Business case for secure service engineering

Aljosa Pasic

Vienna 08/04/2014

Atos

NIS platform deliverable “Business Cases and Innovation Paths”

- Introduction and problem definition
- Methodology for the study
- Business cases
  - Initial sample market and industry analysis
  - Identification of stakeholder requirements
  - Selection and analysis of high impact use cases
  - Cost-benefit analysis of research topics in relation to use cases
  - Initial economic incentive analysis
- Process Definition & Innovation Models
  - Survey of best practices in innovation
  - Technology and research analysis link with ‘Secure ICT landscape’ deliverable
  - Recommendations to H2020 on innovation processes
- Summary of recommendations

Methodology for demand-driven research

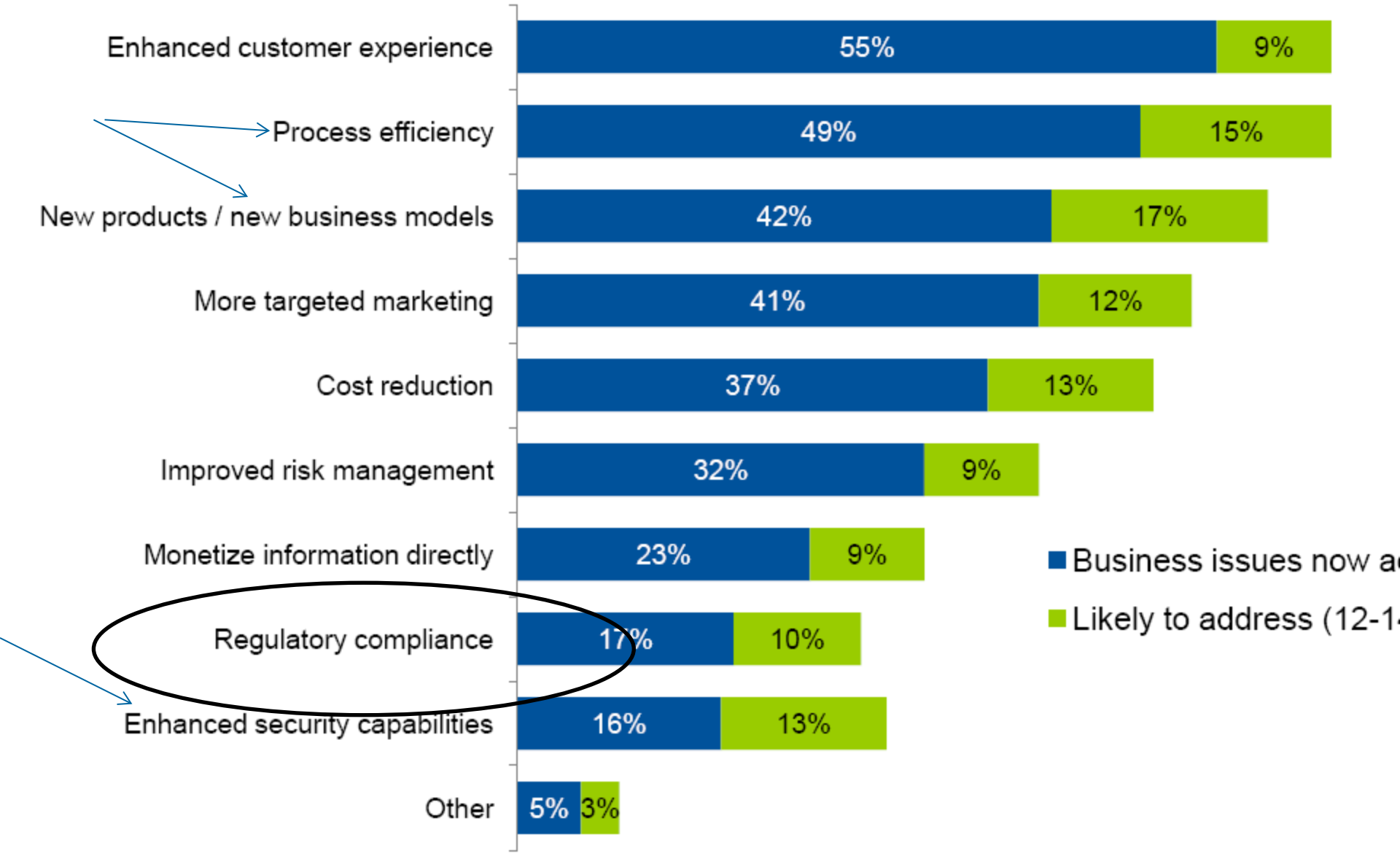
- Define a model and an approach
- Identify stakeholders
  - Describe concerns from their viewpoints
  - Impact of not meeting xxx requirement
- Identify E2E business processes in which XXX plays role
  - Identify steps where security is critical and describe challenges
- Derive set of research topics from above plus external info (SRA etc)
  - Analyse them from the viewpoints: investment, impact, likelihood of success, route to market, dependencies (e.g. on regulation)
- Go back and repeat this process ??

