

ORACLE®

Adam O'Brien
Evaluation Analyst
Oracle Corporation

ORACLE

How Much !!!

The cost impact of different approaches to generating evidence.

Overview

- How to produce the evidence?
- Who produces the evidence?
- A naive conclusion.
- Second thoughts.
- A final conclusion.

How to Produce Evidence?

- When?
- What?
- Who? – the most interesting question because it feeds into the fundamental question of why we do CC evaluations.

These questions aren't independent.

Who produces the evidence

Externally

— By External Consultants

— By an Internal CC team

— By the Developers

Internall

y

ORACLE

External Consultants

Benefits

- CC Expertise
- Easily Parallelisable
- No fixed costs / HR overheads

Weaknesses

- Start with little product knowledge
- Little Retention of IP

Internal Team

Benefits

- CC Expertise
- Organisational Knowledge
- IP Retained within the Organisation

Weaknesses

- Hard to Recruit

Development

Benefits

- Product and Process Expertise
- IP Retained within Development

Weaknesses

- Opportunity Cost

CC Intellectual Property

- The SFRs in the ST
- The SPM
- The Design Documents
- Process Documents
 - Vulnerability Handling
 - Configuration Management
 - Delivery
 - Development Security

Comparing the Approaches

	External	Internal CC	Development
External Costs	High	Low	Low
Dev. Resources	2 months	2 months	12 months
CC Resources	6 months	18 months	6 months
Elapsed Time	12 months	15 months	15 months
Other Benefits	Small impact on development	Retention of IP	Retention of IP, Less Duplication

ORACLE

My Naive Conclusion

Development should create all the documents.

- The process should be easy (or informative!).
- More efficient.
- The CC documents could be used in future development work.

Problems

CC is an **Evaluation** Methodology

- It contains good processes a development organisation might want to use ...
- but it contains lots of other things.
- Forcing development to carry out all the CC activities, many of which are assurance based isn't efficient.

The Cost Of Development Time

If development produce documentation which covers all CC requirements ...

... and this adds 5 minutes work per day ...

... and you employ 10,000 developers ...

That implies very expensive evaluations

= 104 full time equivalent developers

ORACLE

A Hybrid Approach

Each to their own:

- CC specific documents – external consultant
- Design Documents – input from development, finalised by an internal technical writer
- Installation Guide and Vulnerability Analysis – internal consultant (+ technical writer)
- Process Documents – internal project manager (+ technical writer)

ORACLE

The Benefits

- Efficiency – each document is produced by a specialist.
- IP is retained in the right place.
- The documents will be more ‘accurate’.

The Difficulties

- Complex project management ...
- ... compounded by tension over timing.
- HR issues.
- The elapsed time for an evaluation may be longer.

Conclusions

‘A good development team would produce CC evidence automatically.’

This is, inevitably, a myth.

We the hybrid approach works because it:

- Makes use of existing knowledge.
- Minimises impact on development.
- Feeds the **right** IP back to development.



QUESTIONS
&
ANSWERS

ORACLE