Stop doing grunt work

Key to efficiently executing multiple certification efforts

Ashit Vora, ICMC 2017

Acumen Security

About Me

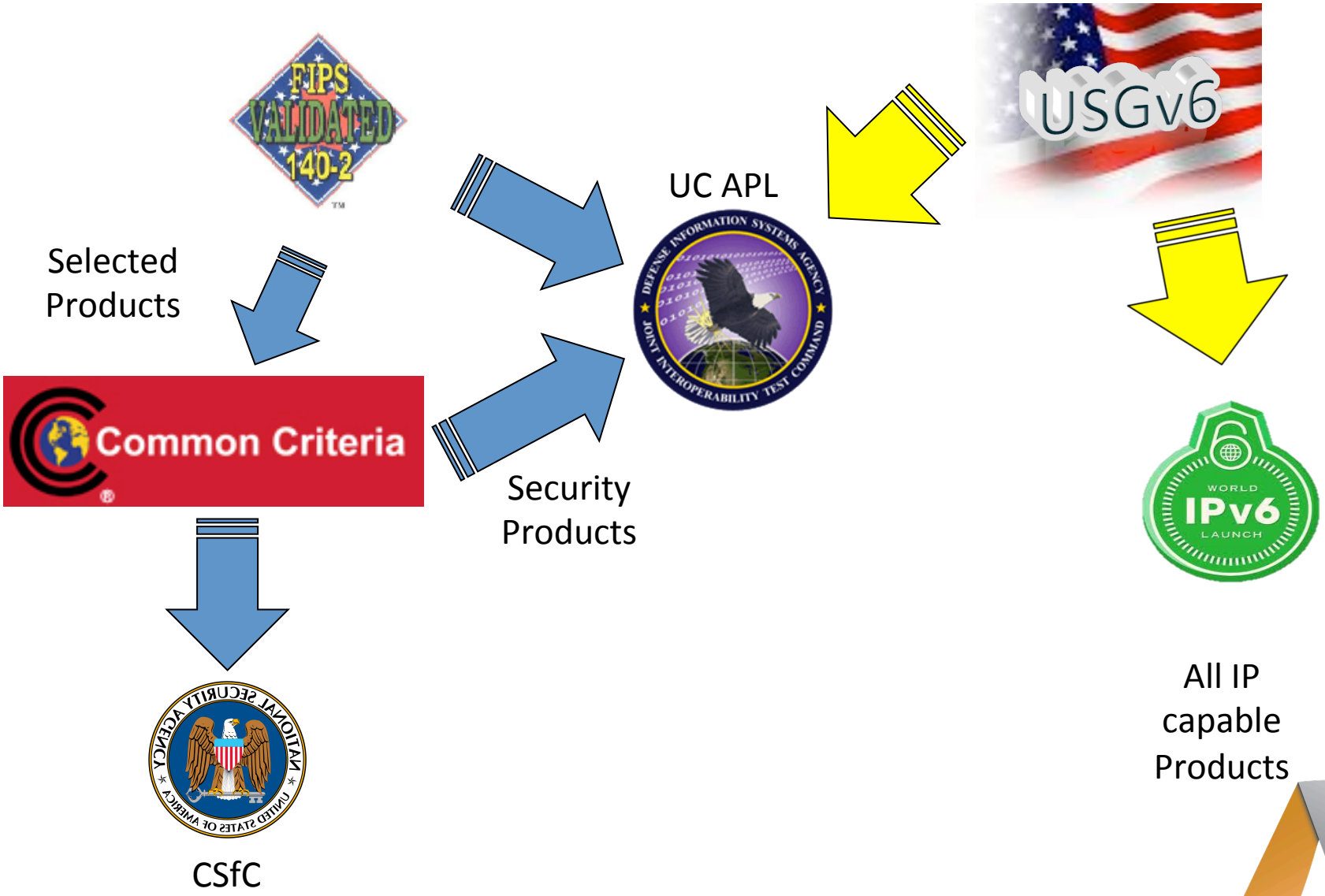
- Co-Founder and Lab Director @ Acumen Security
- 13 years certification and security experience
- Led Cisco's FIPS and CC certification teams

Overview

- Why align certification efforts?
  - Interdependency of certifications
- Challenges
- Efficiencies Gained
- How to successfully align certification efforts?
- Common pitfalls
- Key Takeaways

Why align?