1. Market Initial Segmentation

1. Global demand model with security sub segmentations
   a) Defence and national security
   b) Government and other public sector
      i. Strong requirements, e.g. tax collection
      ii. Low impact/requirements, e.g. local school
   c) Corporate
      i. Strong needs/requirements (e.g. sector regulations) e.g. finance
      ii. Medium
   d) SMEs
   e) Citizens
2. Security topic specific demand model
   1. End user: in-house, outsourced, in cloud
   2. Software company: tailor made, product, components
   3. Existence of S-SDL? Existence of service based software?

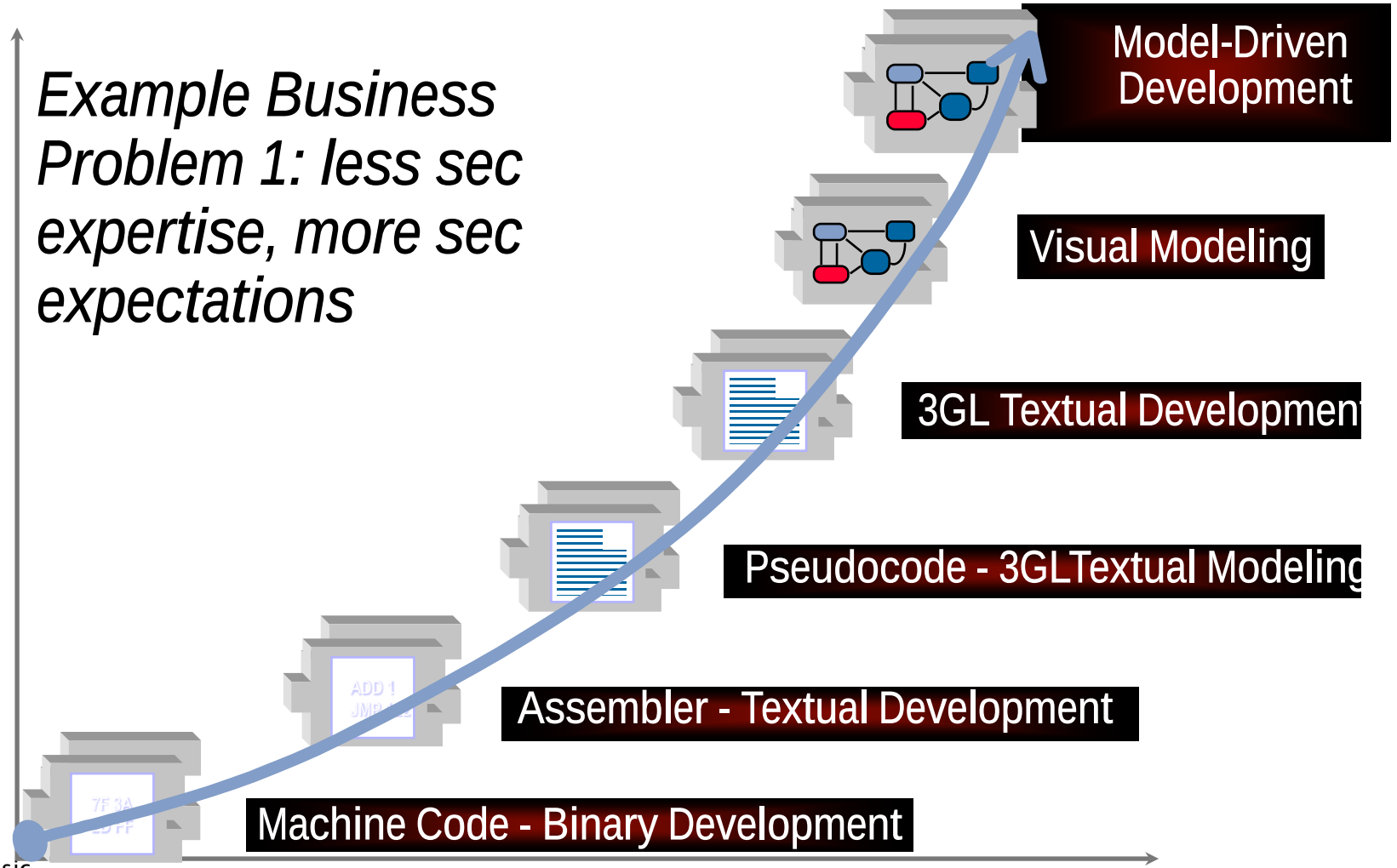
3. **Now calculate market size: 1+ c + ii + service based = ???**

