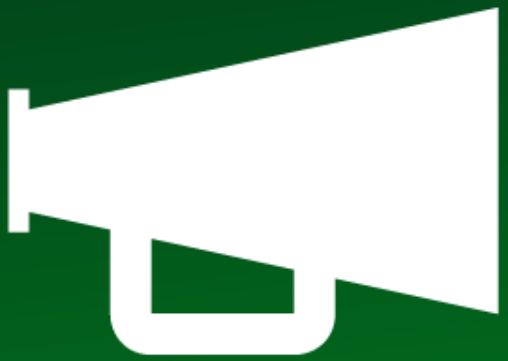
goto; conference



Click ‘engage’ to rate session.

Rate **12** sessions to get the supercool GOTO reward

Join the conversation #gotoldn

goto; conference

When devops meets security

Michael Brunton-Spall

goto; conference

”I'm from the Government and I'm here to help”

goto; conference

”I'm from security and I'm here to help”

goto; conference

Government Digital Service

goto; conference

Simpler, Clearer, Faster

goto; conference

The state of information security in 2015

goto; conference

BS7799-1:1999

goto; conference

ISO27001:2005

goto; conference

Approval to operate

goto; conference

Accreditation

goto; conference

Certification

goto; conference

PCI

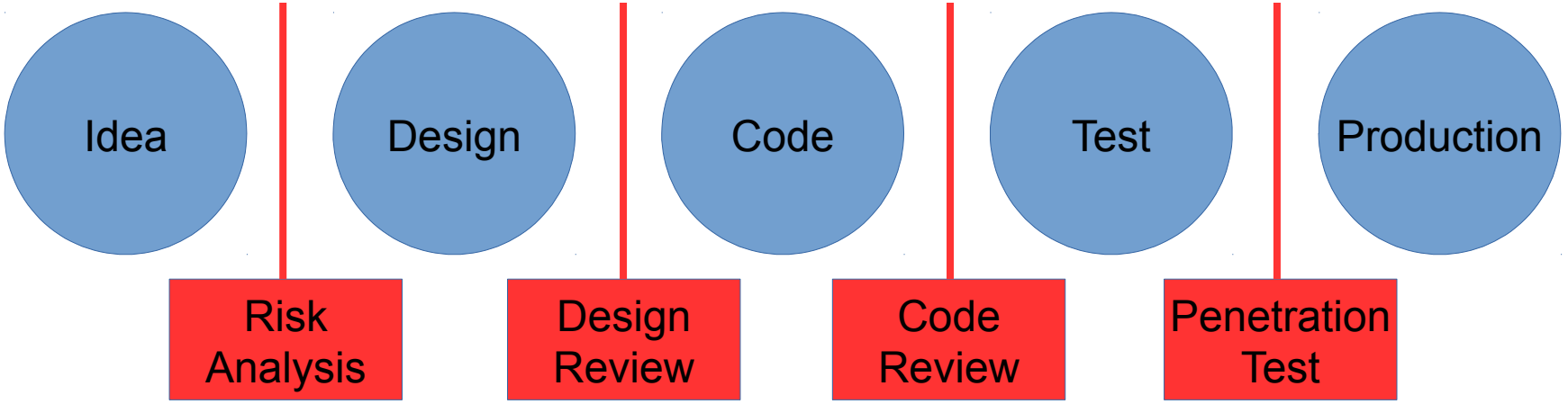
goto; conference

What does this look like?

