ACU
AUSTRALIAN CATHOLIC UNIVERSITY

QUESTnet 2018

Designing a smart cybersecurity strategy for the future on shoe-string budget

Stephanie James, Mark Laffan and Wayne Tufek

28 September 2018

ML1

About ACU

- Australian Catholic University (ACU) is a public not-for-profit university funded by the Australian Government.
- It is open to students and staff of all beliefs.
- We have seven campuses across Australia, located in Adelaide, Ballarat, Brisbane, Canberra, Melbourne, North Sydney and Strathfield. We also have an international campus located in Rome, Italy.
- We have more than 25,000 EFTSL.
- IT currently has under 100 Staff Members with 2 Staff Members working full time on Information Security.
- IT has 3 Associate Directors – IT Applications and Operations, IT Strategy and Program Delivery, and IT End User Computing.

Slide 2

ML1 Presentation:

Agenda page/introduction

Where we were – introduction page – who (size of IT, structure)) what we are, doing,

Challenges in a University - lack of funding, not enough resources

Ops teams doing their own thing. Not enough processes, procedures.

Low maturity level -> assessment done. What is our posture.

Next steps -> look at raising our maturity, gap analysis

RFP -> painful process. Limited budget, couldn't pick a big company like E&Y needed a small company that could work with one person.

The Plan

Putting it together – what we set out to do. Followed NIST.

Identifying Quick (and those not so Quick) wins together - > finding out how hard it is to get ops team to agree on anything

What quick wins we identified.

Challenges on getting things done – BAU getting in the way

PWC audit -> took over the project

Change management process -> no one wanted to do anything until they knew who was doing what -> Our documents will

need to be changed (new teams, different structure)

The process we went through

The documents we produced

How the documents link together

High level outcomes, suggestions, engagement with the business, how to go about it

First year of the roadmap – what projects we will consider working on, getting funded,