Business problems companies are addres

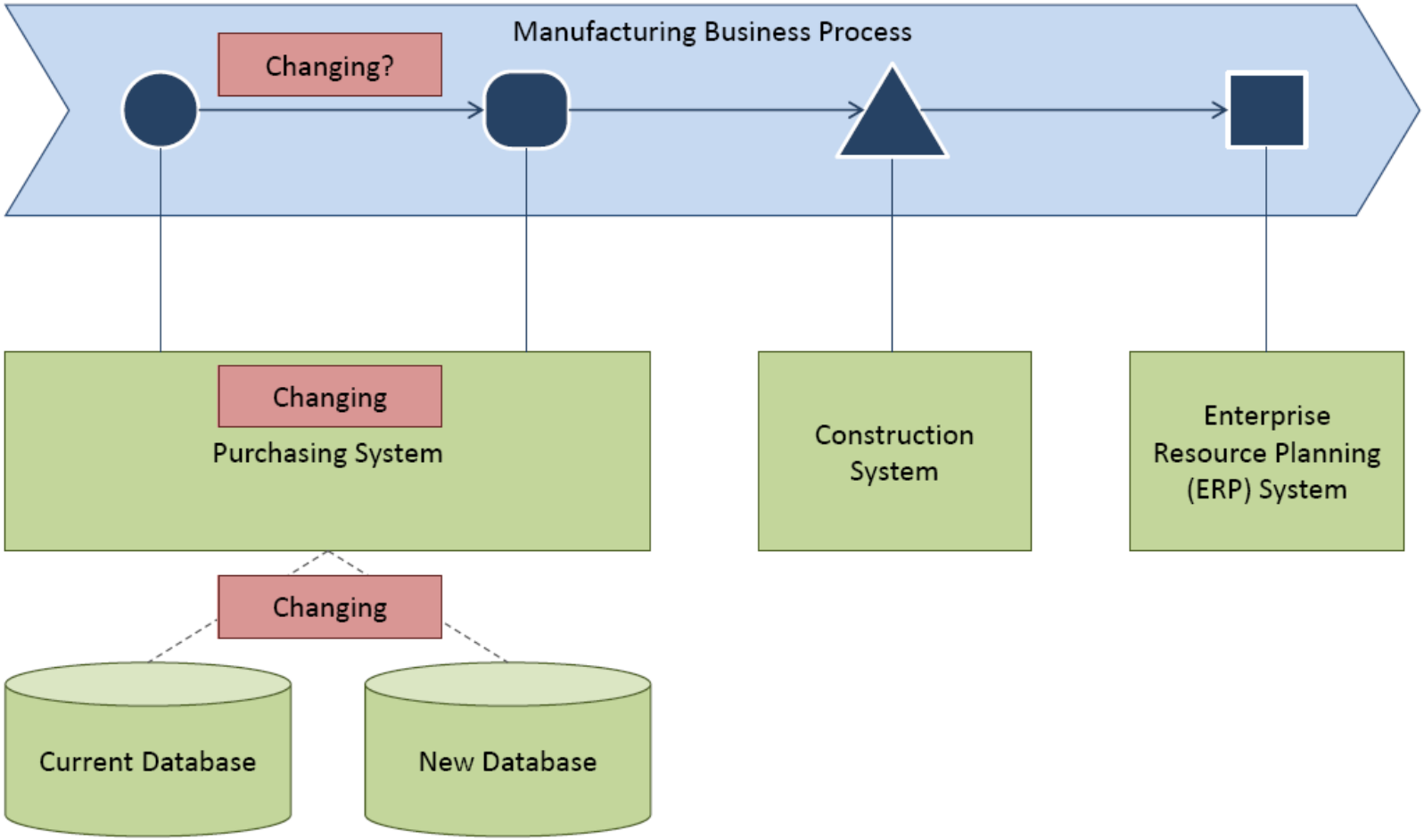


"Survey Analysis: Big Data Adoption in 2013 Shows

Example Business Problem 1: less sec expertise, more sec expectations



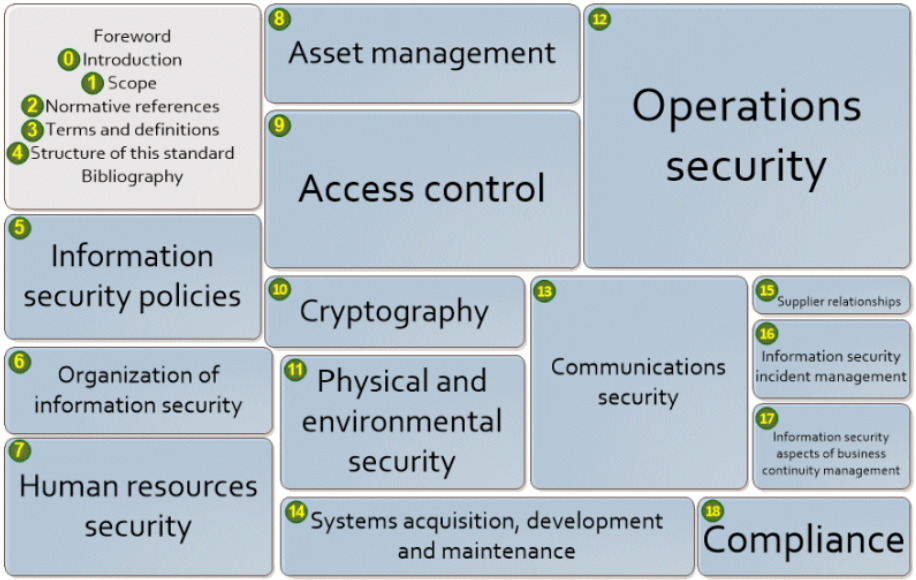
Example Business Problem 2: Change propagation in SOA