goto; conference

Traditional model

goto; conference



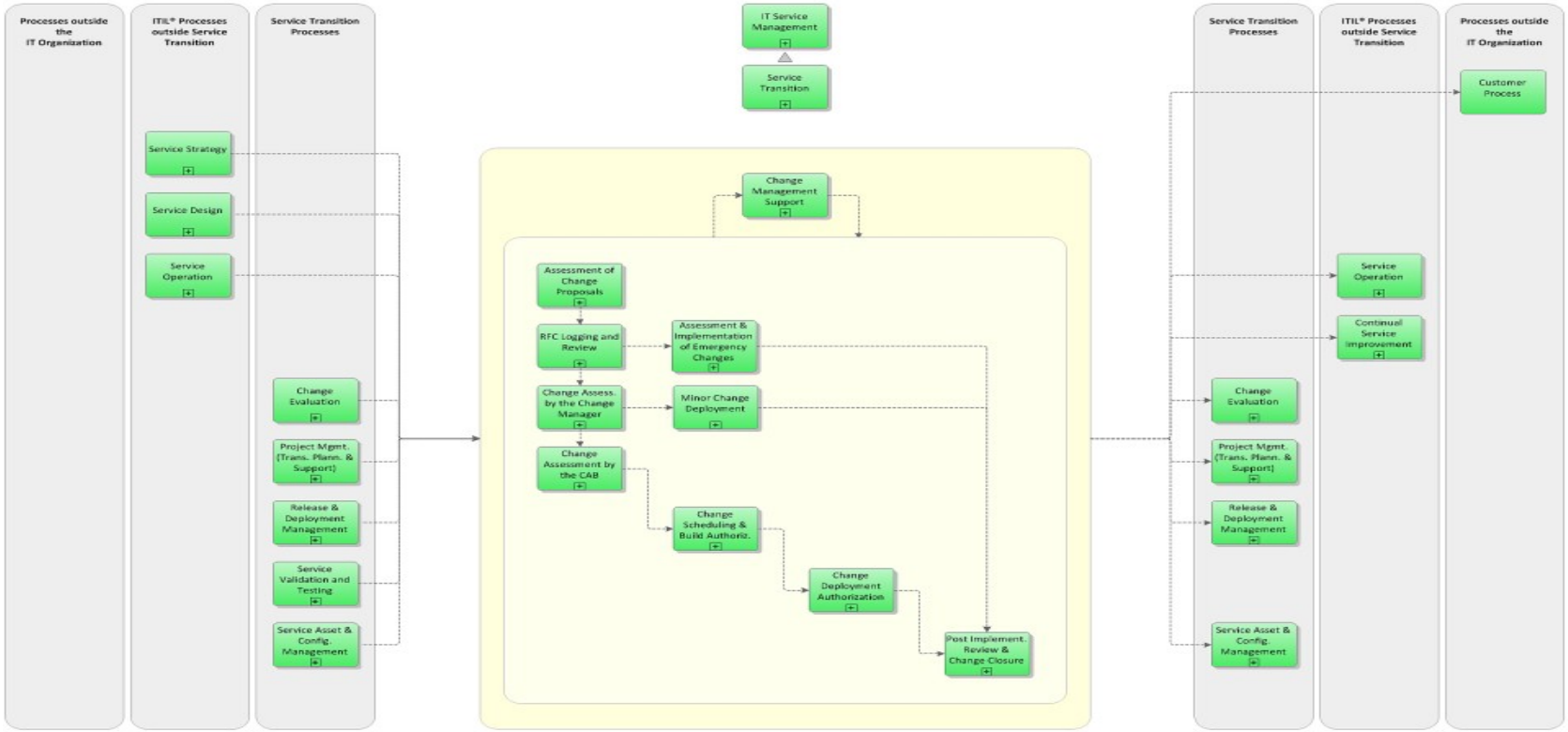
goto; conference

How do we deal with changes?

goto; conference

it process maps

ITIL Change Management



Join the conversation #gotoldn

goto; conference

Agile changes everything

goto; conference

Only do what's needed now

goto; conference

Release It!

goto; conference

MVP and iterate

goto; conference

Focus on flow and cycle time

goto; conference

A security nightmare!

goto; conference

A brave new world for security

goto; conference

Security needs to be an enabler

goto; conference

We reviewed agile projects across government

goto; conference

Biggest consistent finding?

goto; conference

There is no consistency

goto; conference

Most teams don't know how to do this

goto; conference

So what can we do?

goto; conference

Principles over rules

goto; conference

The UK Government published 8 principles

goto; conference

1 - Accept uncertainty

goto; conference

2 - Security as part of the team

goto; conference

3 - Understand the risks

goto; conference

4 - Trust decision making

goto; conference

5 - Security is part of everything

goto; conference

6 - User experience is important

goto; conference

7 - Audit decisions

goto; conference

8 - Understand big picture impact

goto; conference

But what does that mean?

goto; conference

Imagine a new project

goto; conference

Choose security model that's appropriate

goto; conference

At project inception

goto; conference

Understand the threats

goto; conference

Educate decision makers to risks

goto; conference

Make risk decisions, per story, in the team

goto; conference

What do you do about it?

goto; conference

Avoid

goto; conference

Transfer

goto; conference

Accept

goto; conference

Mitigate

goto; conference

Temporarily Accept

goto; conference

What sort of controls might we use?

goto; conference

Active countermeasures

goto; conference

Deter, Detect, Prevent

goto; conference

Reactive countermeasures

goto; conference

Correct, Respond, Recover

goto; conference

Traditional security people understand this

goto; conference

But there's more

goto; conference

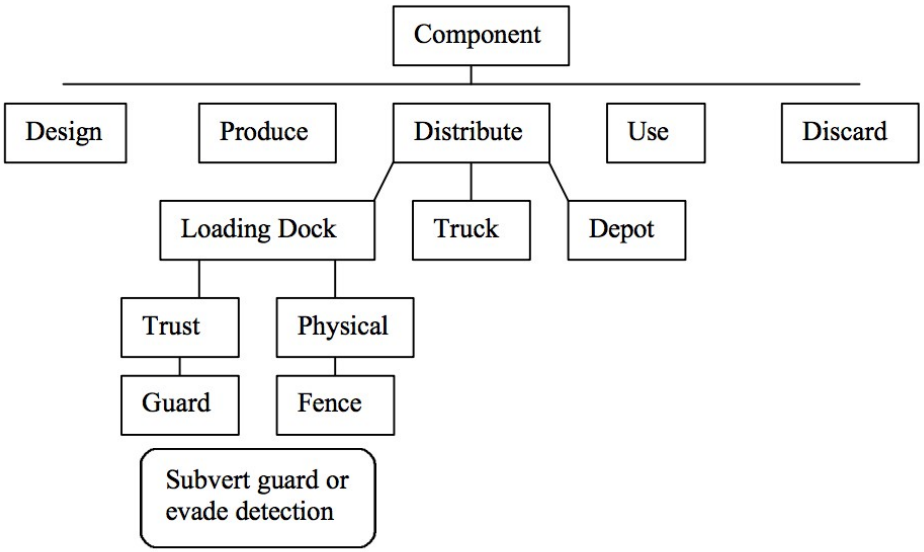
Anti-personas

goto; conference

Misuse cases

goto; conference

Attack trees



https://www.schneier.com/paper-secure-methodology.pdf

goto; conference

Red teams

goto; conference

Automated penetration testing

goto; conference

Automated
Integrated
Repeatable

goto; conference

Please

Remember to rate this session

Thank you!

Join the conversation #gotoldn

goto; conference

Thanks !

Join the conversation #gotoldn