



Sven Pauwels

An integrated approach for Identity and Access Management projects

Limitations and approach to implementations

Nicolas Delcroix



Agenda



- Introduction IS4U
- Introduction DelITad
- Definition IAM
- Problem Definition
- Proposed approach
- Conclusion
- Partnership IS4U/DelITad



Introduction IS4U



- IS4U is an IAM & Compliance competence center
- Profiles
 - Architect
 - Analyst
 - Integrator
 - Project manager
- CISSP, CEH, product certifications
- Member of OASIS and the IDTrust Member Section.



21/11/2008

3



Introduction IS4U



Expertise: IAM, SIEM, BeID, Stong Auth, Penetration testing, R&D

Activities: Advise and evaluate, Implement, R&D, OASIS, Consulting and projects

Partners: SUN, IBM, CA, Oracle, Evidian, Microsoft, PassLogix, PingIdentity, Provisio, DelITad, E-Trinity



21/11/2008

4



Introduction DelITad



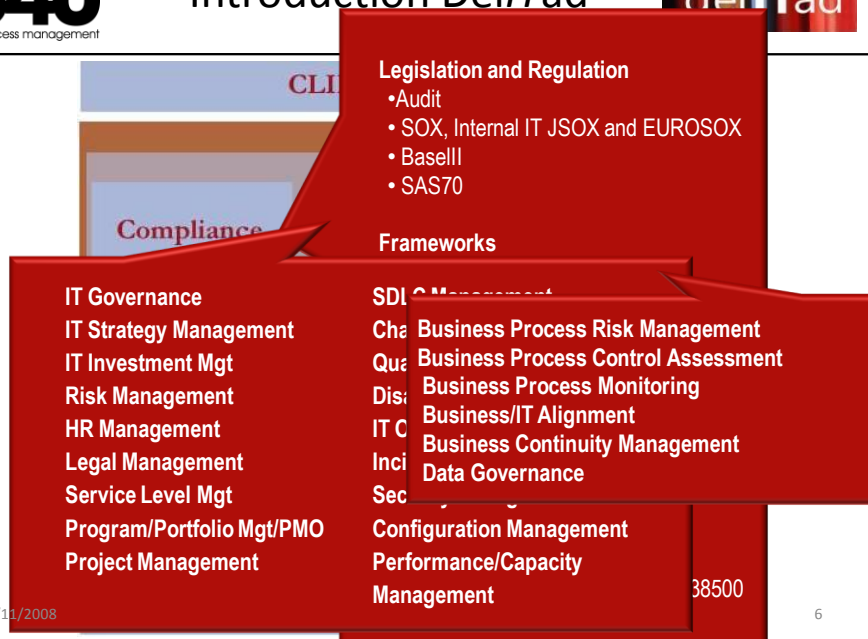
- DellTad – Delivering IT Advisory – is expert firm in IT Audit and IT Governance
- Link between business and IT
- Customer focused
- Process oriented
- We consider **Quality** as crucial for our clients' confidence and the continuity of our business. Therefore, we put quality at stake by providing **competent** and **certified** consultants, clear deliverables and active transition of knowledge between more senior and more junior consultants.

21/11/2008

5



Introduction DelITad



21/11/2008

6

‘Identity and Access Management: is a concept that combines business processes, policies and technologies that enable companies to:

- Provide secure access to any resource.
 - Efficiently control this access.
- Respond faster to changing relationships.
- Protect confidential information from unauthorized users.’
(Wikipedia)

•‘Identity and access management refers to the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources.’
(Microsoft)

21/11/2008

7

‘Identity and Access Management (IAM) is an administrative process coupled with a technological solution which validates the identity of individuals and allows owners of data, applications, and systems to either maintain centrally or distribute responsibility for granting access to their respective resources to anyone participating within the IAM framework.’
(NYS Forum)

Identity management is the set of business processes, and a supporting infrastructure for the creation, maintenance, and use of digital identities.”
(The Burton Group)

21/11/2008

8



Our Definition of IAM



‘Identity and Access management is the set of business processes, policies, procedures and the supporting technology that enable an organization to successfully govern and distribute information and business rules in compliance with relevant legislative and regulatory requirements’
(IS4U and DelITad)

21/11/2008

9



Problem Definition



- Focus on technology instead of business
 - Project supported by IT to solve IT problems
 - ➔ what happens when project touches business ?
 - Project initiated by IT
 - ➔ what happens when input from business is needed ?
 - Project initiated by technology available
 - ➔ will the technology solve the problem ?
 - ➔ are we choosing the right vendor ?

21/11/2008

10

- Unrealistic budgets/approach
 - Start with full-blown project scope
 - ➔ huge price tag
 - ➔ close to impossible to manage the project
 - Start with low-hanging fruit
 - ➔ solves visibility... But...
 - ➔ How do we convince the sponsor to go on ?
 - Start with drafting the complete future architecture
 - ➔ Timeframe ?
 - ➔ What can we show project sponsor at the end ?
 - ➔ Can we justify the budget

21/11/2008

11

- Resistance to change
 - People not involved in all stages of project
 - ➔ why do we need this
 - ➔ why do WE need to change for something YOU implemented
 - ➔ this is not the time to initiate changes...
 - Scope did not include business
 - ➔ input needed for implementation is not available
 - ➔ the technological solution is ready, business isn't
 - ➔ once business is involved... Rethink the solution

21/11/2008

12

- Solution not solving the problem at hand
 - problem was not clear to start with
 - ➔ Was there a problem or was it just a nice to have ?
 - root cause analysis not done
 - ➔ Treat the symptoms iso the disease
 - ➔ Investment delivers successful implementation of the technology... The problem still remains... Is this a success ?
 - the problem we thought we had changed during the project...
 - ➔ was it correctly identified ?