Interdependencies of Certifications



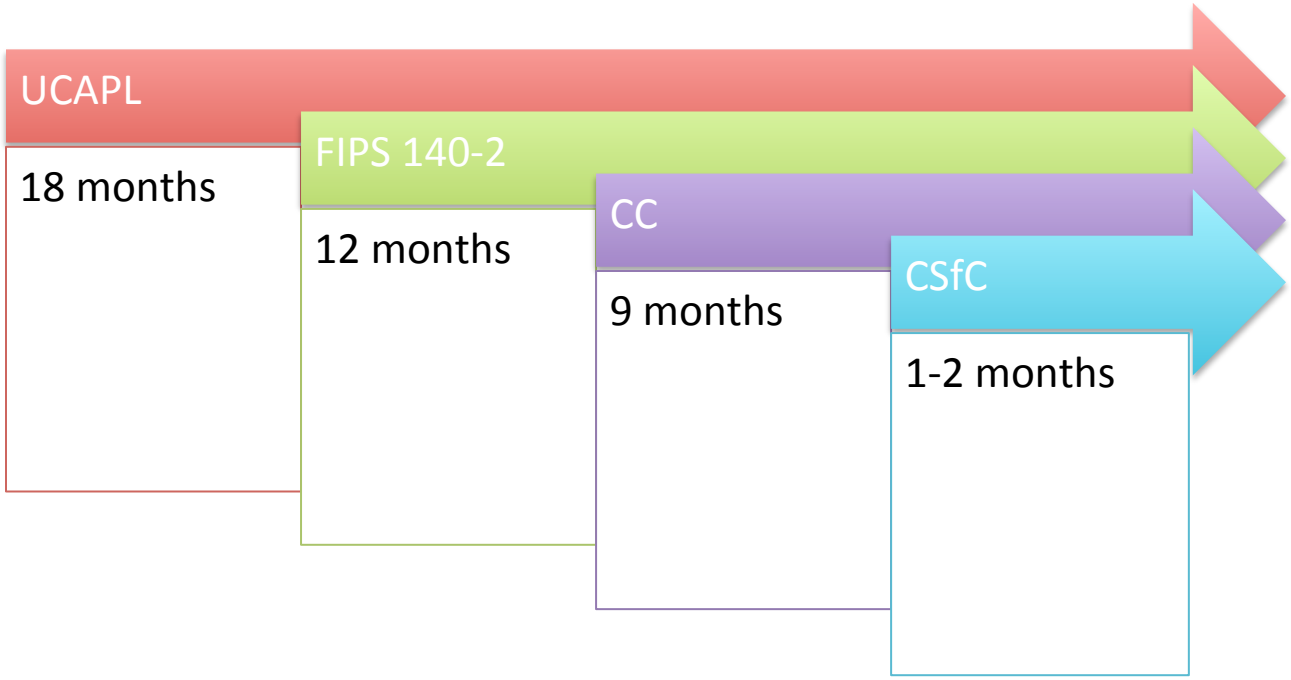
Why align certification efforts?

- Market dynamics and market needs
- Efficiencies
- To escape the cycle of continuous, never ending certification efforts
- You want to have a life!