Lessons learnt/take aways

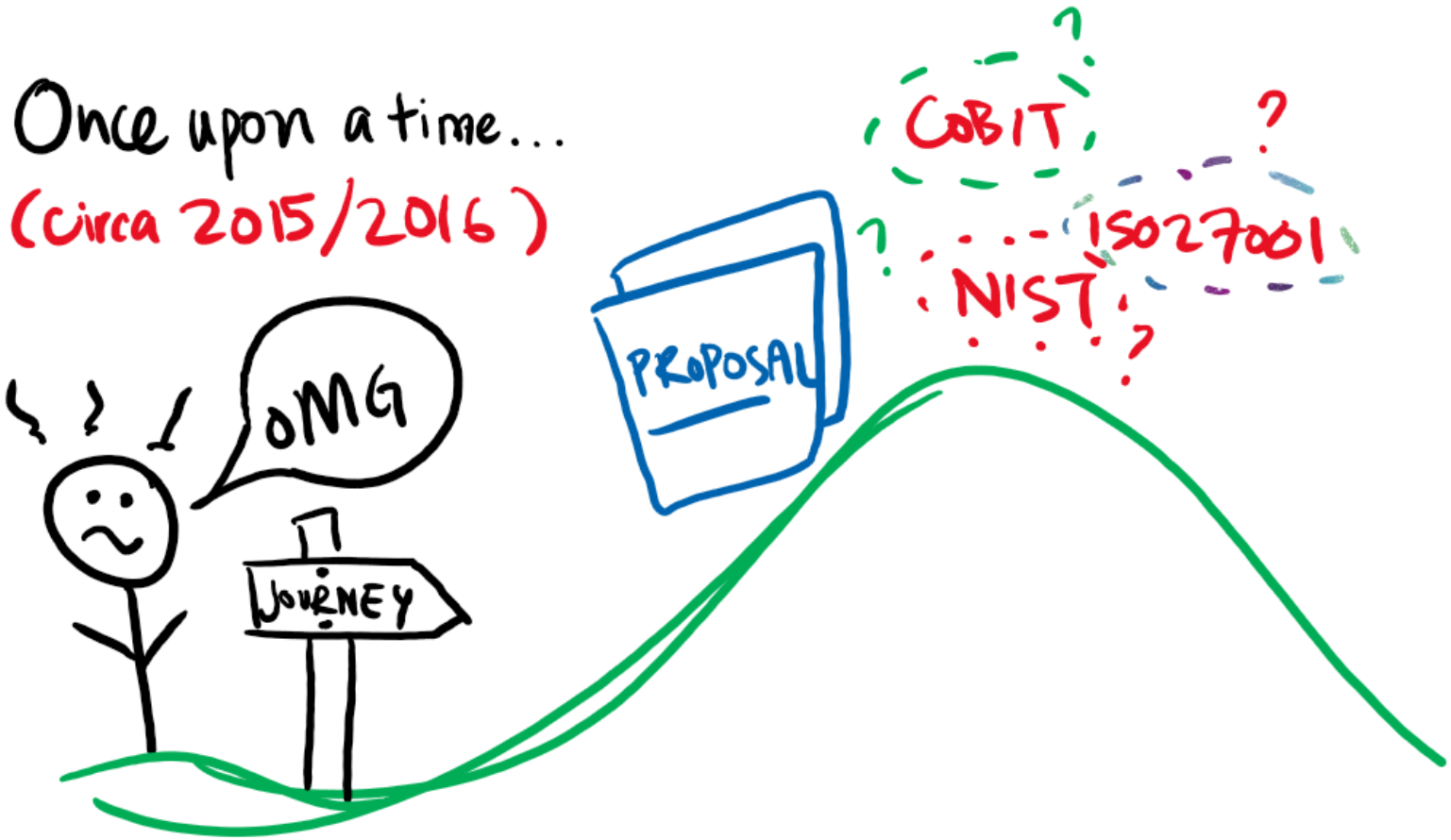
Mark Laffan, 20/08/2018

Everything starts somewhere...

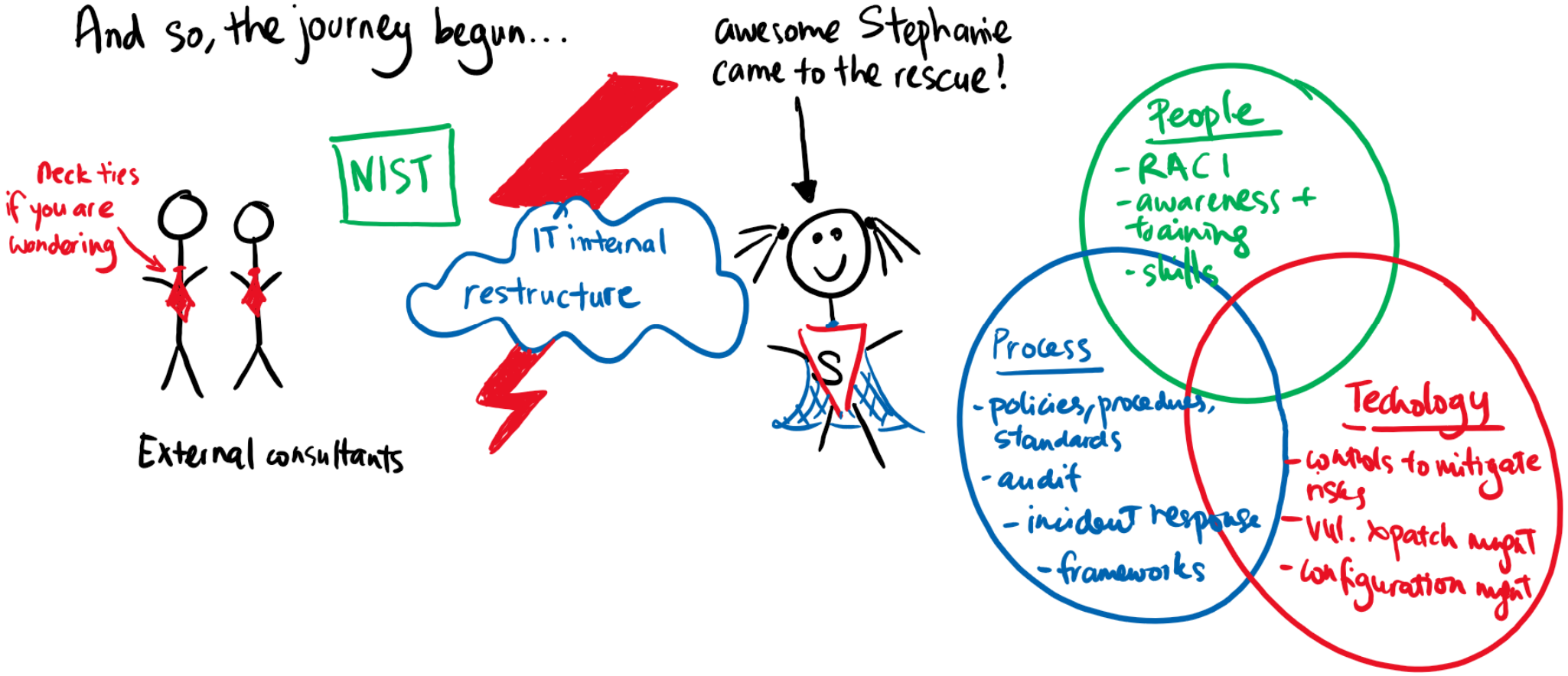
"Everything starts somewhere, though many physicists disagree. But people have always been dimly aware of the problem with the start of things. They wonder how the snow plough driver gets to work, or how the makers of dictionaries look up the spelling of words."