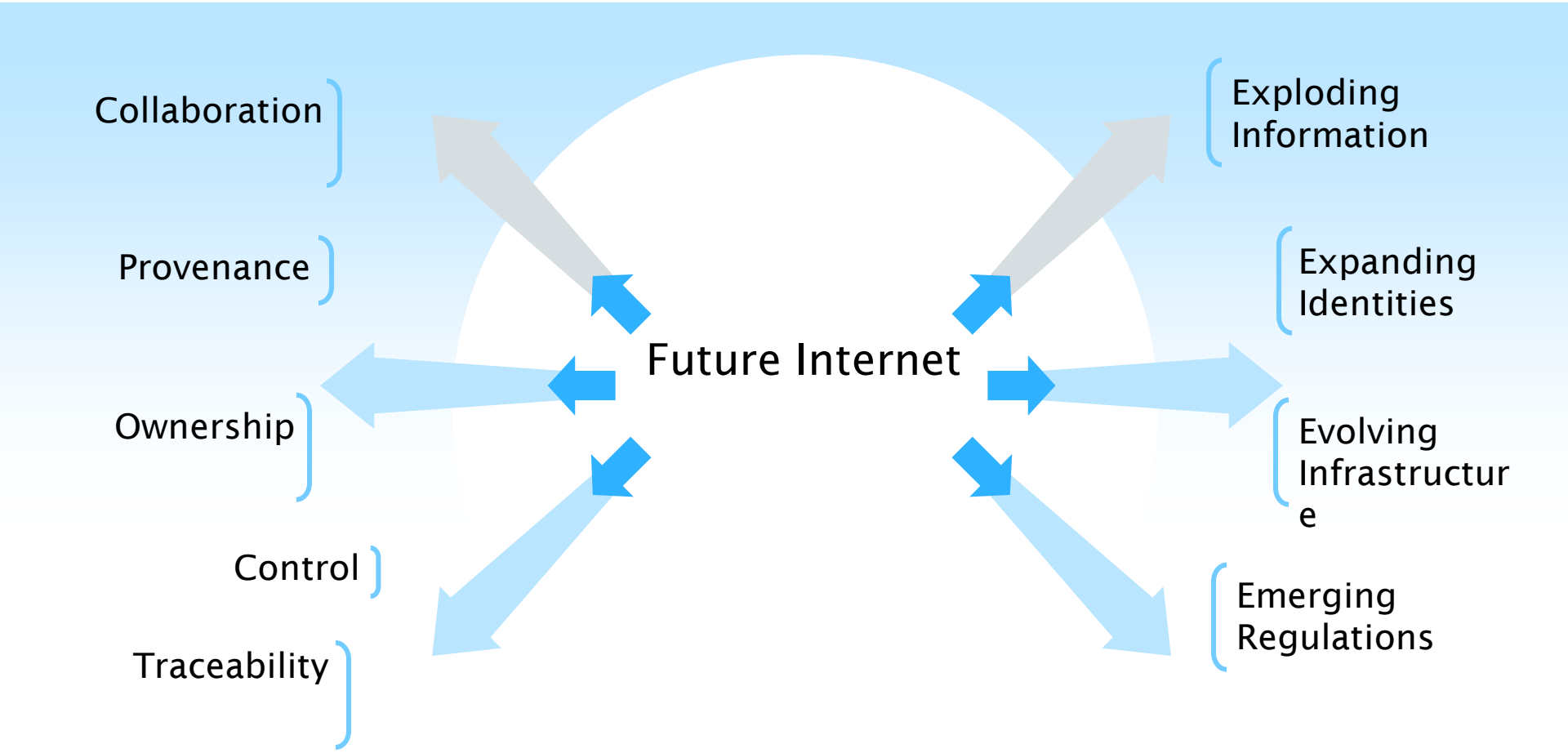
2. Business Problem Refinement

- START from an existing DEMAND, such as e.g. **obligatory compliance** and build USE CASE
- ISO 27002 Section 14: System acquisition, development and maintenance
  - Security requirements of information systems
  - Security in development and support processes
  - Test data
- Additional business goals for USE CASE e.g.
  - Time : agile instead of waterfall SDL
  - Flexibility, interoperability: move to service-based software system
- Additional challenges/risks related to the USE CASE:
  - Evolution, dynamicity etc
- Additional (existing) considerations/ constraints
  - Cost
  - Additional frameworks, etc

Cloud Controls Matrix CCM3.0 domain
AIS -01:
Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance



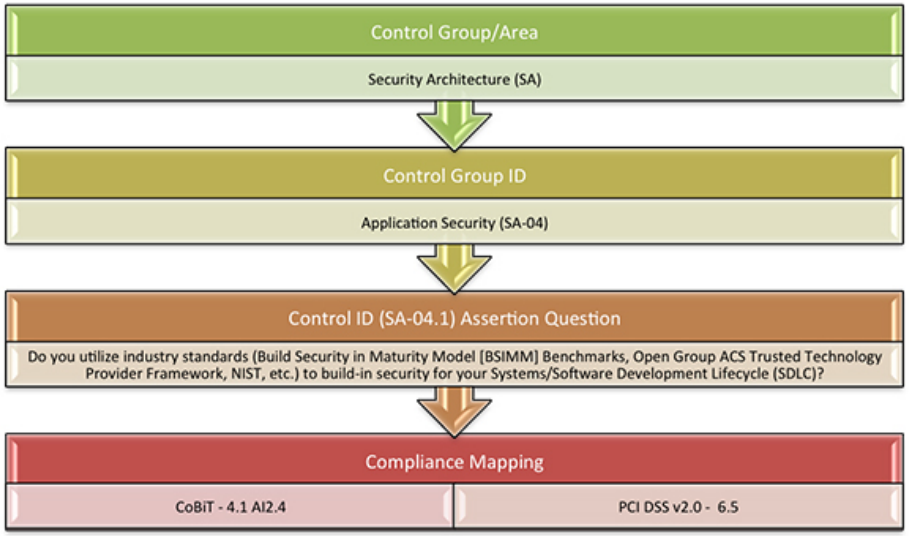
Pick Up Your Future Internet Challenge

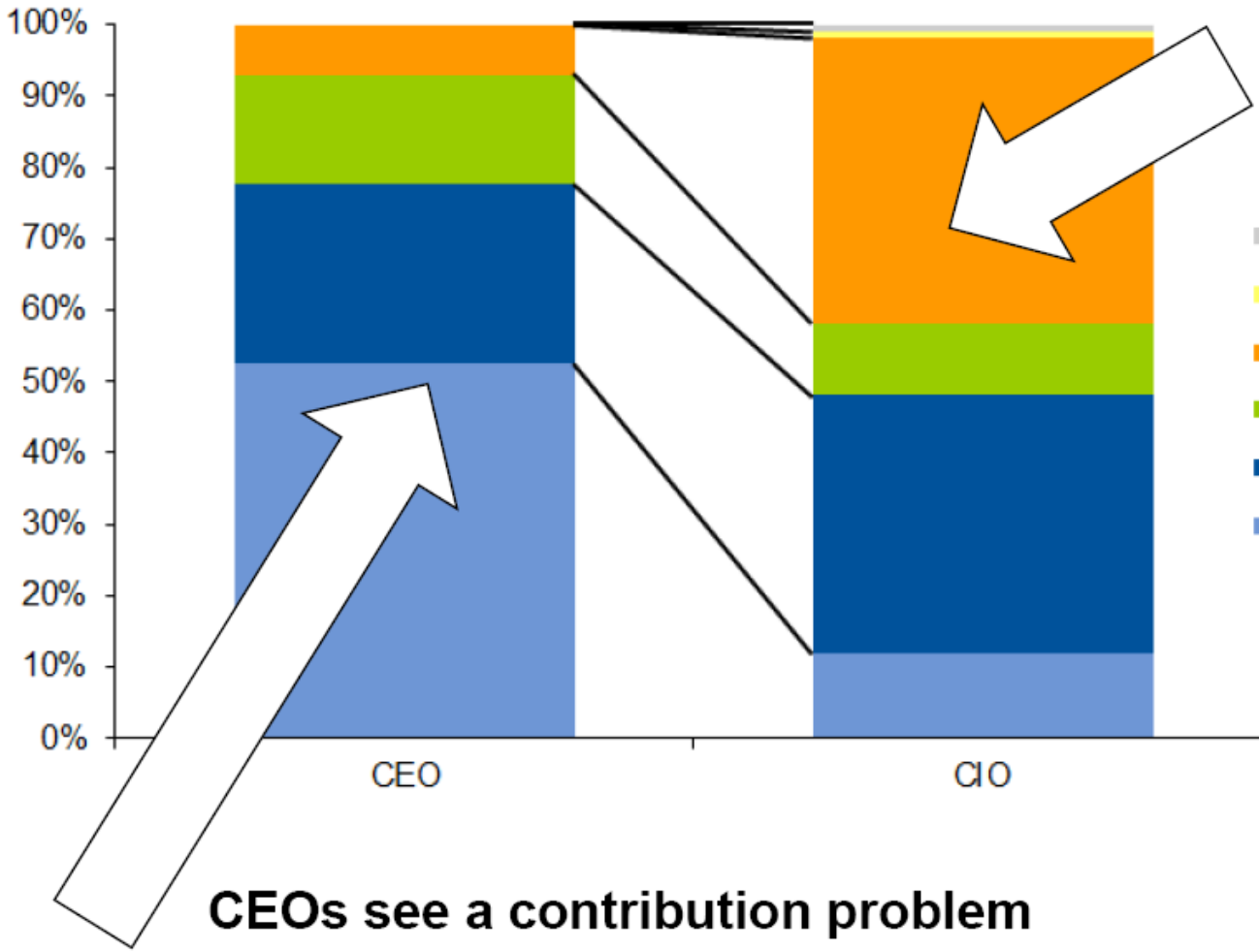


3. Building your business case, parallel to user use case

- CEO : Why should I care?
  CIO (copy+paste) : All companies that accept, store, process or transmit credit card information are each required to report compliance with the Data Security Standard (DSS).
  CISO : How about ISO 27001? It maps into many compliance schemes.
- CEO : OK, I can give you 1 M, but I want to know how do you spend it
  CIO : we will put 40% for implementation, 20% for auditing, etc
  CISO : I will make an estimation for each control/domain

- 35 control objectives, 114 +++ controls in ISO27002:2013, 16 domains 136 controls in CCM v3





CIOs see a communication problem

CEOs see a contribution problem

"What challenges do you believe the Chief Information Officer (or IT Director) must address in order to expand their contribution and importance as a C-level executive?"

4. Impact Assessment (of doing-it or not)

- Software vulnerabilities cost US economy 59 Billion (0,6% of the GDP) (Source: NIST, 2002)
- ROI data for secure sof software inexistent
- Direct monetary value f through secure softwar
- Indirect value: Microso reputation and business grew after SDL introduction
- Compliance cost reduction : e.g. SDL threat analysis helps in the implementation + monitoring of the other steps/controls (complying with FISMA costs 2,3 Billion of which 1 billion is for audit, source :SANS)

Metric	Windows Vista (year 1)	Windows XP (year 1)
Vulnerabilities fixed	36	65
Security updates	17	30
Patch events	9	26
Weeks with at least 1 patch event	9	25

