

It's not all tech: cultural change for DevSecOps

Red Hat Security Symposium
Victoria, BC

Mike Bursell
chief security architect, Red Hat



DevOps - more than just technology

Part I:

What is DevOps? And DevSecOps?

Part II:

Tools, process or culture? Which is most important?

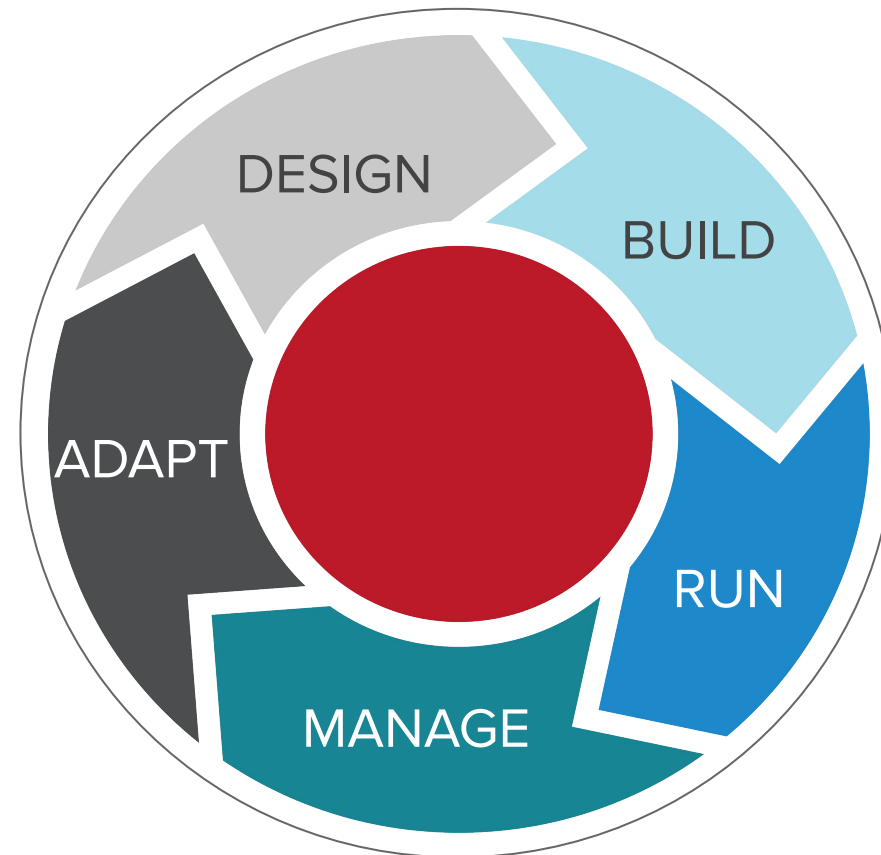
Summary

Part I:

What is DevOps?

What is DevOps? And DevSecOps?

“DevOps is the practice of operations and development engineers participating together in the entire service lifecycle, from design through the development process to production support.”[1]



[1] <https://theagileadmin.com/what-is-devops/>

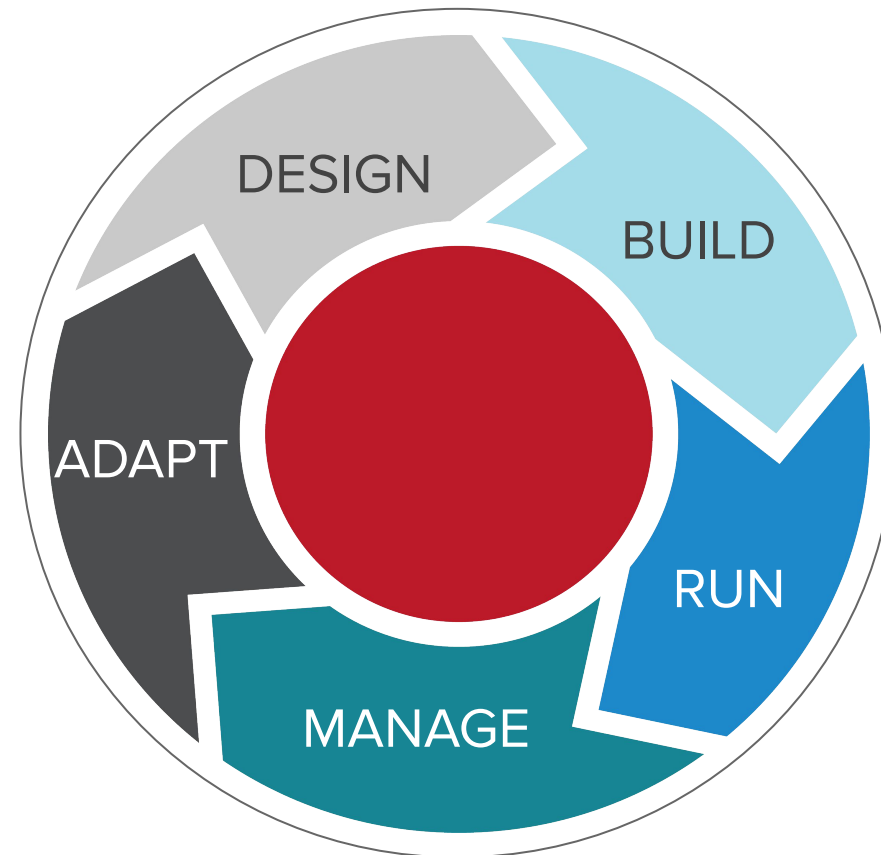
What is DevOps? And DevSecOps?

“DevOps is the practice of operations and development engineers participating together in the entire service lifecycle, from design through the development process to production support.”[1]

“The purpose and intent of **DevSecOps** is to build on the mindset that ‘everyone is responsible for security’...”[2]

[1] <https://theagileadmin.com/what-is-devops/>

[2] <http://www.devsecops.org/blog/2015/2/15/what-is-devsecops>



DevOps and DevSecOps

“For 20 years, people have been leaving security till last” - colleague

DevOps and DevSecOps

“For 20 years, people have been leaving security till last” - colleague

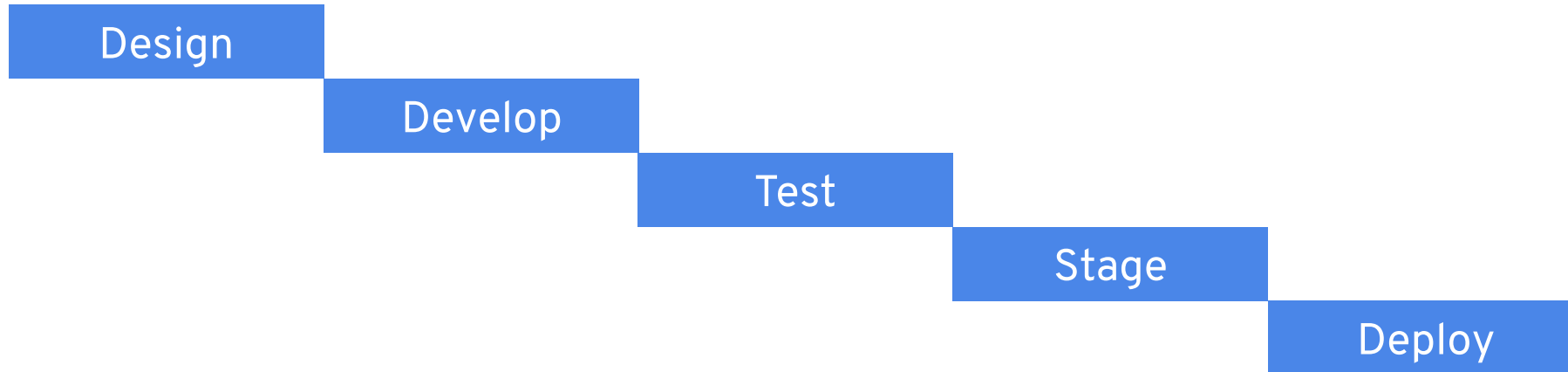
“...you could have missed the last two words out.” - me