Terry Pratchett

How to start?


Once upon a time...
(circa 2015/2016)
OMG
JOURNEY
PROPOSAL
COBIT
ISO27001
NIST

Phase 1


And so, the journey begun...
Neck ties if you are wondering
External consultants
NIST
IT internal restructure
awesome Stephanie came to the rescue!
People
- RACI
- awareness + training
- skills
Process
- policies, procedures, standards
- audit
- incident response
- frameworks
Technology
- controls to mitigate risks
- Vul. & patch mgmt
- configuration mgmt

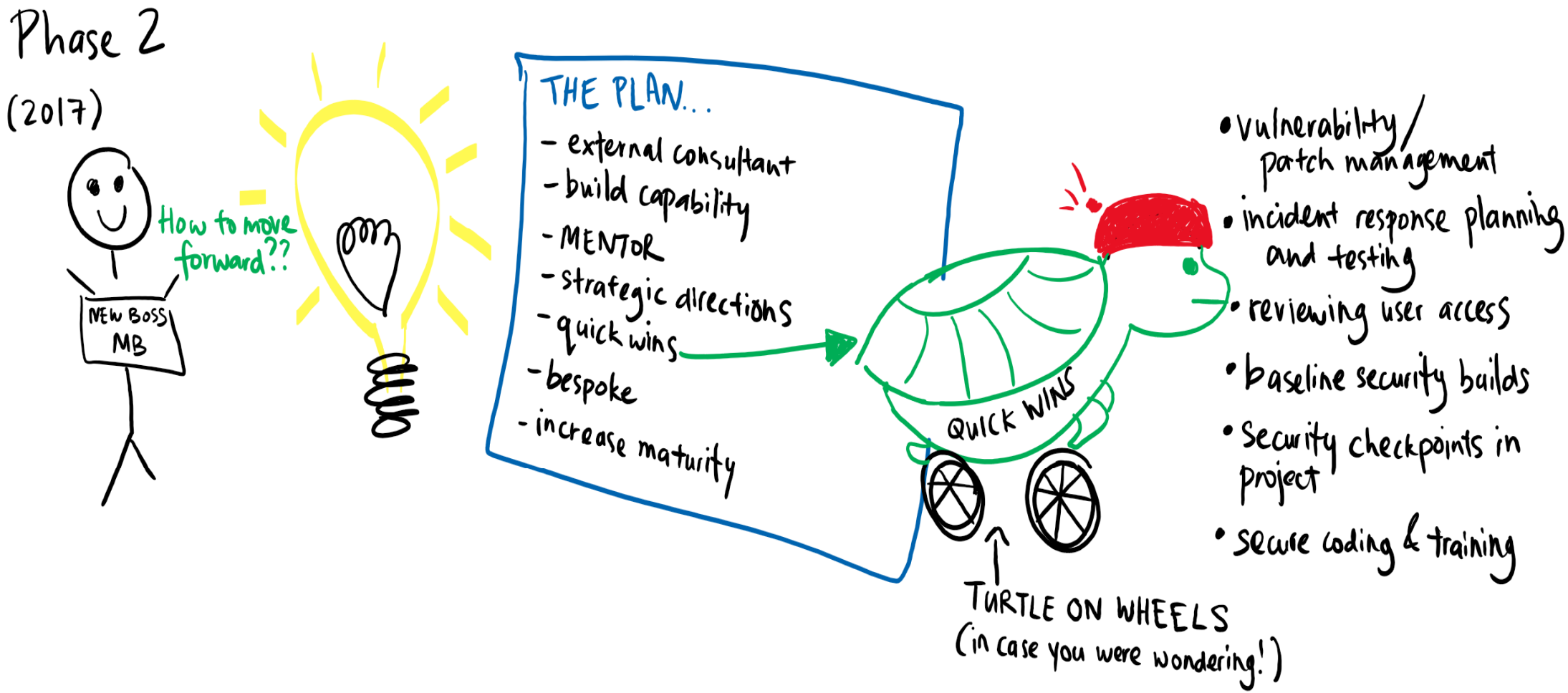
Our Adopted Security Controls/Capability Framework