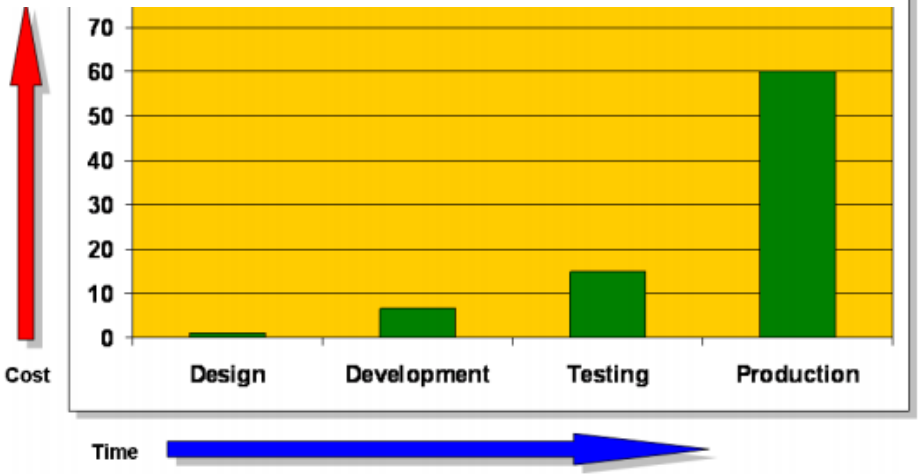


Figure 3: The cost of security

5. Identify processes, challenges and value proposition

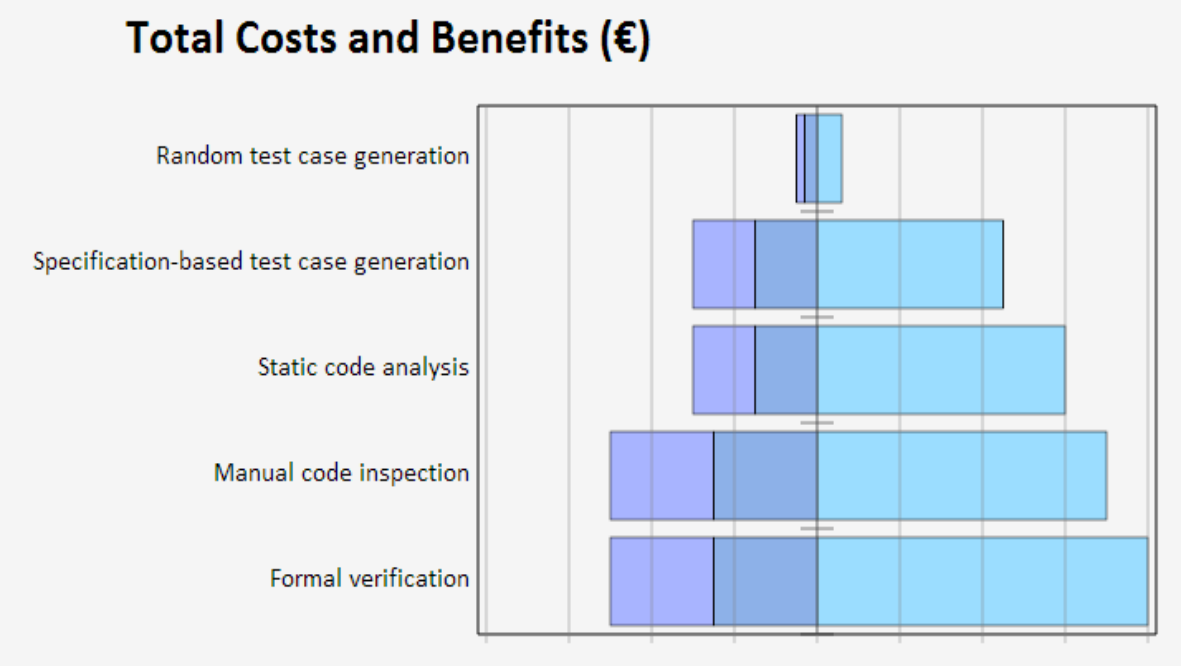
- Go to step 1 and customize your value proposition for the target customer
- You satisfy compliance requirement (start point, business related requirement)

- You save more money by preventing vulnerabilities than by detecting them (direct gain)
- The early assurance is more cost-effective than late assurance (direct gain)
- This is the best practise for secure service-based SDL (reputation, indirect gain)
- You can build-in continuous monitoring "probes" (and save €€€ on audits, indirect gain)
- You can move towards the near real time (integrated) risk management (indirect gain)
- You can address software evolution/adaptation through MDS and policy automation (indirect gain)
- You can avoid errors and save cost through requirements transformation