DevOps and DevSecOps

“For 20 years, people have been leaving security till last” - colleague

“...you could have missed the last two words out.” - me

Classic waterfall project

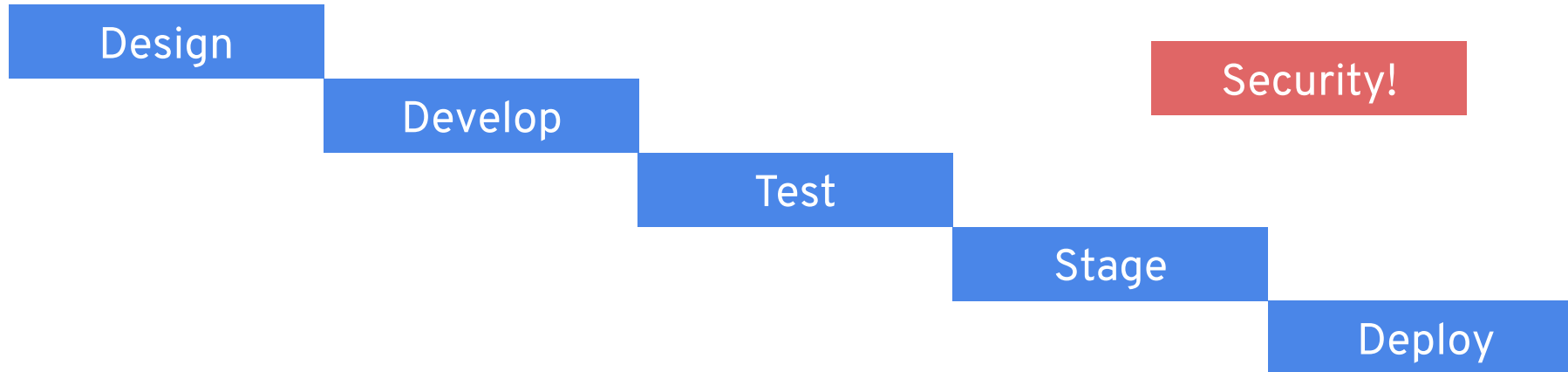


DevOps and DevSecOps

“For 20 years, people have been leaving security till last” - colleague

“...you could have missed the last two words out.” - me

Classic waterfall project

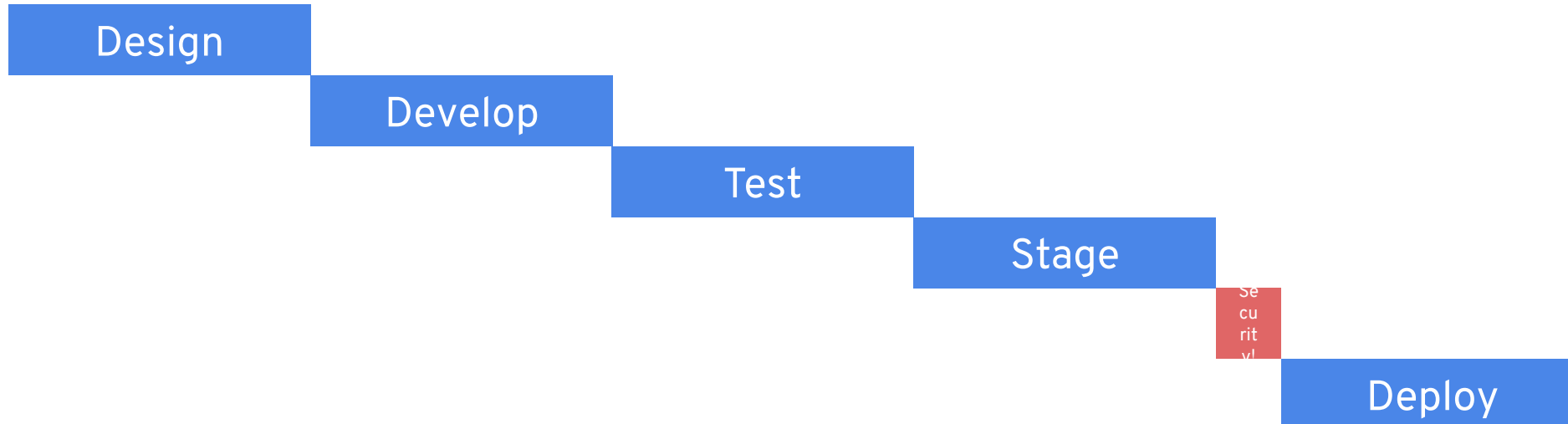


DevOps and DevSecOps

“For 20 years, people have been leaving security till last” - colleague

“...you could have missed the last two words out.” - me

Classic waterfall project - project manager's hope

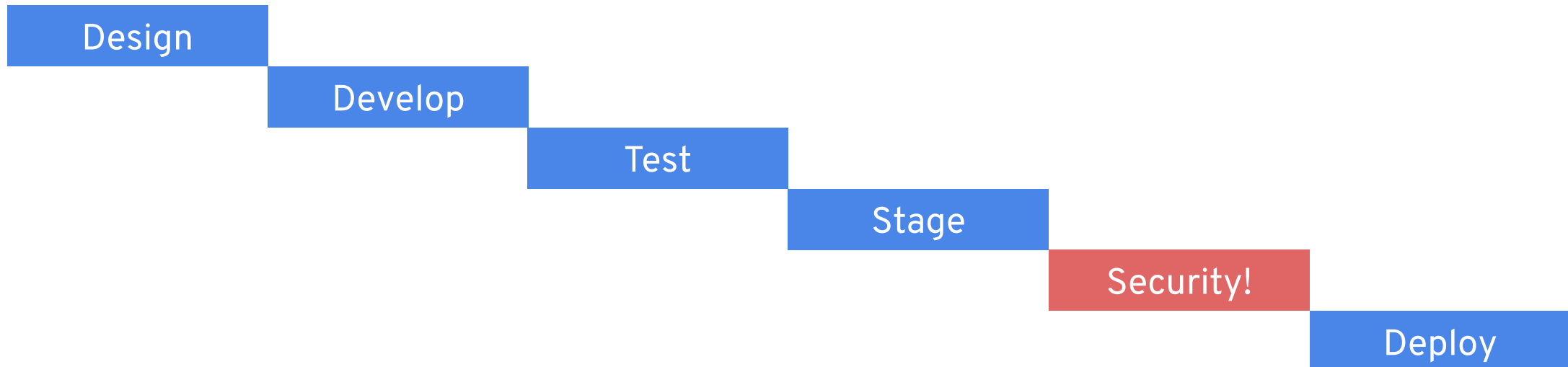


DevOps and DevSecOps

“For 20 years, people have been leaving security till last” - colleague

“...you could have missed the last two words out.” - me

Classic waterfall project - security architect's guesstimate

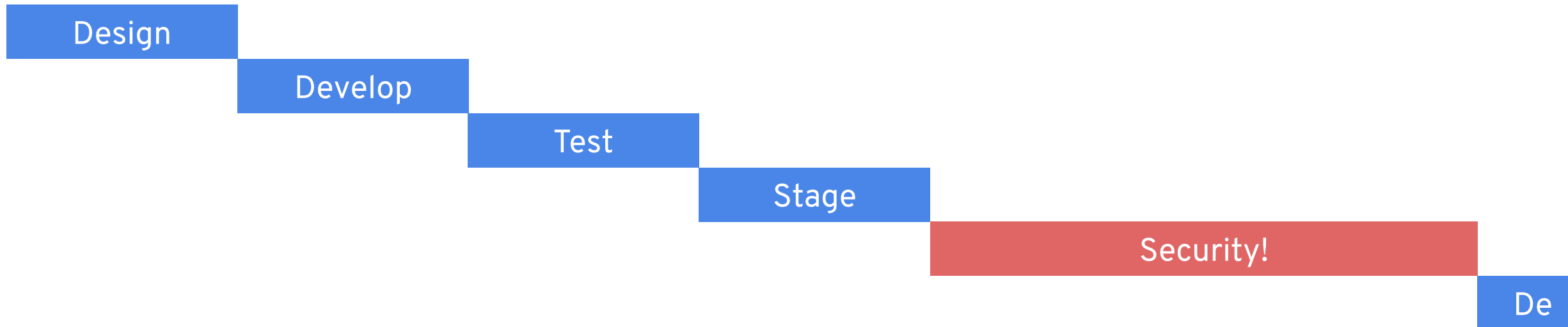


DevOps and DevSecOps

“For 20 years, people have been leaving security till last” - colleague

“...you could have missed the last two words out.” - me

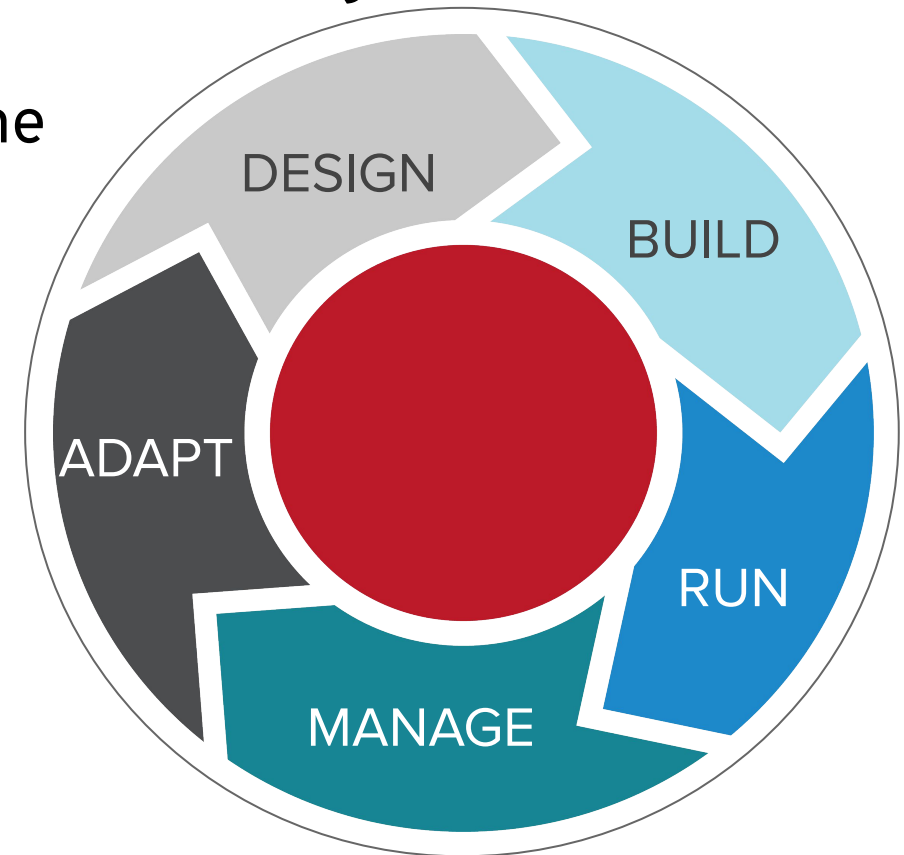
Classic waterfall project - actual



DevOps and DevSecOps

“For 20 years, people have been leaving security till last” - colleague

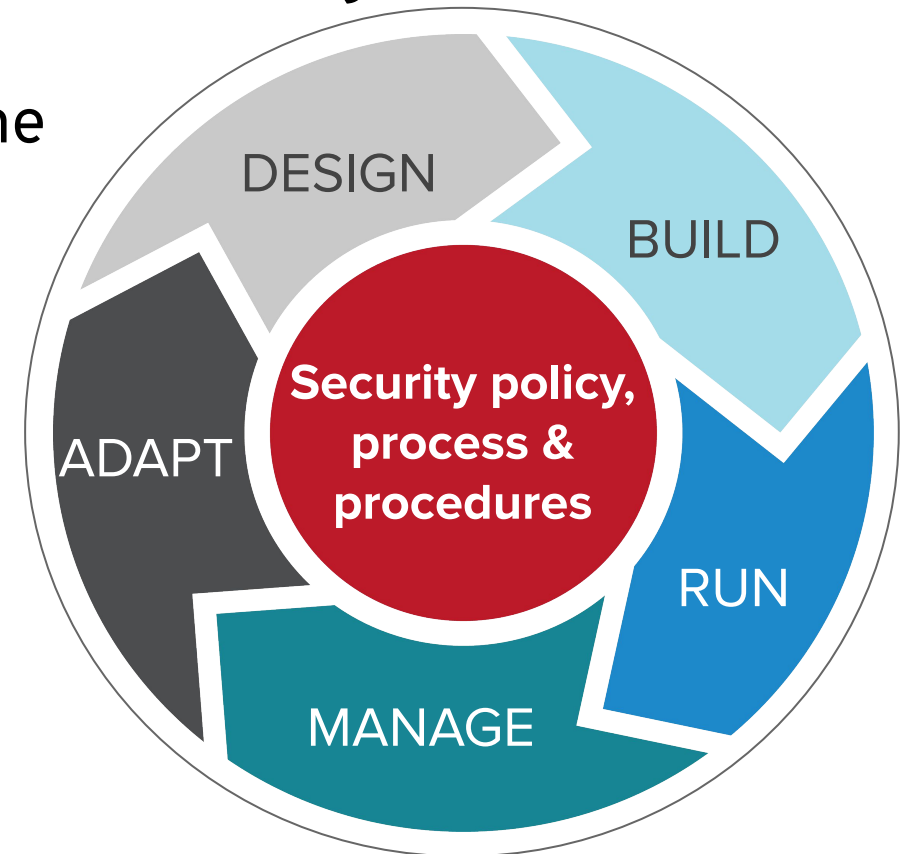
“...you could have missed the last two words out.” - me