The NIST framework helps organisations understand, structure, manage, and reduce cybersecurity risks.

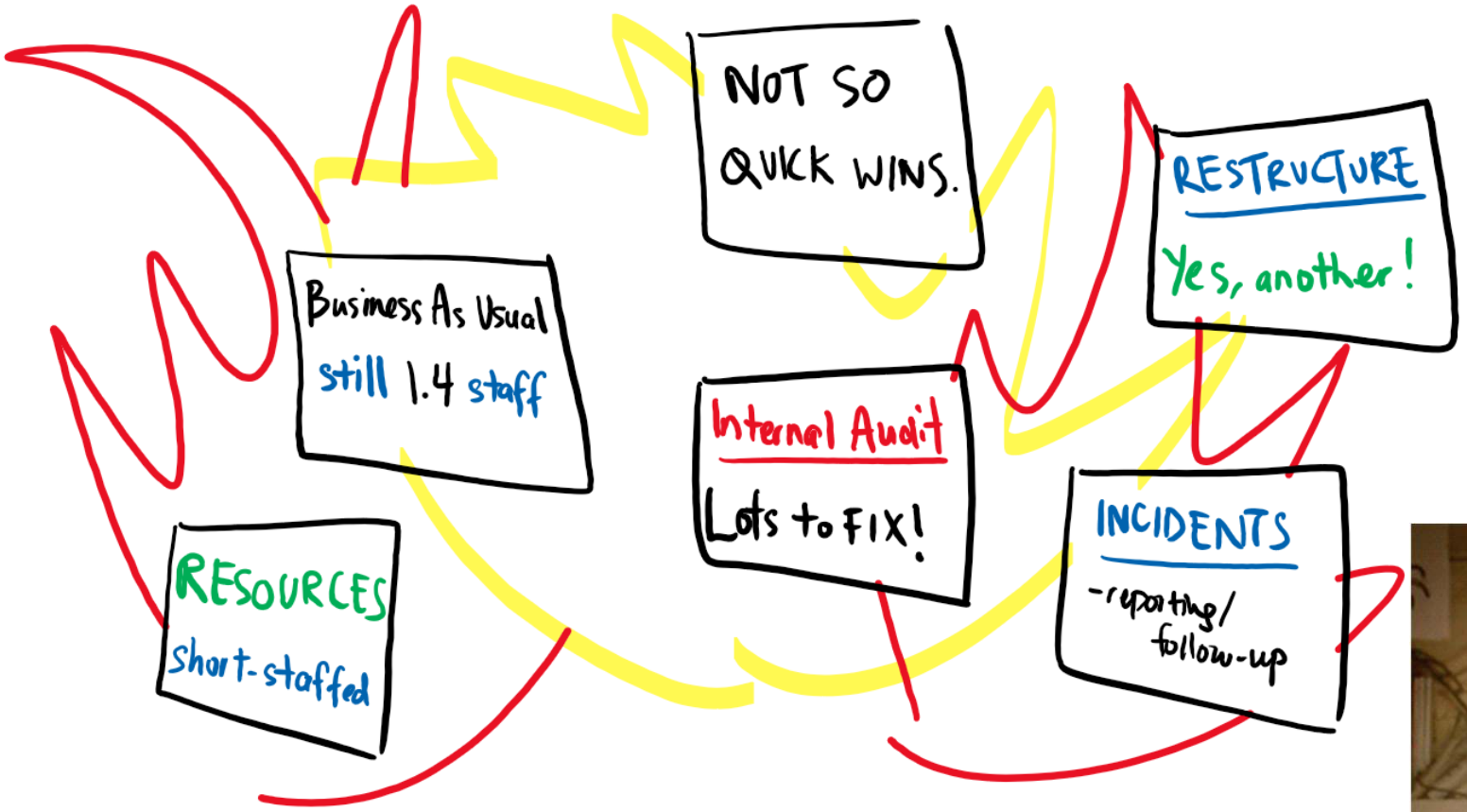
Cybersecurity violations can cause substantial financial losses, damage reputation, or cause outages that may permanently damage a company's market position.