Challenges to alignment nirvana

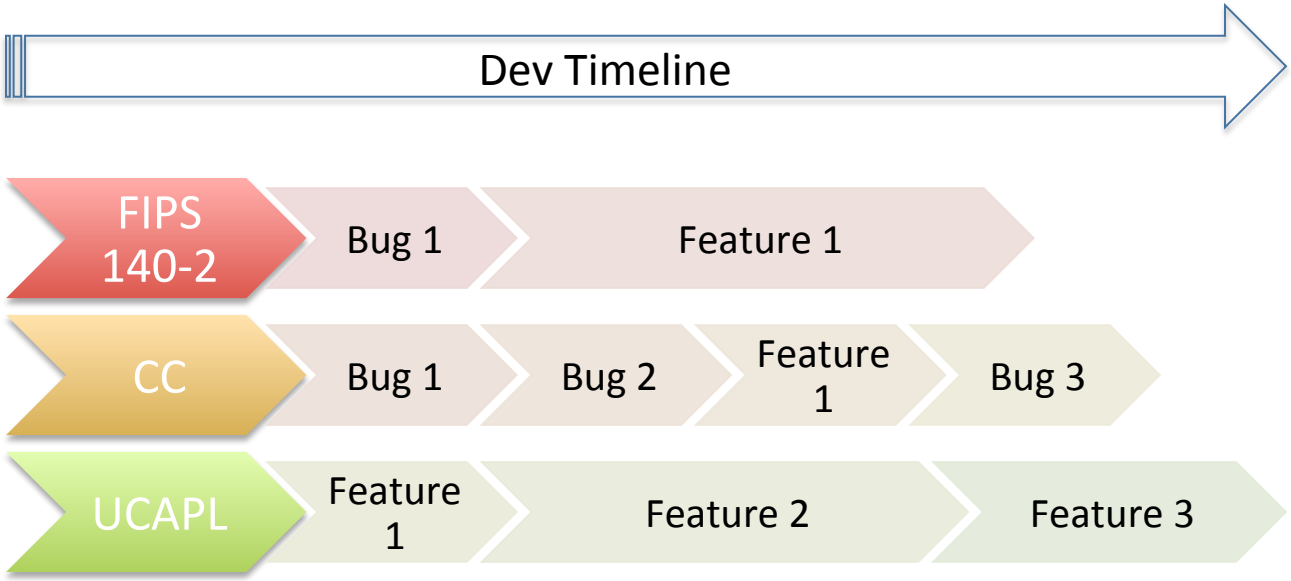
It is not all doom and gloom, I promise

