IBM Systems and Technology Group

Managing Multiple and Emerging Standards

William Penny
2455 South Road
Poughkeepsie, NY, USA 12603
IBM Corporation
wpenny@us.ibm.com
845-435-3010

Agenda

- Research/Standards/Requirements
- Product Development
- Customer Deployment
- What to do?

Objective

Customers are interested in **assurance** that the products that they use can be operated in a secure manner.

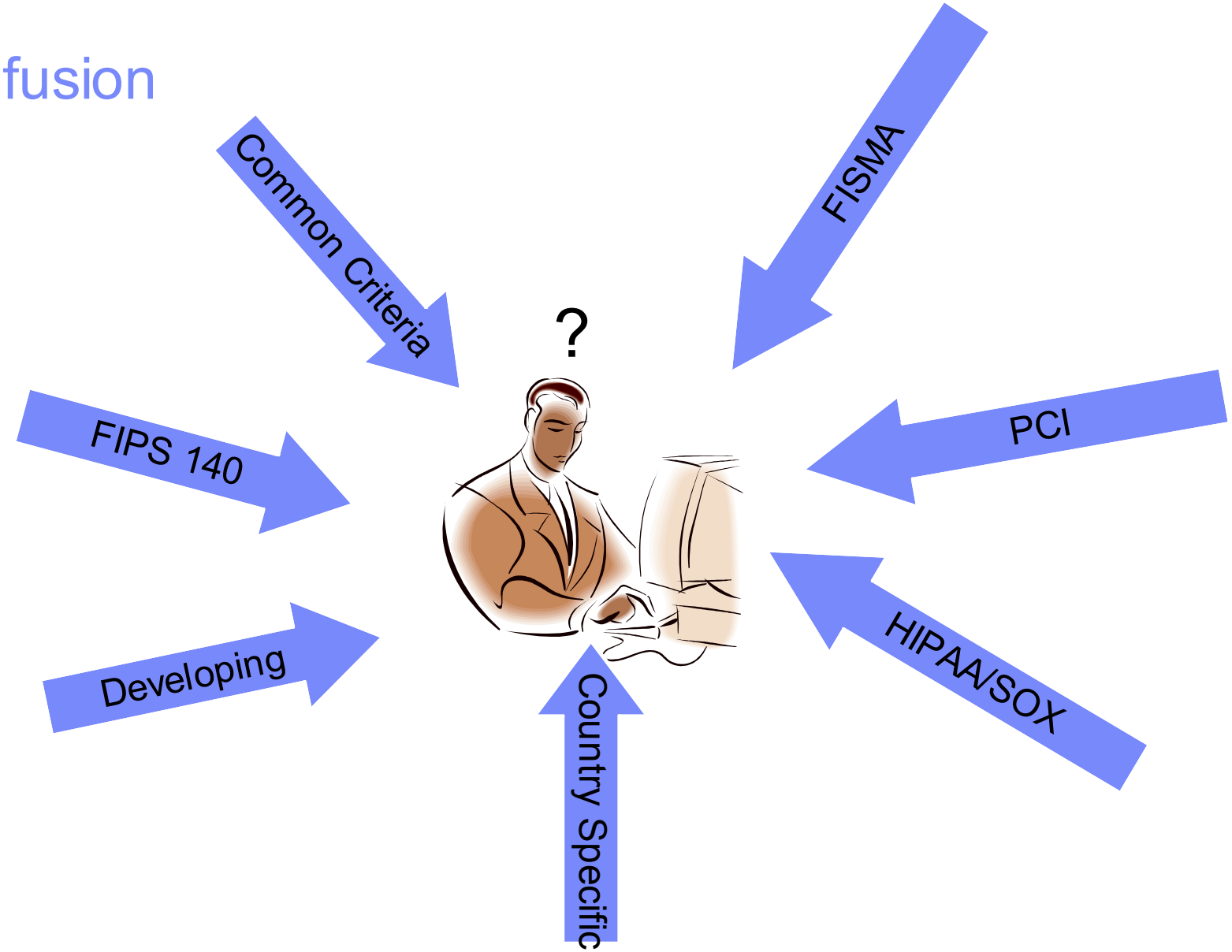
Security Research

- Systems and Network Security (NIST)
  - http://csrc.nist.gov/groups/SNS/index.html
- Center for Information Systems Security Studies and Research
  - http://cisr.nps.navy.mil/

