



Cabinet Office

Michael Brunton-Spall
Lead Security Architect
Government Digital Service
@bruntonspall

Agile Security

What is agile?

Manifesto for Agile Software Development

We are uncovering better ways of developing software by doing it and helping others do it.
Through this work we have come to value:

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

That is, while there is value in the items on the right, we value the items on the left more.

While the things on
the right have value,
the things on the left
have more value

Individuals and interactions over processes and tools

Working software over comprehensive documentation

Responding to change over following a plan

Customer collaboration over contract negotiation

Contracts, Planning, Documentation, Processes and Tools

Collaboration, Change, Deliverables, People

Building software together

Support and trust

Simplicity

Maximising work not done

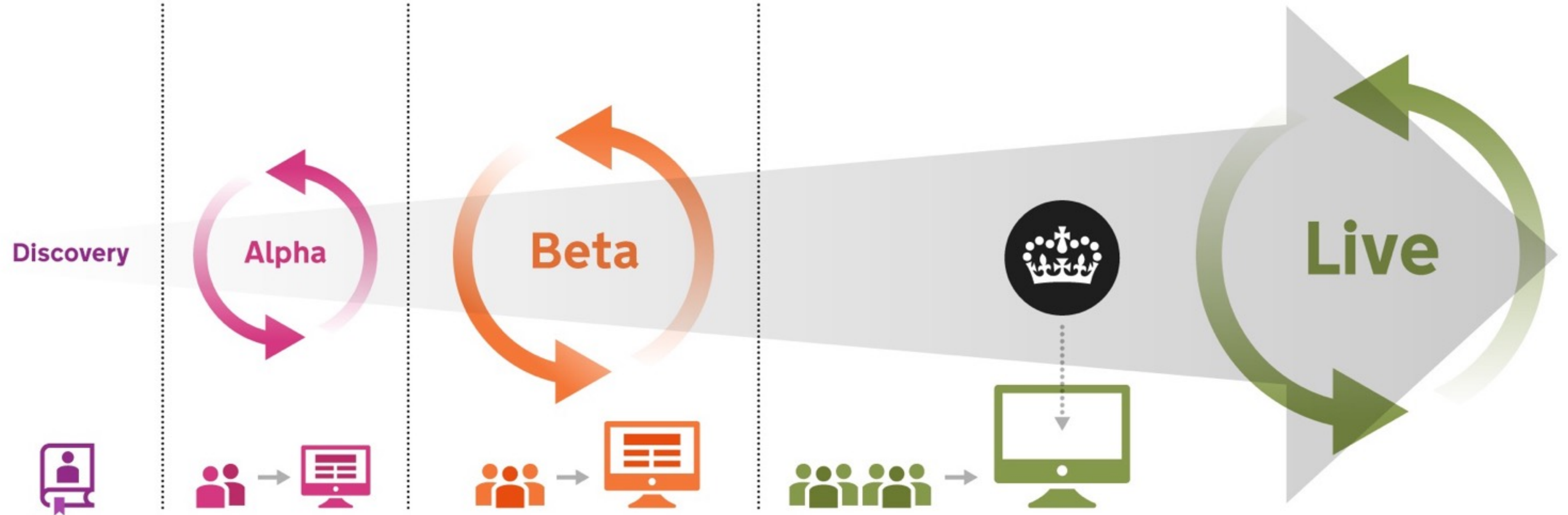
What does this mean
today?

Minimum viable product or service

Iterate

Release early, release
often

User needs



Secure Agile Development

Security must be an
enabler of the team

The unit of delivery is
the team

The unit of decision
making is the team

Risk

Educate the team to
the threats

Keep a running risk log

Apply risk decisions per story

Apply controls per story

Security debt

Simple systems are
more secure

Choosing the secure
method must be the
easiest option

Secure Agile Operations

Infrastructure as code

```
class varnish::package {
  package { 'varnish':
    ensure => installed,
  }
}

class varnish::config($upstream_port, $strip_cookies) {
  include varnish::restart

  $app_domain = hiera('app_domain')

  file { ['/etc/default/varnish':
    ensure => file,
    content => template('varnish/defaults.erb'),
    notify => Class['varnish::restart'], # requires a full varnish restart to pick up changes
  }

  file { ['/etc/default/varnishncsa':
    ensure => file,
    source => 'puppet:///modules/varnish/etc/default/varnishncsa',
  }

  file { ['/etc/varnish/default.vcl':
    ensure => file,
    content => template('varnish/default.vcl.erb'),
  }
}
```

Infrastructure as testable code

```

context 'with aliases' do
  let(:params) do
    {
      :port => 8000,
      :app_type => 'rack',
      :vhost_aliases => ['foo', 'bar'],
      :domain => 'example.com',
      :vhost_full => 'giraffe.example.com',
    }
  end

  it { is_expected.to contain_nginx__config__vhost__proxy('giraffe.example.com').with_aliases(['foo.example.com', 'bar.example.com']) }
end

context 'with an upstart post-start script' do
  let(:params) do
    {
      :port => 8000,
      :app_type => 'rack',
      :domain => 'foo.bar.baz',
      :vhost_full => 'giraffe.foo.bar.baz',
      :upstart_post_start_script => '/bin/true',
    }
  end

  it do
    is_expected.to contain_file('/etc/init/giraffe.conf').with(:content => %r{post-start script\s*\n\s*/bin/true\s*\n})
  end
end

```

@normal

Scenario: check quick answers load

When I visit "/vat-rates"

Then I should see "VAT rates"

@normal

Scenario: check guides load

When I visit "/getting-an-mot"

Then I should see "Getting an MOT"

@normal

Scenario: check transactions load

When I visit "/apply-renew-passport"

Then I should see "UK passport"

@normal

Scenario: check benefit schemes load

When I visit "/pension-credit"

Then I should see "Pension Credit"

@normal

Scenario: check homepage content type & charset

When I visit "/"

Why does that matter?

Australian Signals Directorate

Whitelisting

Patch Management

Admin controls

Dealing with security patches

What machines are affected?

```
class nginx::package(  
  $nginx_package = 'nginx-full',  
  $version       = 'present',  
) {  
  
  include govuk::ppa  
  
  # nginx package actually has nothing useful in it; we normally need nginx-full  
  package { 'nginx':  
    ensure => purged,  
  }  
  
  package { 'nginx-common':  
    ensure => $version,  
    notify => Class['nginx::restart'],  
  }  
  
  package { $nginx_package:  
    ensure  => $version,  
    notify  => Class['nginx::restart'],  
    require => Package['nginx-common'],  
  }  
}
```

```
(michaelbruntonspalldev@ubuntu work/puppet)% ack-grep nginx::package::version  
hieradata/common/precise.yaml
```

```
5:nginx::package::version: '1.4.4-1~precise0'
```

```
hieradata/common.yaml
```

```
151:nginx::package::version: '1.4.6-1ubuntu3.1'
```

```
hieradata/class/frontend.yaml
```

```
2:nginx::package::version: '1.4.6'
```

```
hieradata/class/backend.yaml
```

```
2:nginx::package::version: '1.4.5'
```

Updating machines in test

```
hieradata/test.yaml  
2:nginx::package::version: '1.4.7'
```

```
(michaelbruntonspalldev@ubuntu work/puppet)% ack-grep nginx::package::version  
hieradata/test/frontend.yaml  
2:nginx::package::version: '1.4.7'
```

What does Agile and DevOps give you?

Automated Testing

Infrastructure as code

Fast repeatable deploys

Audit logs

Code review of infrastructure changes



Cabinet Office

Michael Brunton-Spall
Lead Security Architect
Government Digital Service
@bruntonspall