Varying Certification Timelines*



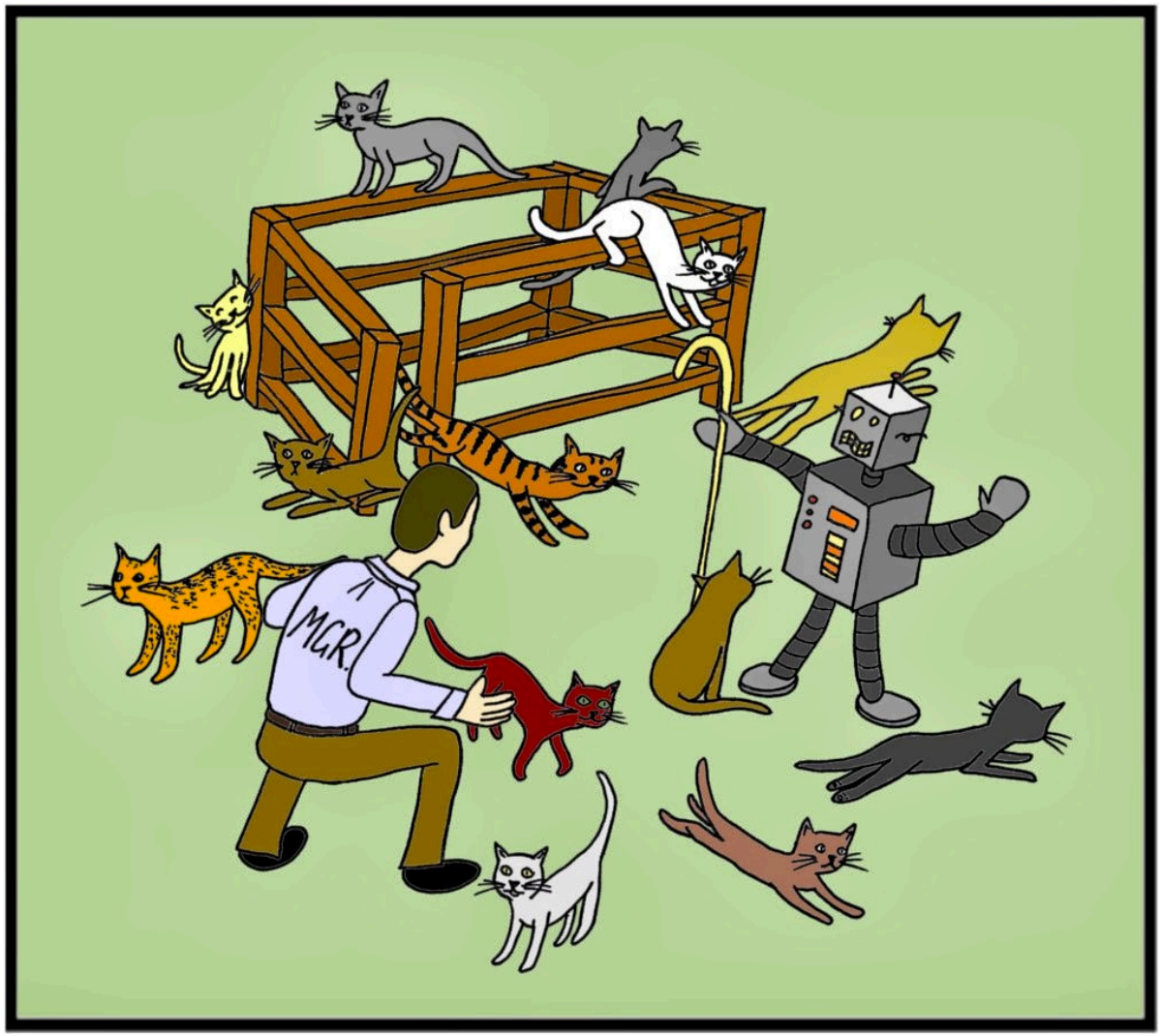
* Your mileage might vary!