Standards

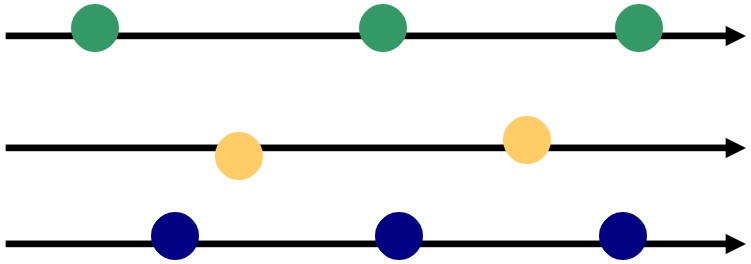
- Common Criteria
  - Multiple protection profiles
- ISO 27001
- CMVP (FIPS 140-2)
- PCI
- US Government
  - FISMA
  - HIPAA
- Other national standards

Confusion

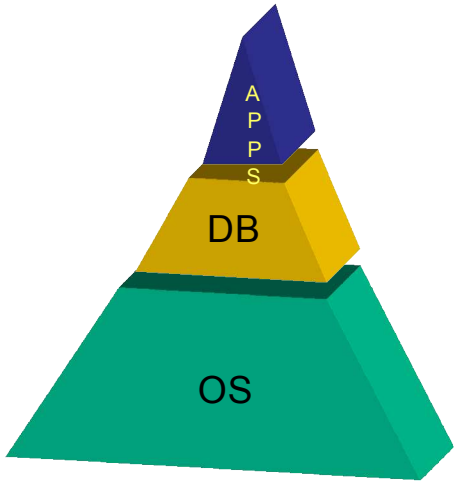


Development Plans – Multiple Releases

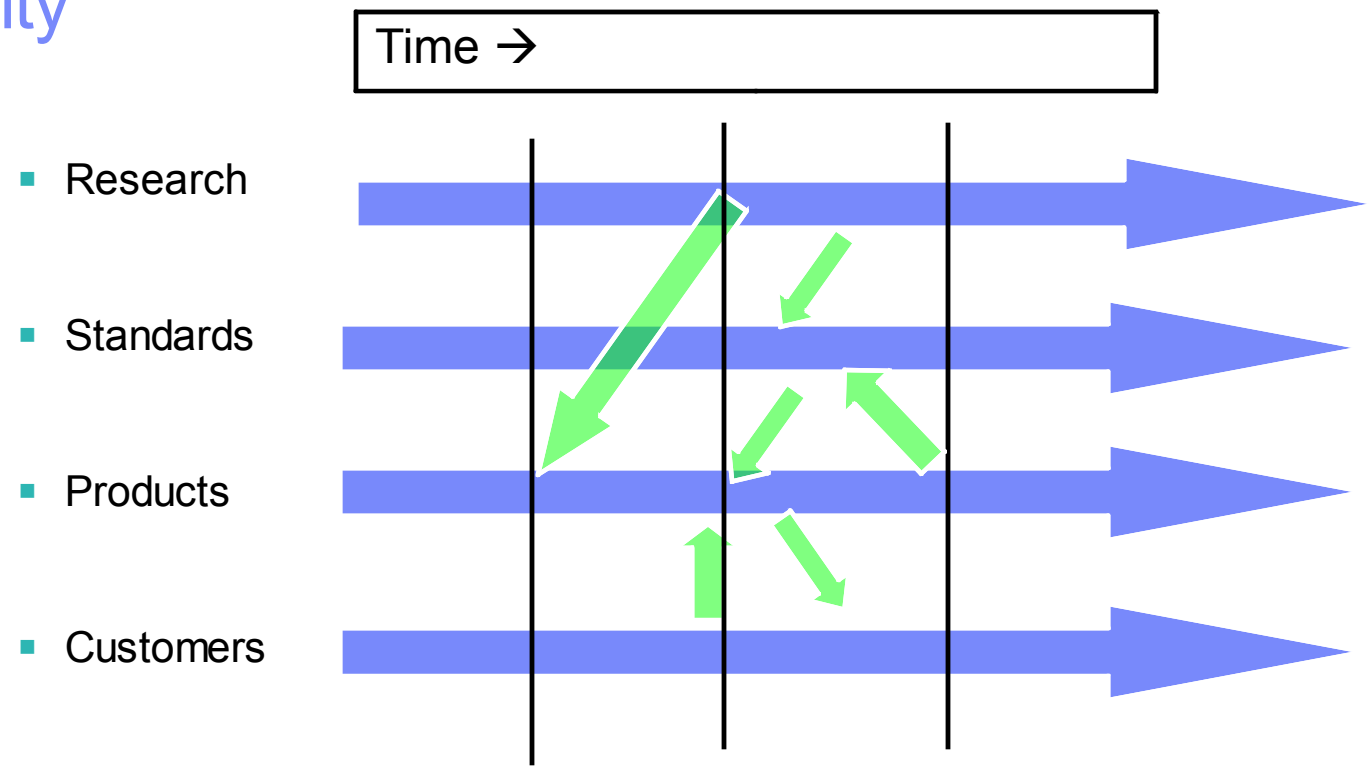
- Operating Systems
  - Release 1, Release 2, Release 3
- Databases
  - Release 1 , Release 2
- Applications
  - Release 1, Release 2, Release 3



Composition not yet practical !