Capability	Description
Identify	Develop the organisational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure protection of the enterprise's assets.
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

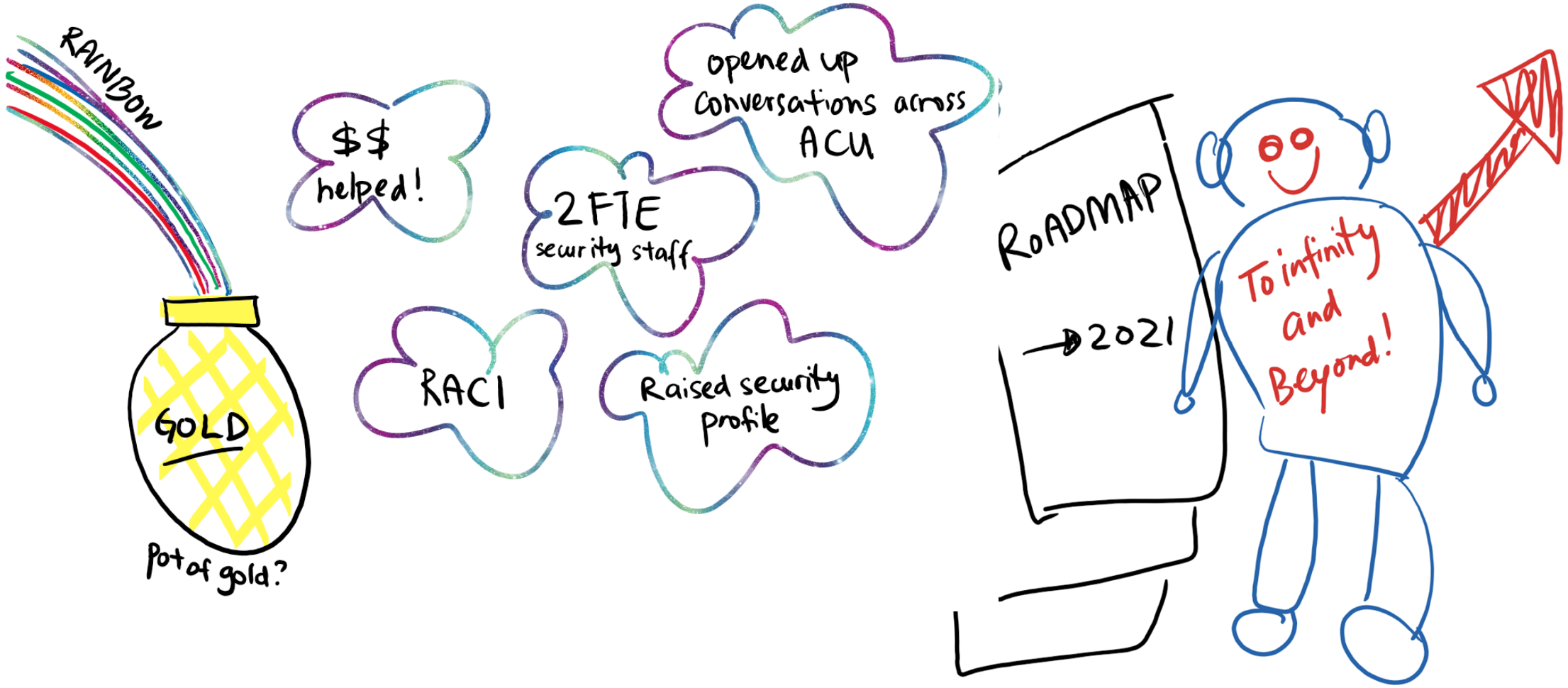
Phase 2


Phase 2
(2017)
NEW BOSS
MB
How to move forward??
THE PLAN...
- external consultant
- build capability
- MENTOR
- strategic directions
- quick wins
- bespoke
- increase maturity
QUICK WINS
• vulnerability / patch management
• incident response planning and testing
• reviewing user access
• baseline security builds
• Security checkpoints in project
• secure coding & training
TURTLE ON WHEELS
(in case you were wondering!)

