evaluation criteria.
Vendor Long List (20)	Final selection of the best option based on the market evaluation criteria.
Vendor Short List (5)	Final selection of the best option based on the market evaluation criteria.
PoC Candidates (2)	Final selection of the best option based on the market evaluation criteria.
Selected partner (1)	Final selection of the best option based on the market evaluation criteria.



Introduction of an IT Solution – Vendor Selection



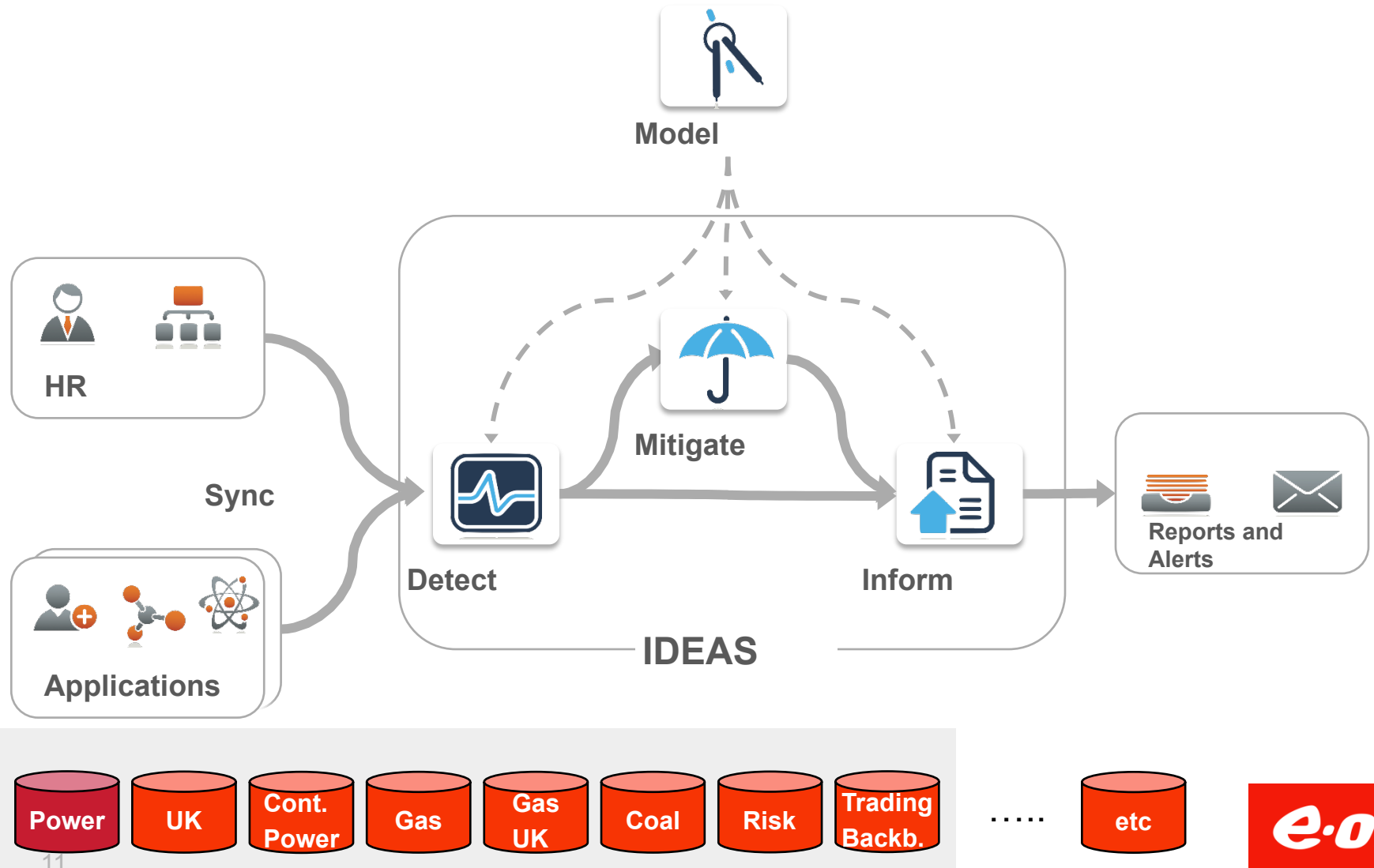
The Software Partner

- The **CrossIdeas** Identity & Access Governance platform (IDEAS) was selected
- Why did EGC choose CrossIdeas? The logo for CrossIdeas features a stylized 'C' composed of green and blue squares, followed by the word 'CrossIdeas' in a blue and green sans-serif font.
- Risk/SoD modelling paradigm: 1to1 fit with Auditor requirements
- Proximity
- Consultative approach rather than product sale

Project roadmap (high level)

- **Phase 1 (june-Dec 2012): ‘Understand the risk’**
 - Detective approach, no changes to existing user provisioning processes
 - Implementation of User and SoD controls on 8 top critical applications
- **Phase 2 (2013): ‘Reduce the risk’**
 - Onboarding of additional applications (including Ruhrgas)
 - Access Certification
- **Phase 3 (2014+): ‘Avoid the risk’**
 - Implementation of more mature SoD controls
 - Streamline access request management

Logical architecture



Benefits

EGC is now in control

- **One single view on ‘who could do what’**
- **Real-time detection of several types of access risks:**
 - On User: SoD, Sensitive Access, orphan/service accounts;
 - On Application Roles: intrinsic SoD violation.
- **Ability to immediately react** by appropriate counter-measures such as periodical review processes, revoking accounts, etc.

‘Audit Ready, M&A Ready’

Lessons learned

Challenges ahead