Varying feature development timelines



Budget considerations

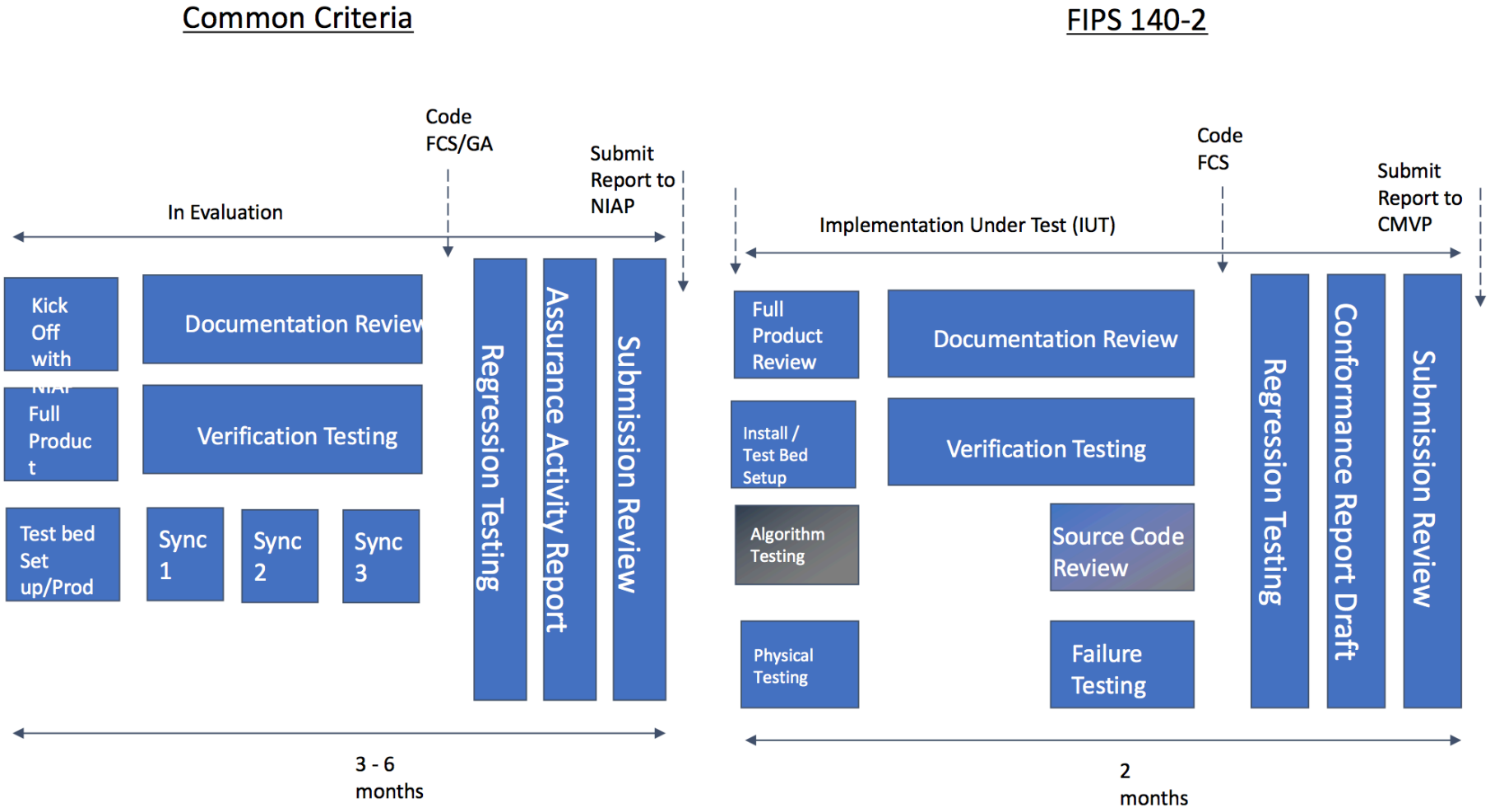
Managing multiple teams



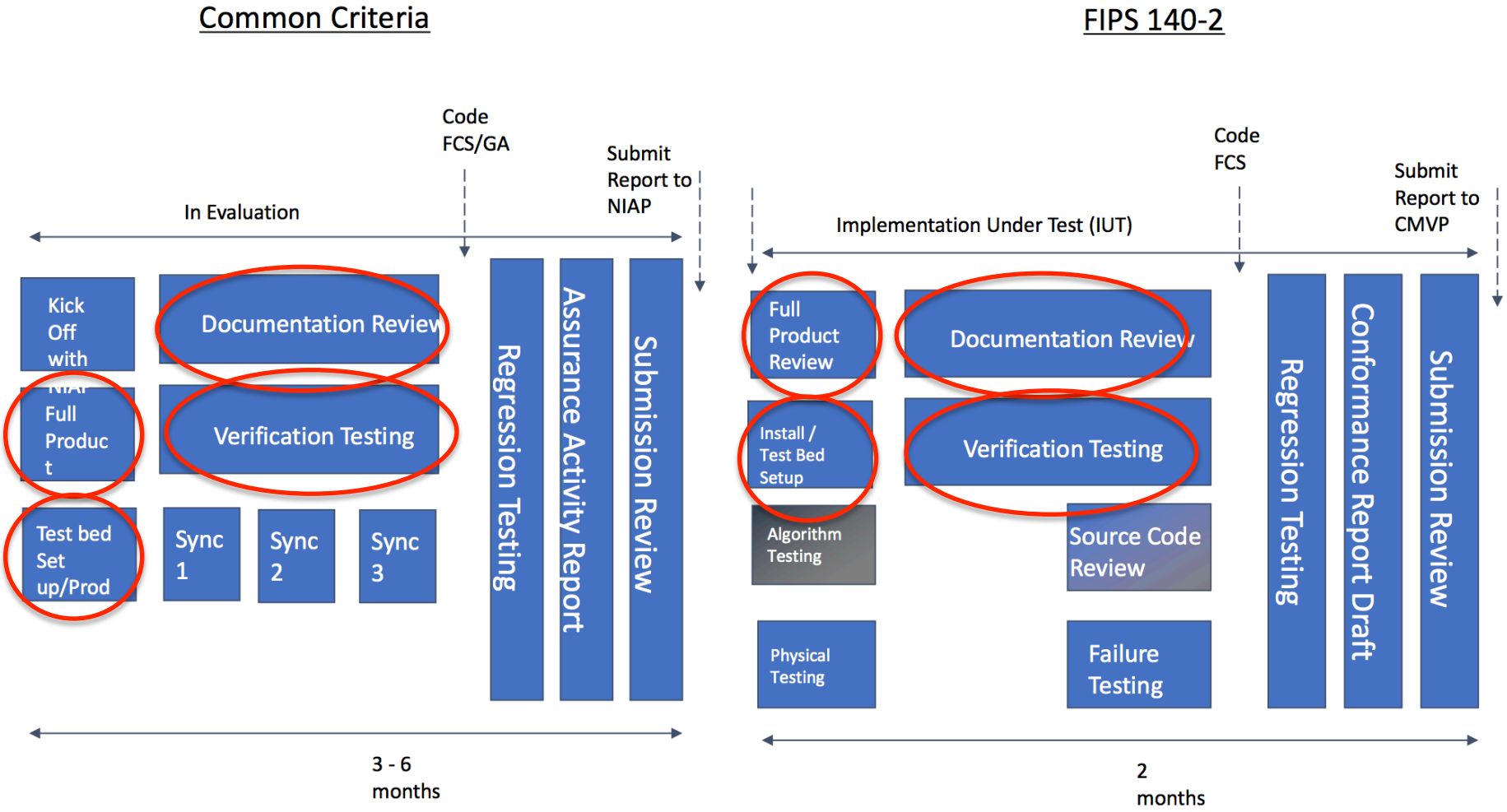
Is it worth the effort?

YES!

FIPS v/s CC timelines



Holy Repetition Batman!



Examples of efficiencies – FIPS/CC

- Entropy assessment
- Product set-up/configuration
- Crypto related requirements
- Ensuring the strictest interpretation of requirements are being considered
- Functional testing -> majority of FIPS positive testing is covered by NDcPP testing

There is about 20-25% efficiencies to be gained by running FIPS and CC in parallel

Okay, I am sold on the idea!

How do I go about aligning my certification efforts?

How to…

- Gather certification requirements
- Perform gap analysis for each certifications that need to be pursued
  - Extra points for combining gap analysis meetings
- Identify which certification efforts you can tackle at one go
  - Function of gaps to be fixed, resources availability and budget
- Use a GA/FCS as your central pole when creating certification plan
  - This makes normalizing certification timelines across validation efforts simpler
- Work with a lab that has the personnel and skills to run parallel certification efforts
- Drink copious amounts of coffee or beverage of choice!

Common Pitfalls

Danger ahead!

Where things can go awry?

- Over ambitious!
- Resource availability
- One certification effort dragging down the overall certification ship
- Requirements creep
- Labs having different teams running different programs
- Lack of alignment/buy-in from product teams

Key Takeaways

Parting thoughts…

- With planning, right team and right external partners it is possible to leverage efficiencies across multiple certification efforts
- Start small and then build on success and experience
- Aligning FIPS and CC (PP/cPP based evaluations) is a good starting point
- Ensure your product team buys into this idea
- Ensure your lab looks at this as a single certification effort
- Be ready to change plans and have contingencies in place

Questions?

Thank you!

Acumen Security

avora@acumensecurity.net

www.acumensecurity.net

@acumensec