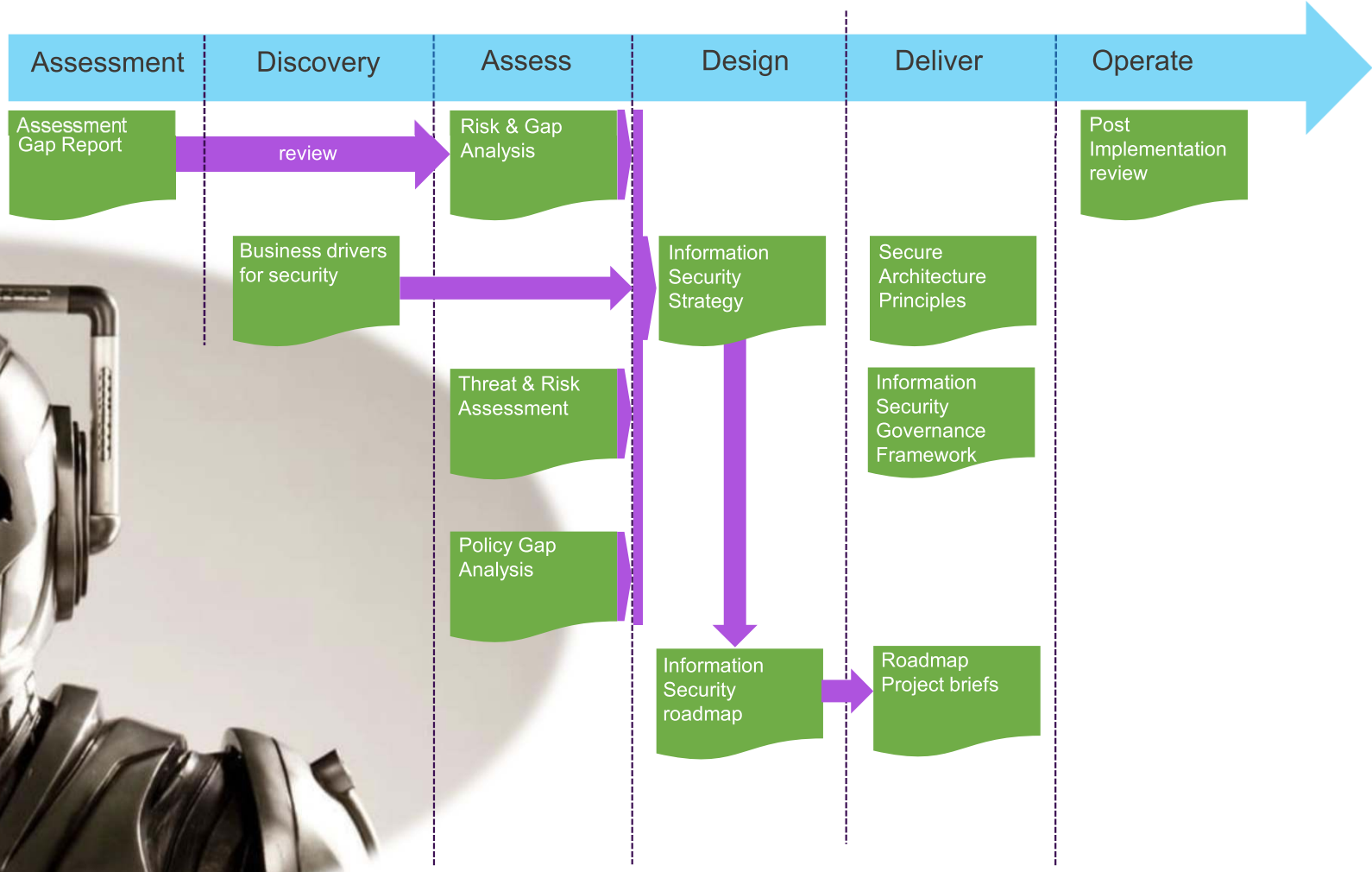
Things that went wrong...



Things that went right



The plan! The plan!