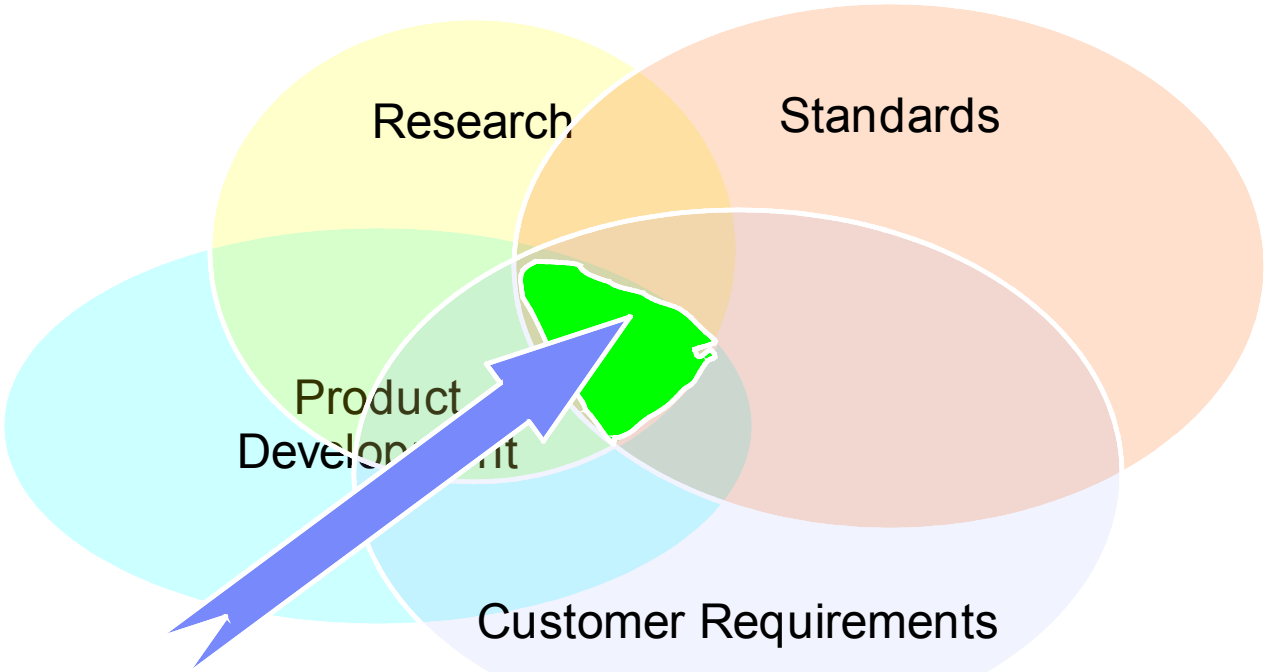


Velocity



- All of these are moving forward and changing.
- Developers react to research, standards and customer requirements
- Customer deploy based on law, standards and threats (perceived and real)

The Sweet Spot



The 'Sweet Spot' – Everything Aligns

And this is a moving target!

Development

- Waterfall or Agile or other
  - Expects requirements to drive development
  - This is not practical or possible in this arena
- Can we anticipate standards?
  - Requires expense, engagement, expertise
- Can we anticipate customer requirements?
  - Requires expense, engagement, expertise, but…
  - Different from the standards work

Customer Deployment

- Lags Product Development (well… of course!)
- Potentially long deployment time – even after a decision is made
- Current customer usage sometimes lags research and standards by years

Challenges

- Multiple Standards cost
  - Money
  - Time
  - Confusion
- Emerging Standards cost
  - Money
  - Product Delays
  - Confusion

What to do???

Response in Development (not a solution)

- Engage in Research/Standards/Customer Business Models
  - Understand each area
  - Influence directions of standards and products
  - Reach common understanding and goals
- Products
  - Must plot minimum acceptable path
  - Very difficult to do

Challenge for the CC

- **Provide a pro-active involvement to focus research and standards bodies into a convergent set of adaptable standards and guidelines**
- **Provide a roadmap for standards development that allows product developers and customers to plan**

Suggestion – a New model

- Look beyond Product Evaluation
  - Too costly and difficult to do right
- Consider a ‘Process Evaluation’ or ‘Assurance’
  - Model after manufacturing
  - Control limits
  - Not every piece Is tested
- Educate
  - Understand that no software product is defect free
  - Security standards do not guarantee security

Thank You!

Questions?