DevOps and DevSecOps

“For 20 years, people have been leaving security till last” - colleague

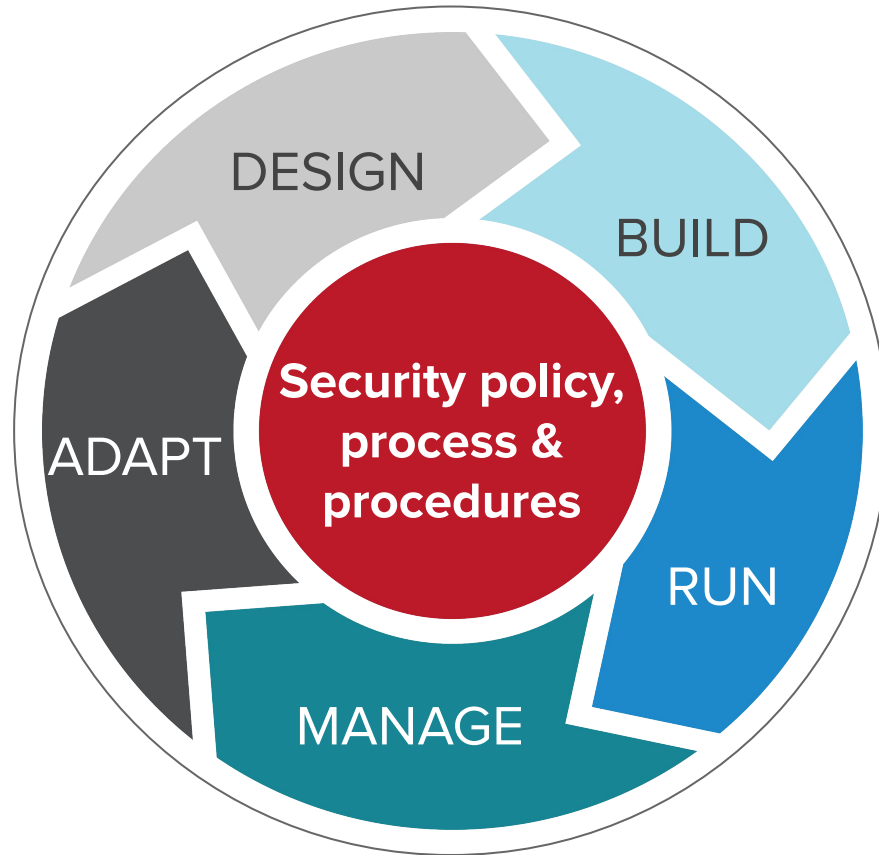
“...you could have missed the last two words out.” - me



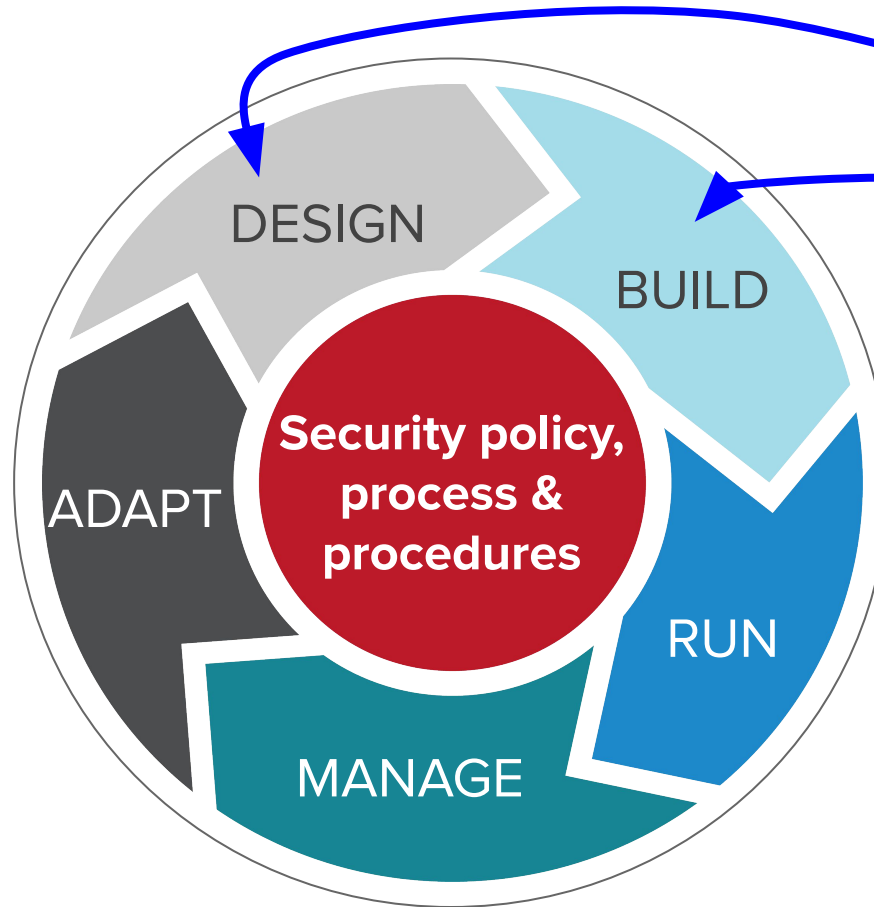
Example 1:

where the expertise lies

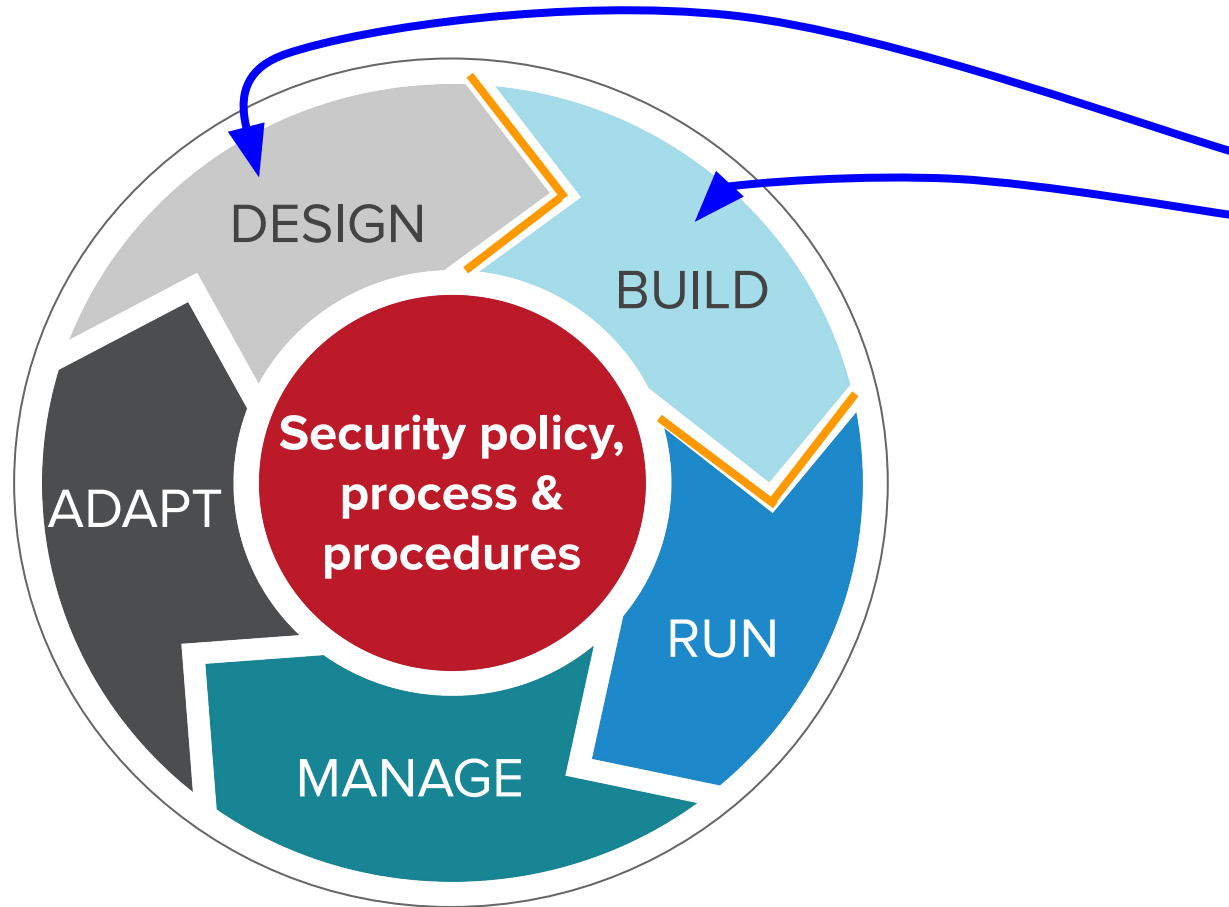
“Devs and shinies” (the Smaug problem)