21/11/2008

➔ were all problems to be tackled identified ?

13

- Limited management buy-in
 - Not enough results to show
 - ➔ Management loses confidence
 - ➔ Too much presure to implement partial solutions...
 - Limited buy-in at the start
 - ➔ Unclear why we need this solution
 - ➔ Unclear who should participate

21/11/2008

14

- Lack of business change management
 - no involvement of lower management or people in the field
 - all new processes are defined and drafted in the new technology... But nobody is aware
 - lack of guidance in changing

21/11/2008

15

Root-cause analysis shows us:

- Flavor of the day
 - ➔ Do we need this or is this nice to have ?
 - ➔ So many products... What to choose ? (Fear of making the wrong decision can cause serious delays)
 - ➔ Environments change... Does the technology follow ?
- Scope creep
 - ➔ If we can do this... Then we can also...
 - ➔ Problem changes/grows during project (or did the problem just become more clear ?)
 - ➔ People involved in later stages will point out new needs

21/11/2008

16

Root-cause analysis shows us:

- Lack of streamlined communication
 - ➔ communication keeps information alive and up to date
 - ➔ getting everybody involved helps identifying all problems and needs
 - ➔ communication creates awareness and willingness to participate
 - ➔ communication saves money...

In other words: Better Business/IT Alignment in IAM projects

21/11/2008

17

Proposed approach
Thre Hourglass model



Start

1. Project Kick-off

Problem description

2. High level security governance assessment

3. Root Cause Analysis

4. AS-IS security implementation & Business process analysis

Solution description

5. Solution selection & Implementation plan

Implementation

6. Technical implementation

7. Business & IT Process implementation

Handover

8. Awareness & Business and IT training

21/11/2008

18

Start

- Step 1: Project Kick-Off
 - indispensable...scoping, planning, cooperating

Problem description

- Step 2: High-level security governance assessment
 - security policies, security organization, security process documentation, monitoring,...

- Step 3: Root Cause Analysis
 - What are the real problems we need to solve ?

21/11/2008

19



Problem description

- Step 4: As-is security implementation & business process analysis
 - test current security policies, organization, monitoring,...
 - describe current business processes
 - describe the AS-IS situation

Steps 2 to 4 give the needed pre-requisites for the following steps

21/11/2008

20



Solution description

- Step 5: Solution selection & Implementation plan
 - determine TO BE situation
 - choose the solutions to fill the GAPS
 - BPR/ ITPR
 - technology
 - Both go hand in hand...
 - create an implementation plan
 - for the technology
 - for the business and IT processes



21/11/2008

Implementation

- Step 6: Technical Implementation
 - implement the choosen technology according the newly defined processes
- Step 7: Business & IT process implementation
 - get the newly defined processes in place



21/11/2008

22

Handover

- Step Awareness & Business and IT training
 - train administrators in maintaining the technology
 - train the users in using the technology
 - explain the new processes put in place and how the technology supports them
 - explain why the new processes are needed and how they help improving the business

QA & PM

Overall QA and PM ensure results in time of proper quality and within budget.

21/11/2008

23

This approach is promoted for our new clients...

An example where the approach is introduced after the facts...

- project started with limited scope and limited communication
- driven by product choice
- implementation started based on the information in the RFP

During the first weeks of the project several issues were raised

During architecture definition it became clear that:

- scope needed to change
- not everyone was aware of the project and the consequences on processes
- not all processes were well defined
- communication was a real problem

21/11/2008

24

Introducing our methodology allowed us to:

- start over
 - get all the right people involved
 - help in defining the scope and the problems at hand
 - help in defining the processes needed
- product choice was already done, in this case this was not a problem
- Extra cost:
 - part of the initial effort in defining the architecture was lost
 - extra effort needed to re-promote the project after the first go.

21/11/2008

25

8 steps are our proposed secret to IAM Success.

- Improve communication
 - Internally in organization
 - over time during different steps
 - different people responsible for different steps (internal or ext)
- Streamlining communication and different steps is key
- A joint offering as proposed by IS4U and DelITad is a way of guarantying this streamlining and communication
 - all steps to come are known up front
 - results are streamlined over different steps
 - All layers in the organization are involved at all times
 - Overall QA and PM guard quality and informationstreams
 - Every step is performed by or enabled by experts

21/11/2008

But of course there is no such thing as a silver bullet!!

26



Partnership IS4U/DelITad



IS4U

- IAM Expertise
- Vendor Independent
- Technical implementation

DelITad

- IT Governance Expertise
- IT Auditing
- Business Implementation

=> End-to-End independent expertise capable of delivering the methodology as described before.

21/11/2008

27

The cover of the 'Questions & Answers' document. It features a black and light blue diagonal split. The top left corner has the IS4U logo and the name 'Sven Pauwels'. The center has the title 'Questions & Answers' in large white text. The bottom right corner has the name 'Nicolas Delcroix'. The bottom edge features a red and blue striped pattern with the delITad logo in white.

IS4U
Identity & access management

Sven Pauwels

Questions & Answers

Nicolas Delcroix

delITad