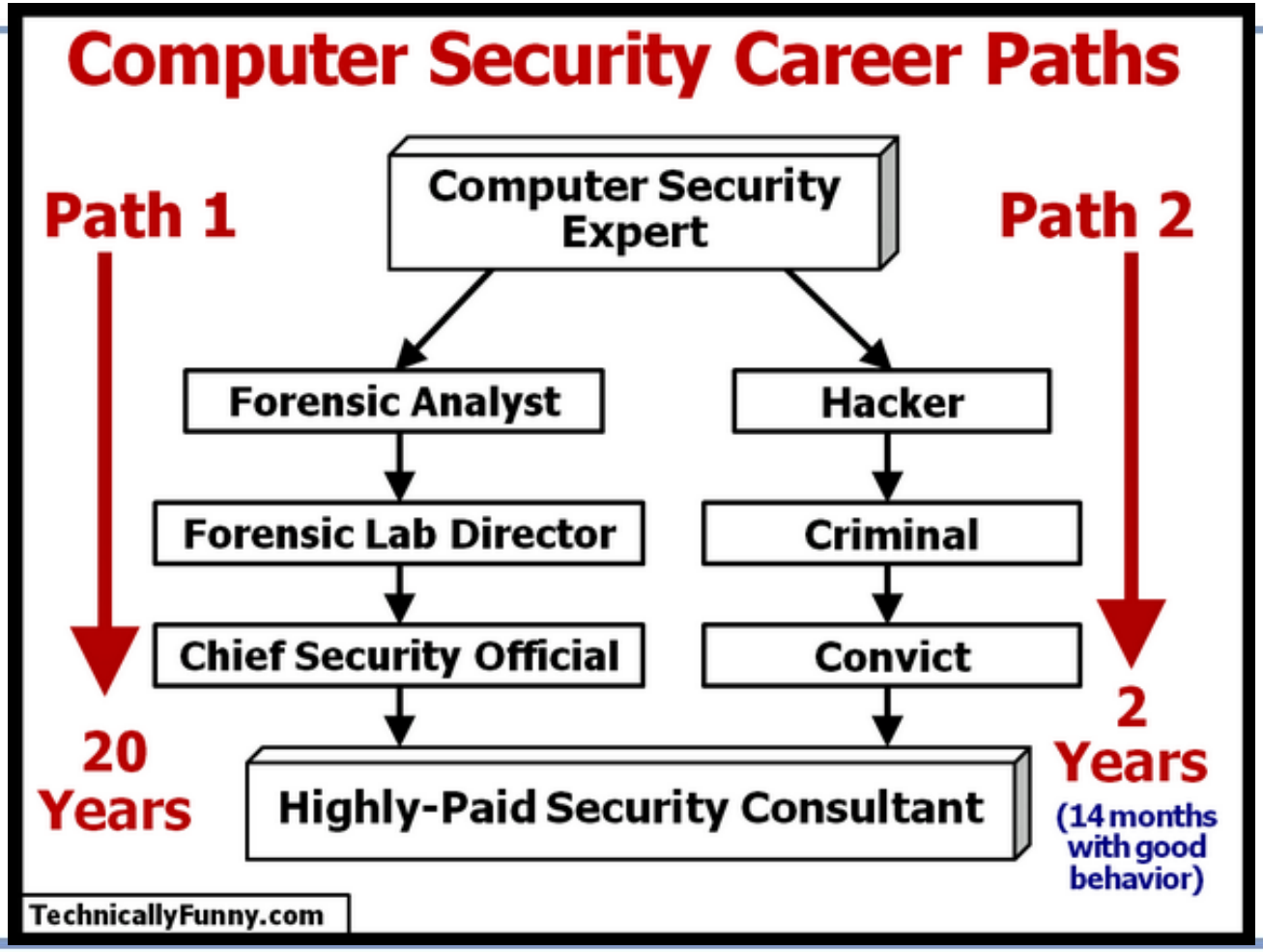
6. Identity research topics

- Integration of early and late assurance
- Risk driven development
- Socio technical multi stakeholder requirements elicitation…

- Prioritisation according to:
  - investment, impact, likelihood of success, route to market, dependencies (e.g. on regulation
  - NESSoS SecEval +CBK , OWASP CIO Guide



That is all !!!


Computer Security Career Paths
Path 1
Computer Security Expert
Path 2
Forensic Analyst
Hacker
Forensic Lab Director
Criminal
Chief Security Official
Convict
20 Years
Highly-Paid Security Consultant
2 Years
(14 months with good behavior)
TechnicallyFunny.com

Thanks

For more information please contact:
T+ 34 91214 8800
M+ 34 675 639383
Aljosa.Pasic@atos.net

Atos (Spain)
Albarracín 25
E-28037 Madrid

www.atos.net