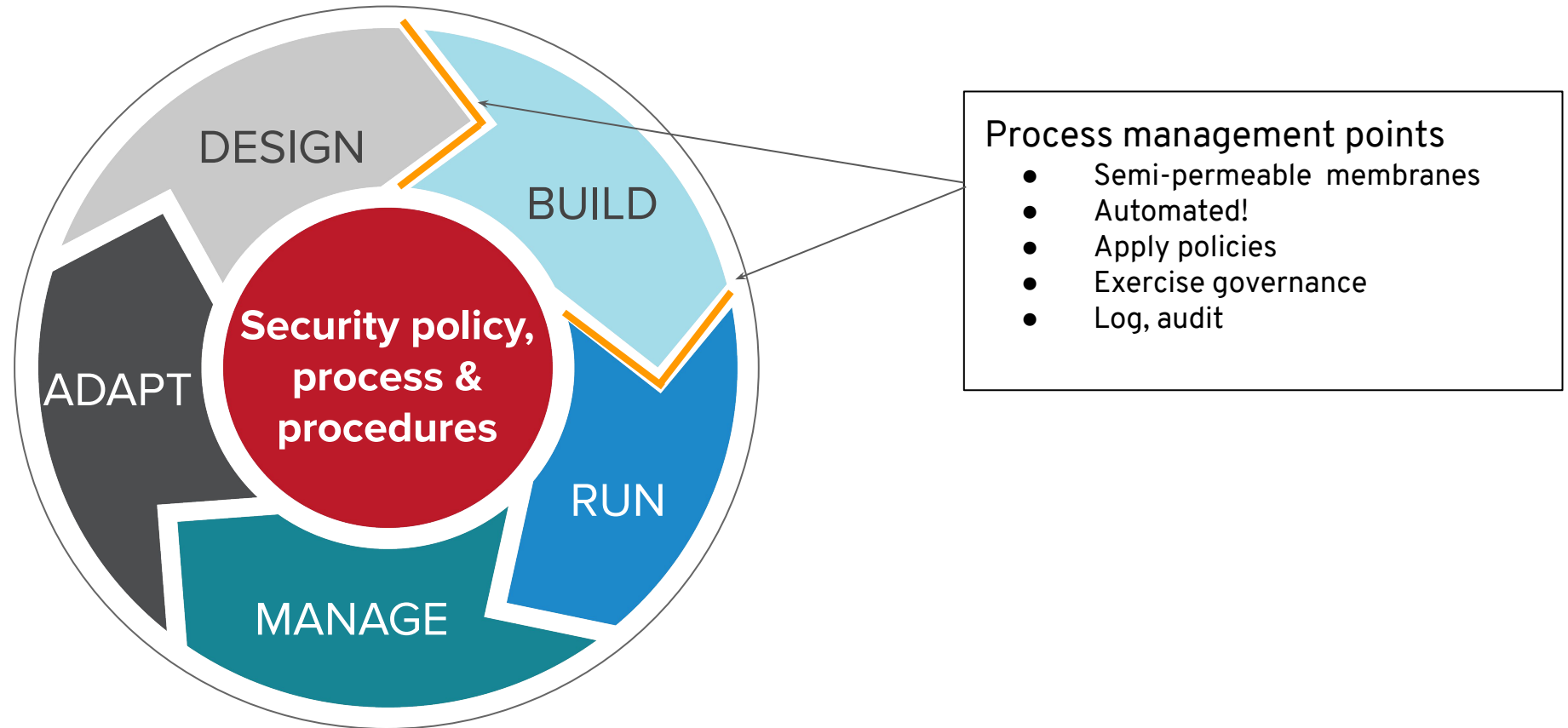
Steps in the process



Steps in the process



Steps in the process

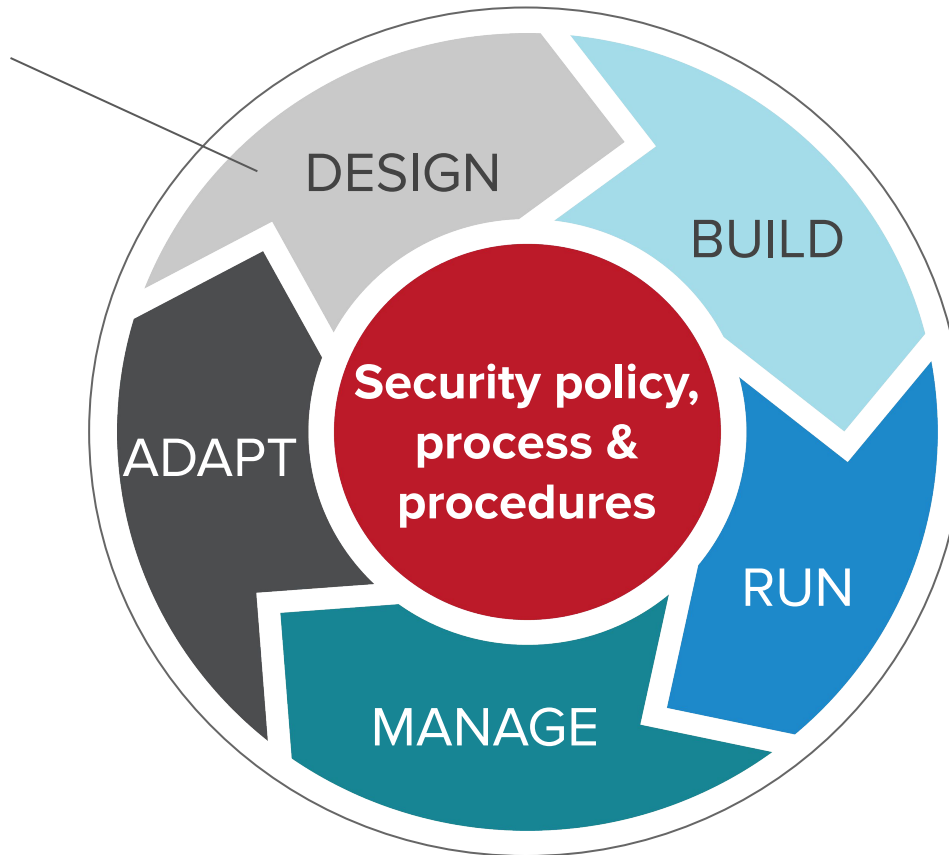


Example 2:

loving your inner auditor

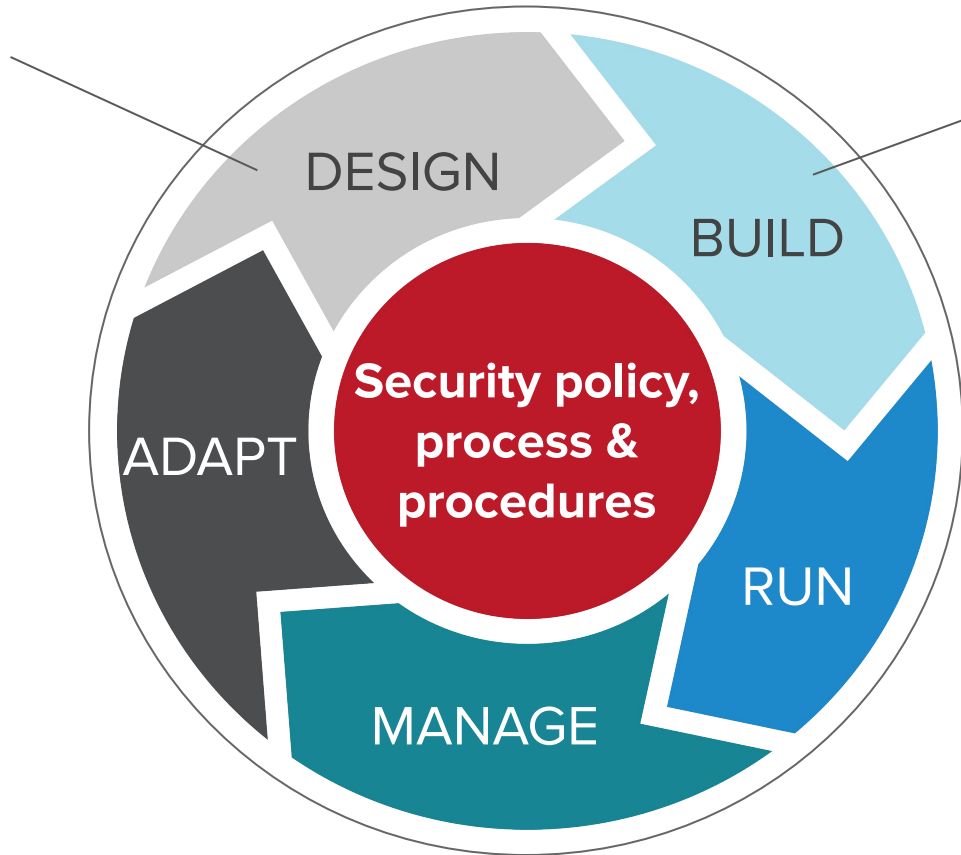
Steps in the process

Identify security requirements & governance models



Steps in the process

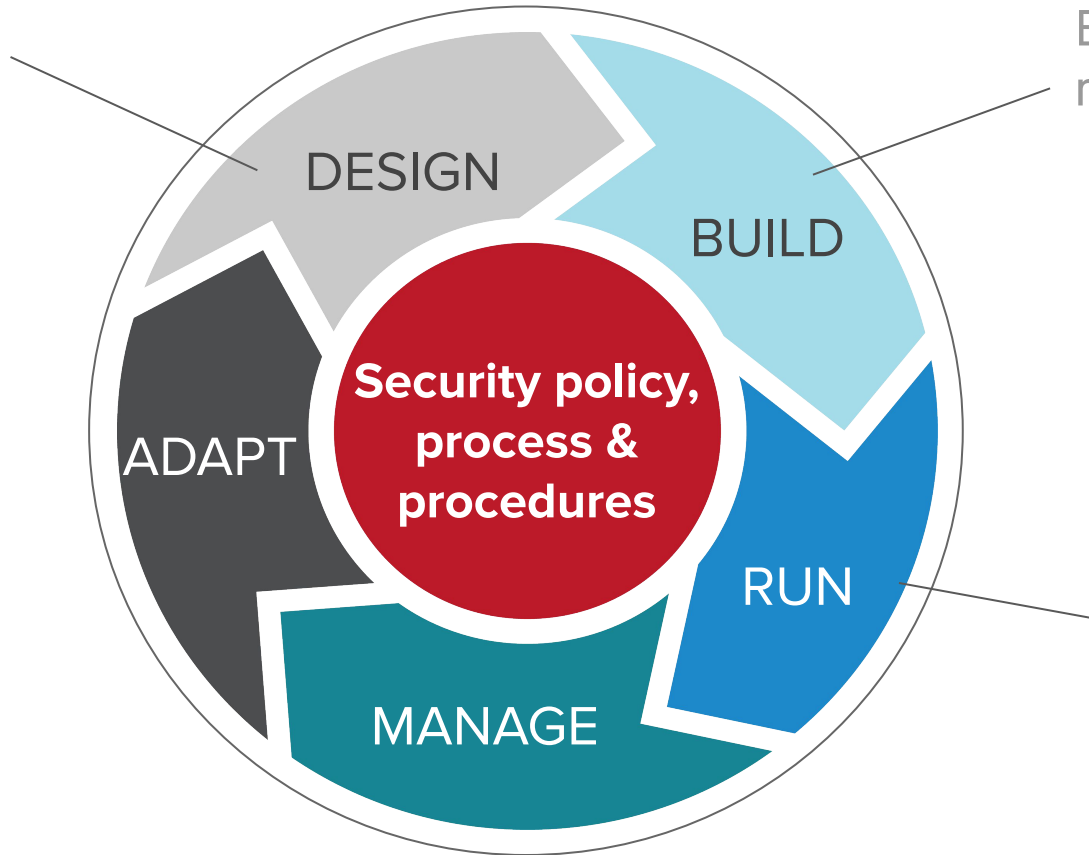
Identify security requirements & governance models