Cybersecurity Roadmap

Improvement Activity	!	?	$	Months 0 - 12	12 - 24	24 - 36
Policies, procedures and standards						

Key

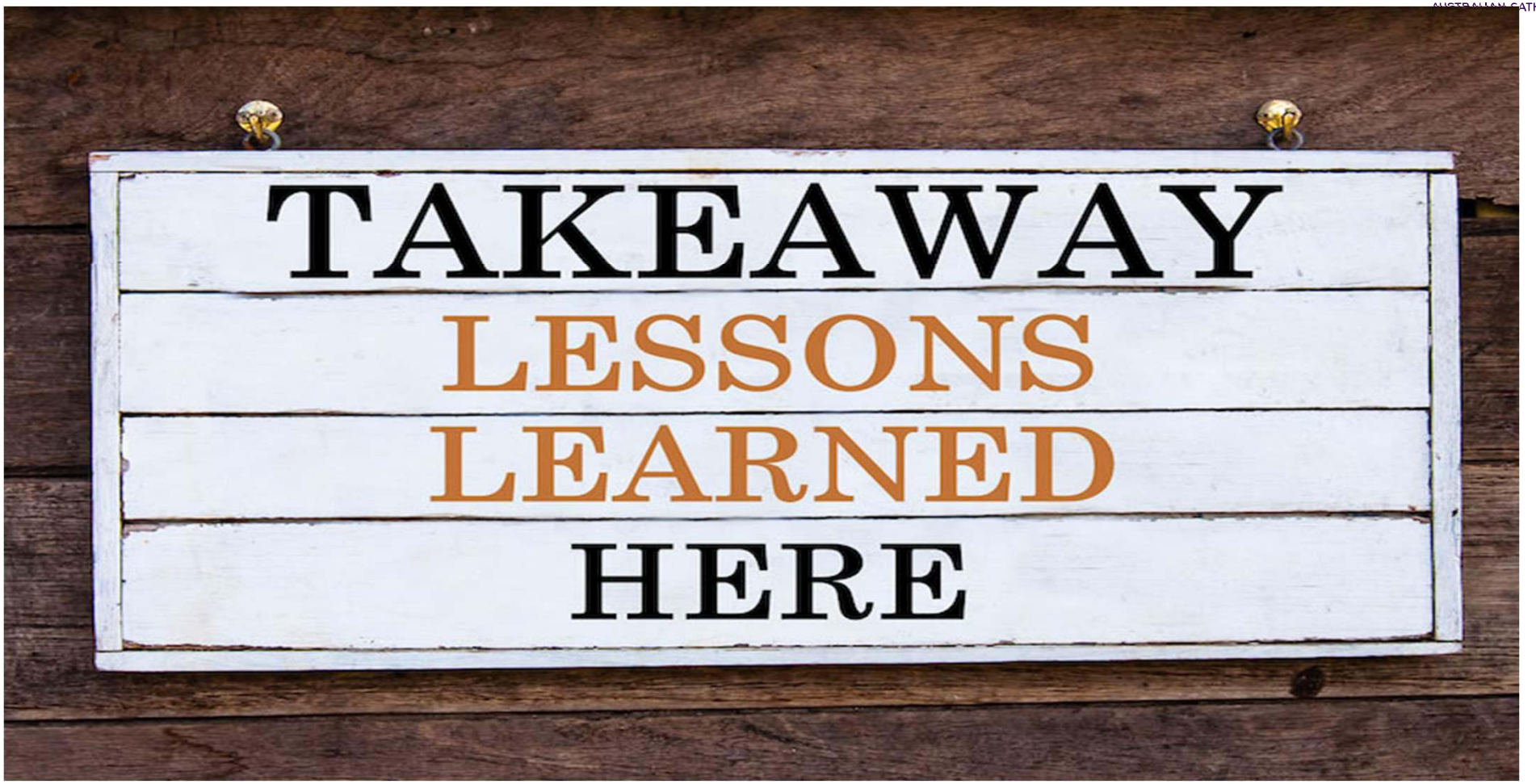
!
High priority
Medium priority
Low priority

?
High Complexity
Medium Complexity
Low Complexity

$
High Cost (> $500,000)
Medium Cost (> $50,000)
Low Cost (< $50,000)

0 – 12 months – Identify key improvement activities, produce business cases and get funded

Takeaways!



Questions?


IT WAS GREAT! WE TALKED ABOUT OUR FIRST CARS, WHERE WE WENT TO ELEMENTARY SCHOOL, OUR NIECES AND NEPHEWS...
DUDE-- SOUNDS MORE LIKE SHE GOT ALL YOUR ONLINE SECURITY QUESTIONS.
rhymeswithorange.com
©HILARY B. PRICE Dist. by King Features 5-16-2013