Built-in from the start;
not bolted on

Steps in the process

Identify security requirements & governance models

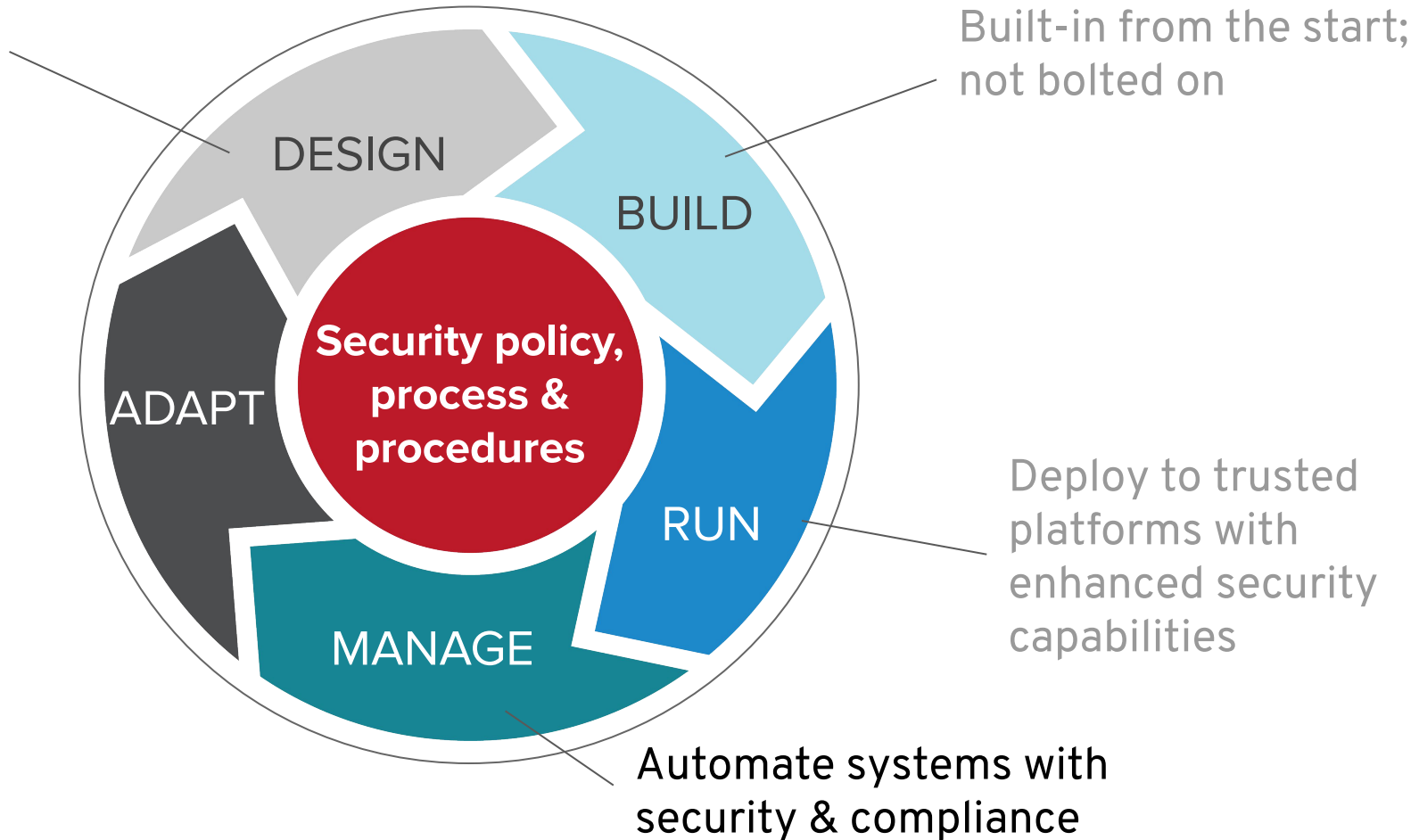


Built-in from the start; not bolted on

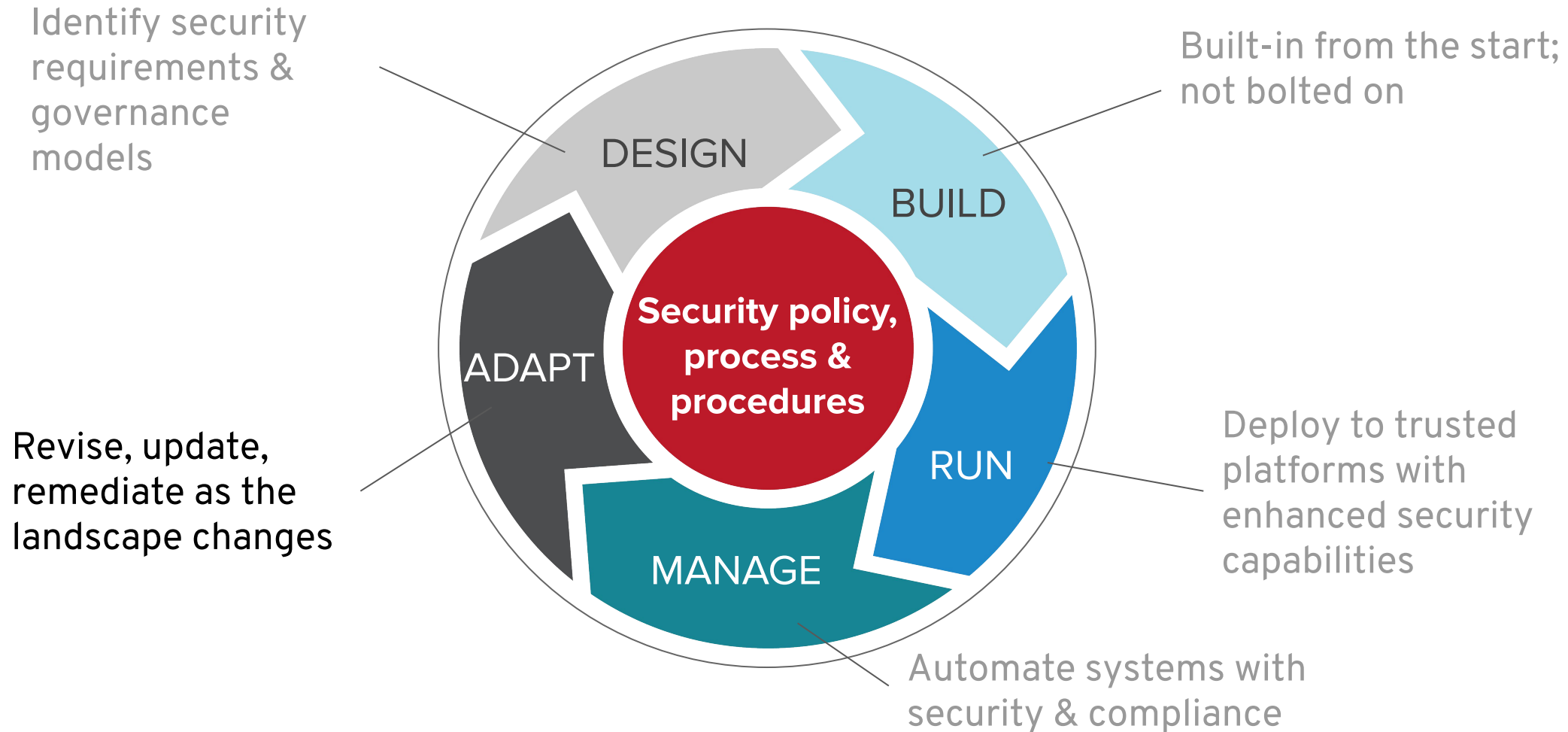
Deploy to trusted platforms with enhanced security capabilities

Steps in the process

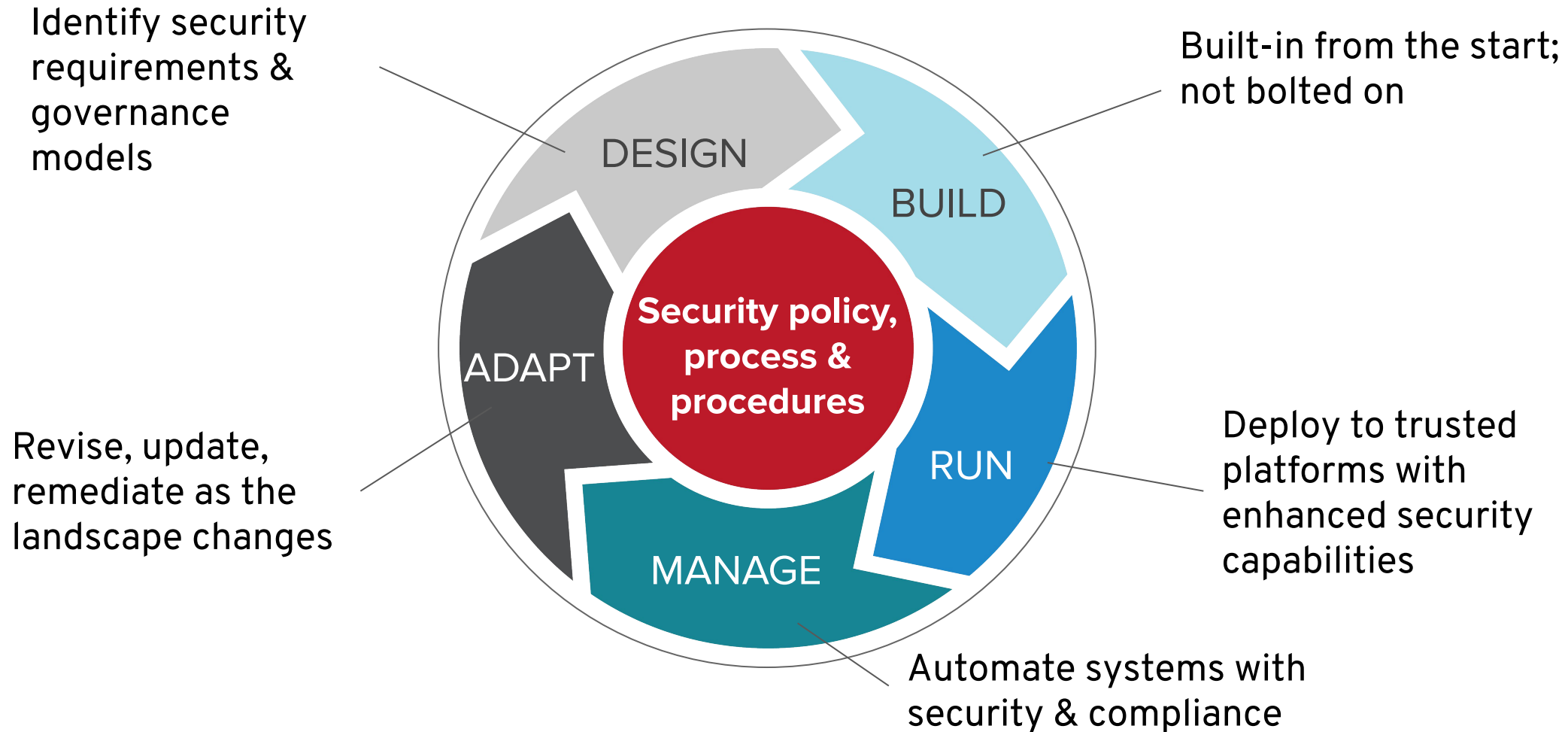
Identify security requirements & governance models



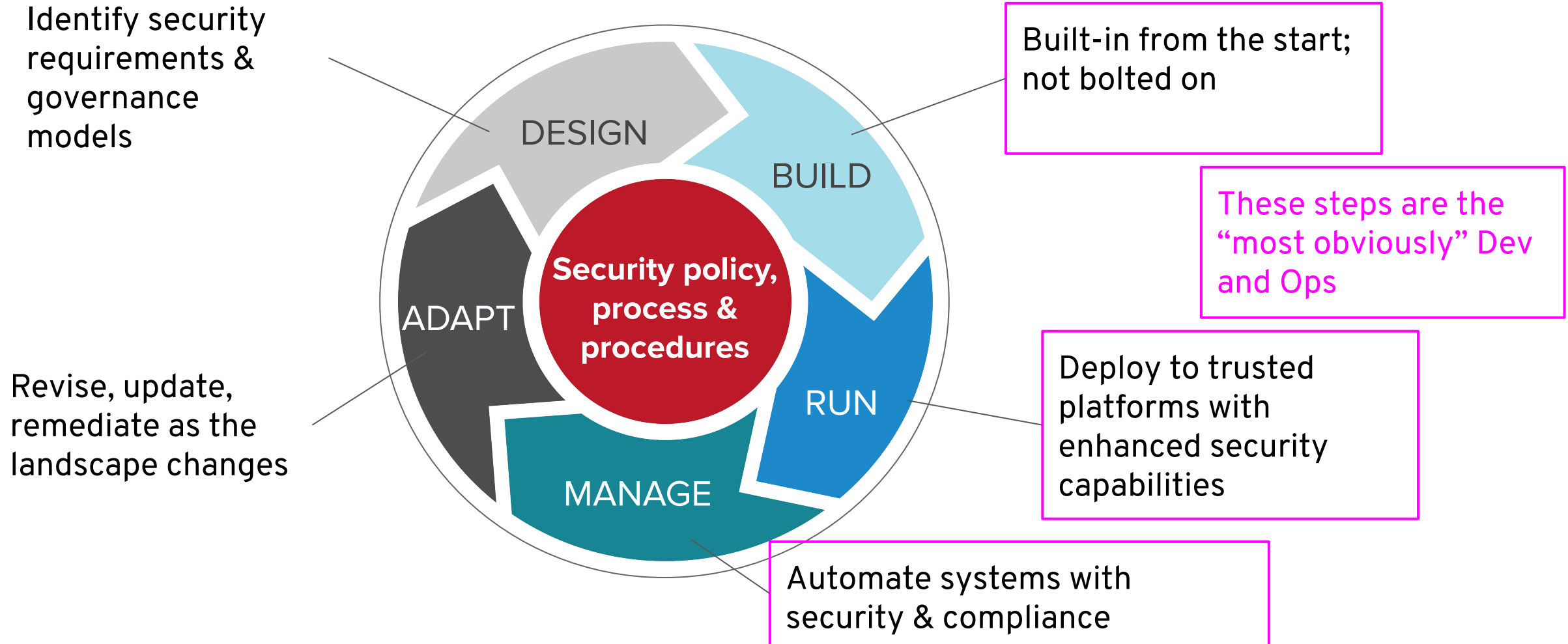
Steps in the process



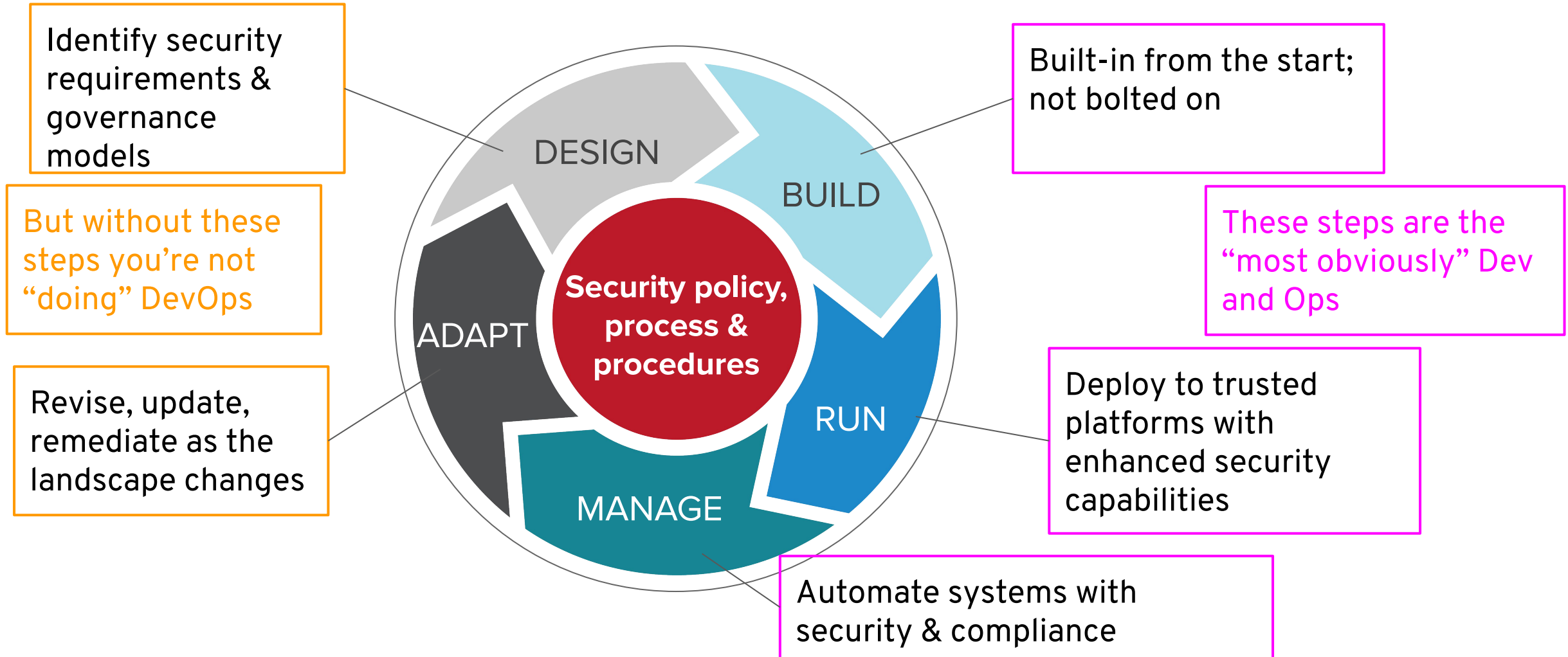
Steps in the process



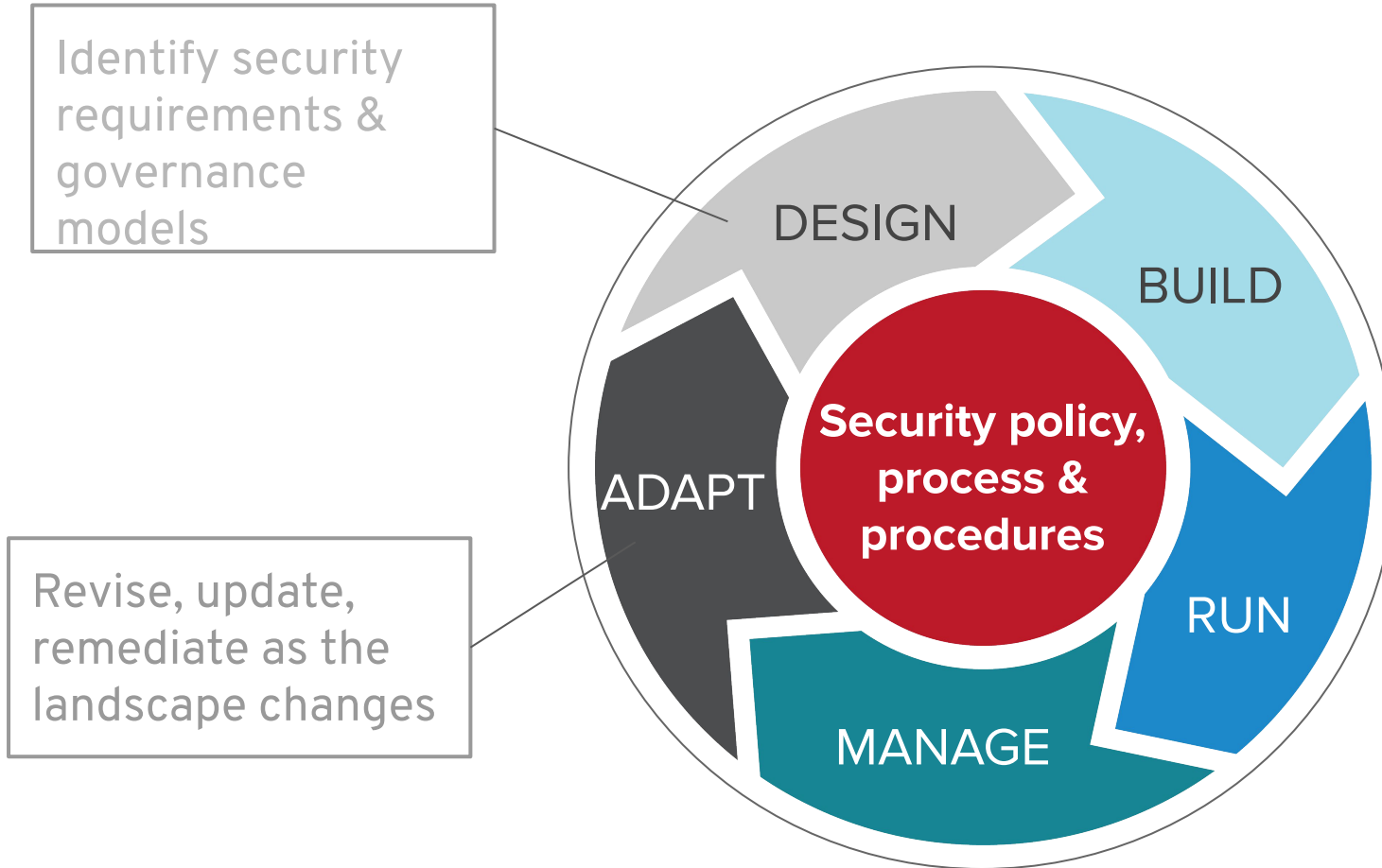
Steps in the process



Steps in the process

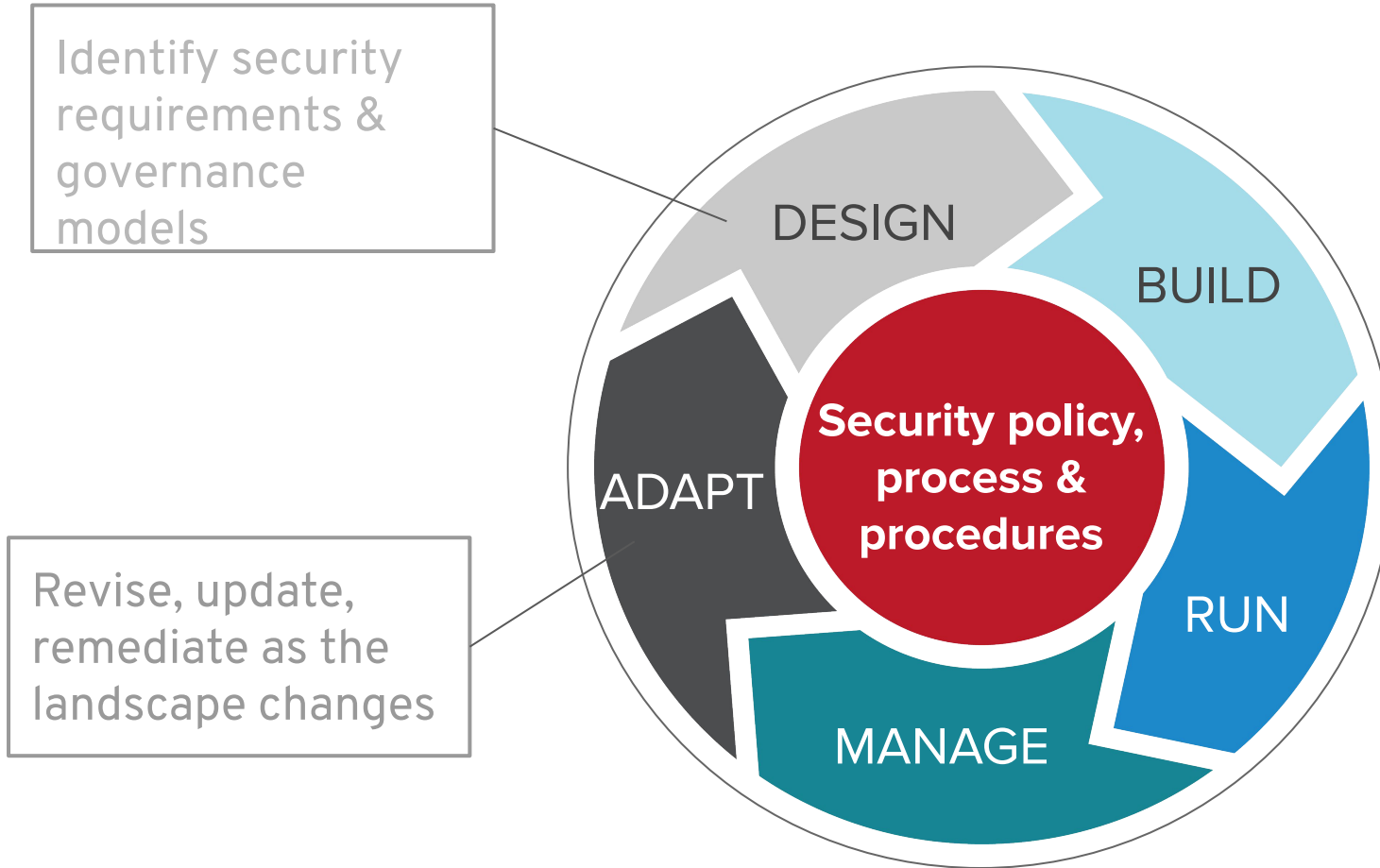


Steps in the process



Governance

Steps in the process

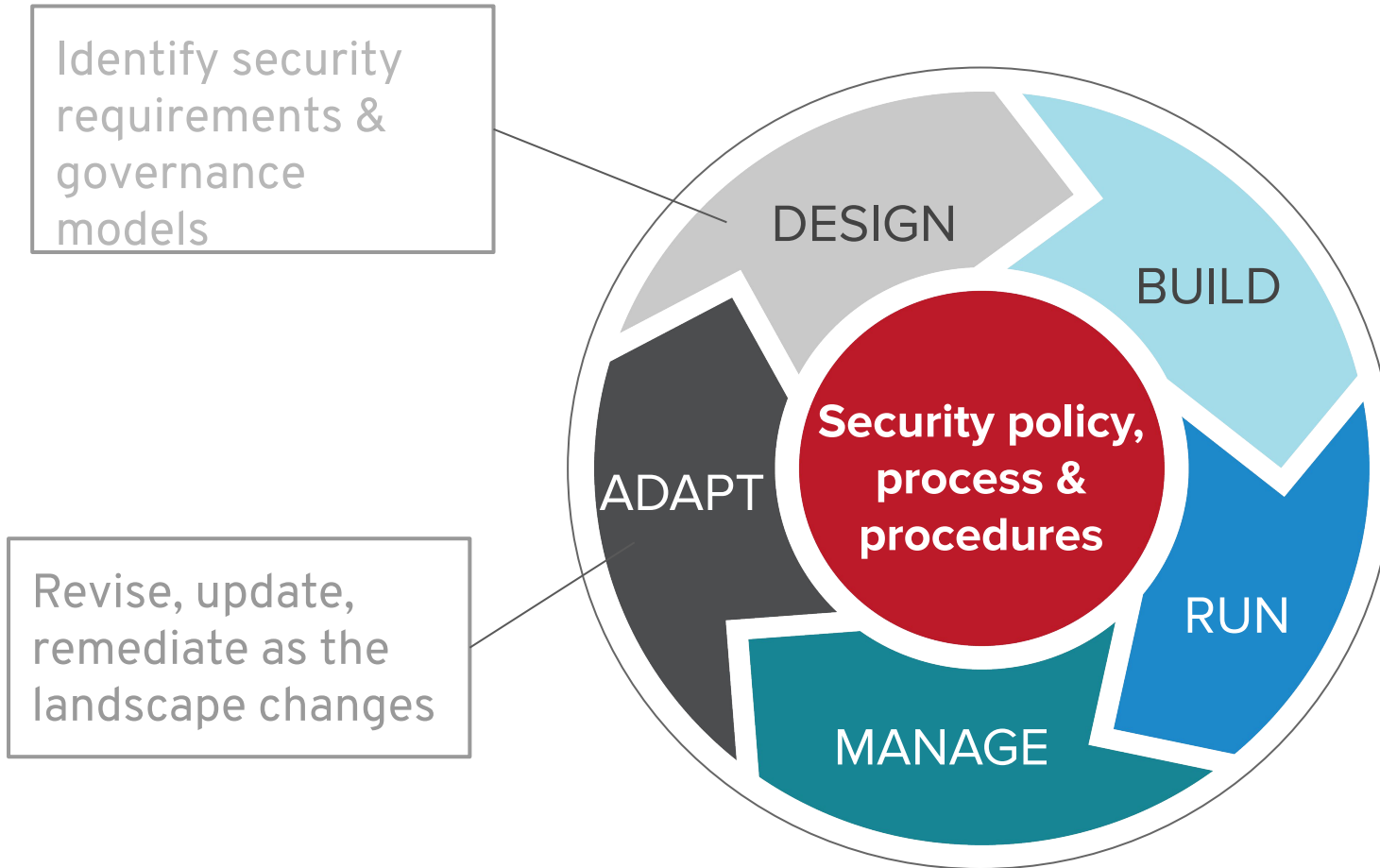


Governance



Policy

Steps in the process



Governance

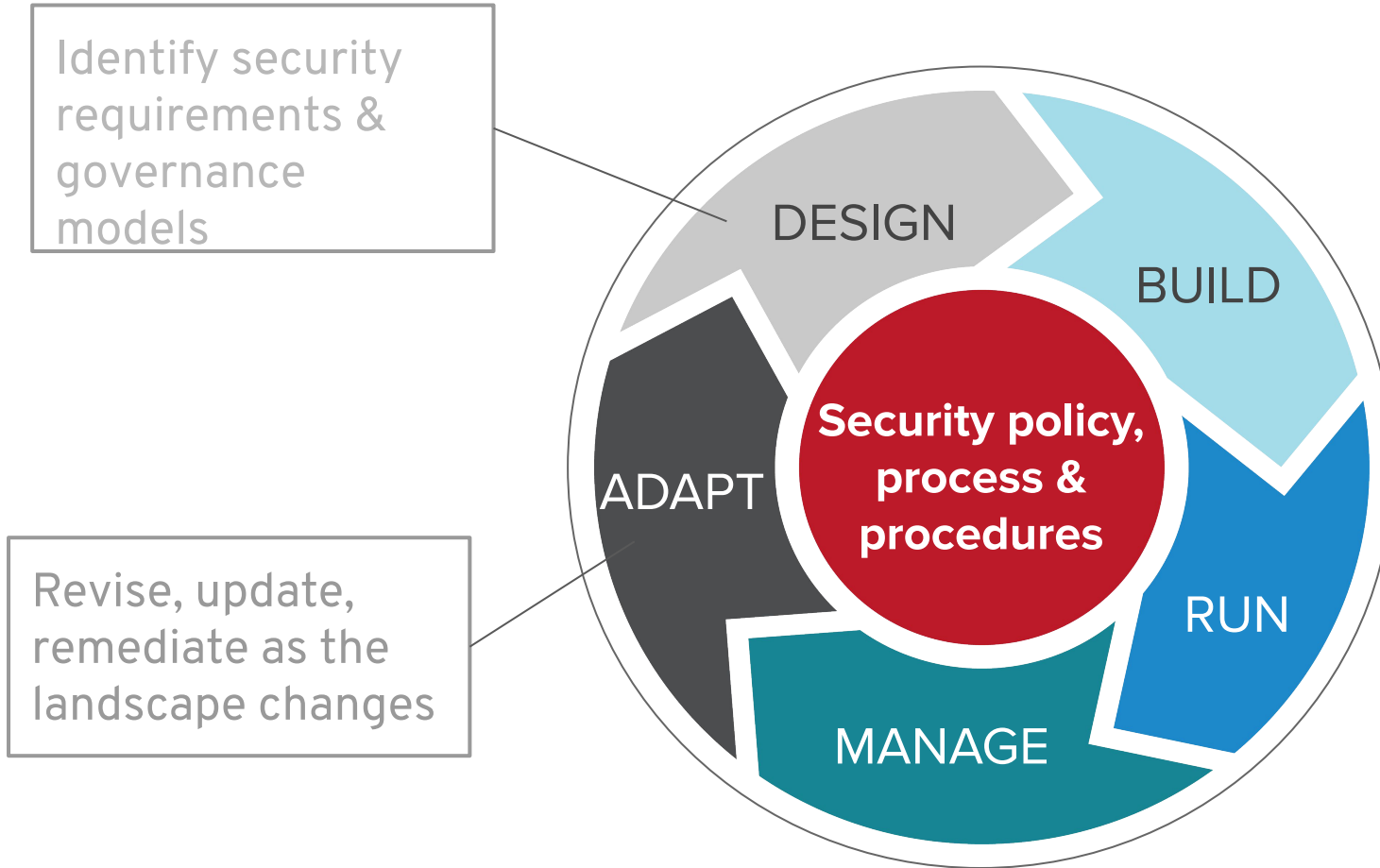


Policy



Process

Steps in the process



Governance



Policy

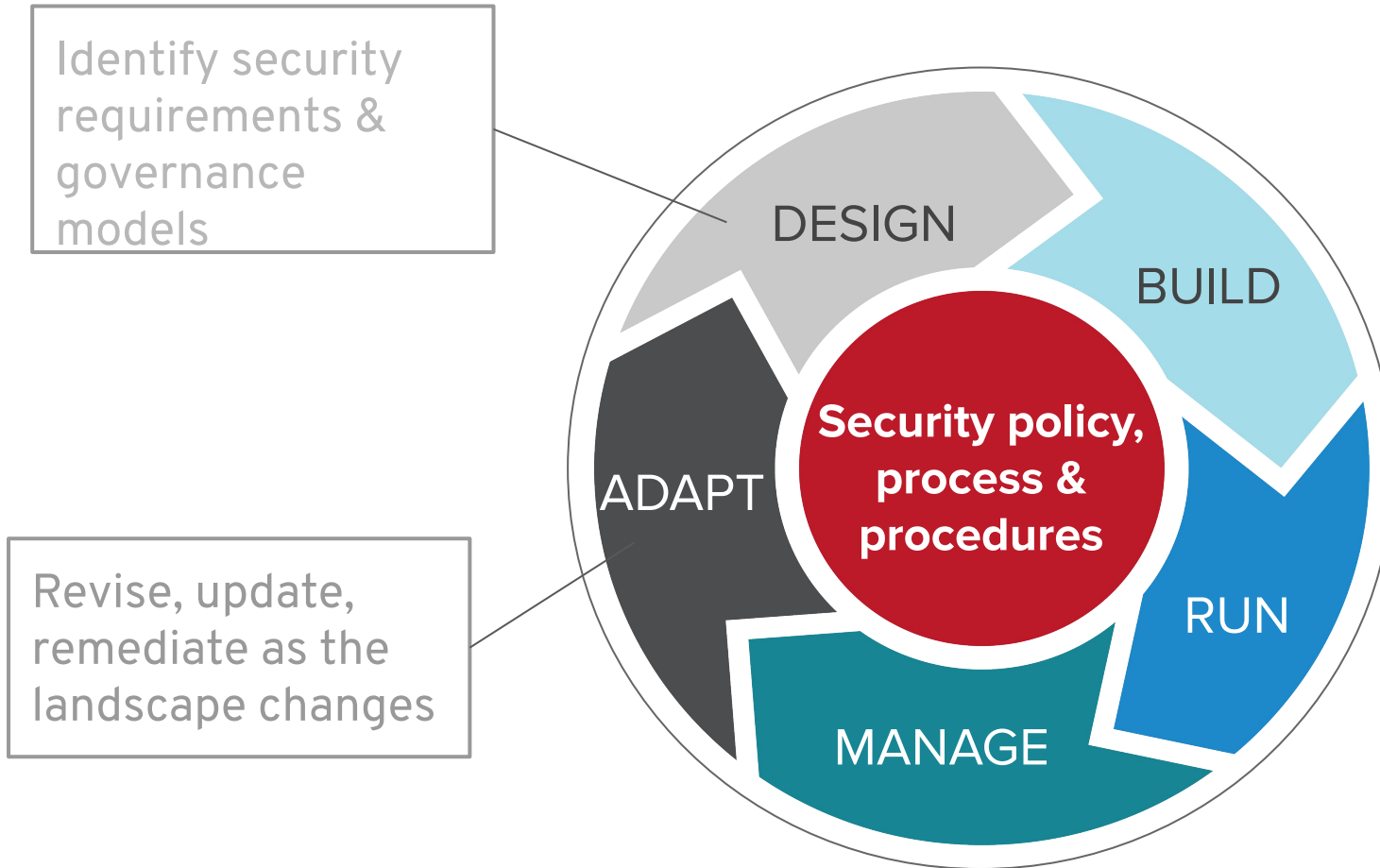


Process



Artefacts

Steps in the process



Governance



Policy



Process

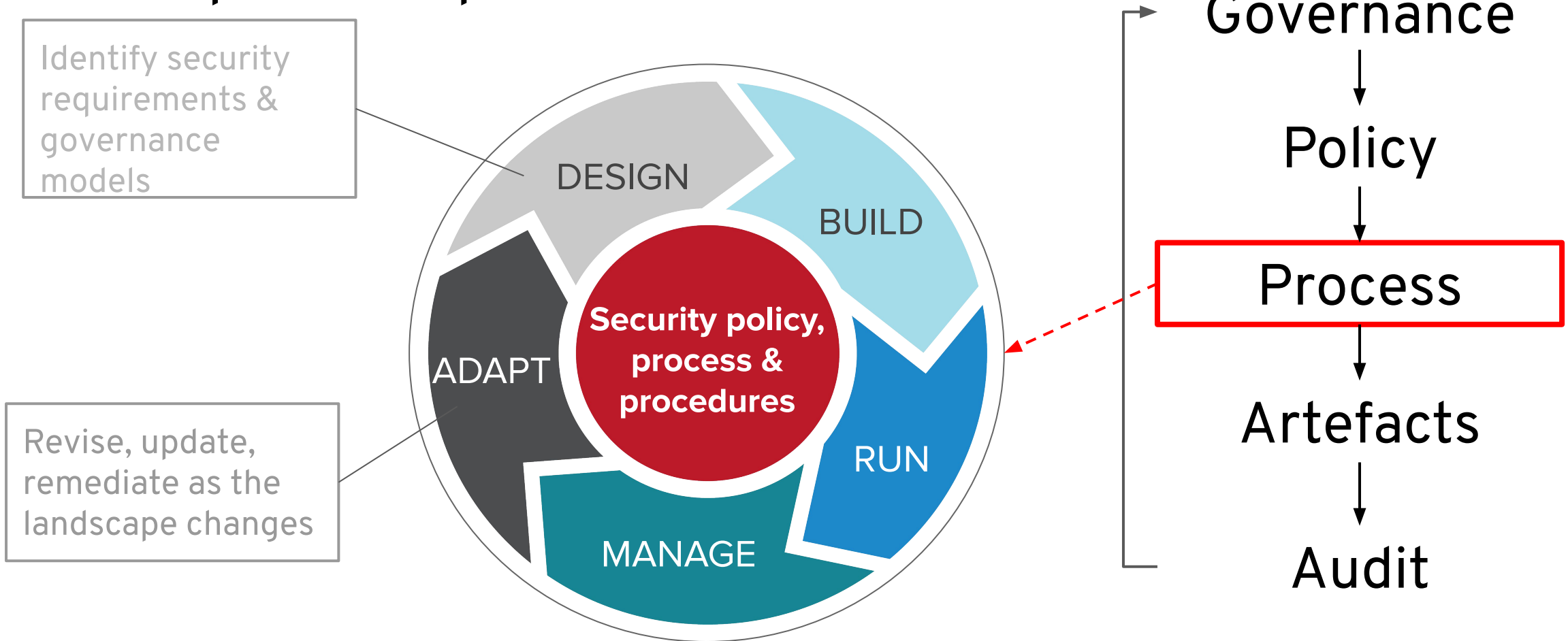


Artefacts



Audit

Steps in the process



Part II: process or culture?

Which is most important?

It's the culture (obviously)

It's the culture (obviously)

1. Get executive buy-in

It's the culture (obviously)

1. Get executive buy-in
2. Choose enthusiasts

It's the culture (obviously)

1. Get executive buy-in
2. Choose enthusiasts
3. Choose cross- functional team
 - (Security folks are people too!)

It's the culture (obviously)

1. Get executive buy-in
2. Choose enthusiasts
3. Choose cross- functional team
 - (Security folks are people too!)
4. Consider who might put obstacles in your way

Digression!

Digression - obstacles

Not invented here

- Fear of the unknown



Digression - obstacles

Not invented here

- Fear of the unknown

My domain

- Fear of loss of control



Digression - obstacles

Not invented here

- Fear of the unknown

My domain

- Fear of loss of control

Stuck in my ways

- Fear of the new



Digression - obstacles

Not invented here

- Fear of the unknown

My domain

- Fear of loss of control

Stuck in my ways

- Fear of the new

People managers

- Fear of loss of power



Digression - obstacles

Not invented here

- Fear of the unknown

My domain

- Fear of loss of control

Stuck in my ways

- Fear of the new

People managers

- Fear of loss of power

Commissioning managers

- Fear of loss of deadline



Digression - obstacles

Not invented here

- Fear of the unknown

My domain

- Fear of loss of control

Stuck in my ways

- Fear of the new

People managers

- Fear of loss of power

Commissioning managers

- Fear of loss of deadline

Unions

- Fear of lack of certainty



Digression - obstacles

Not invented here

- Fear of the unknown

My domain

- Fear of loss of control

Stuck in my ways

- Fear of the new

People managers

- Fear of loss of power

Commissioning managers

- Fear of loss of deadline

Unions

- Fear of lack of certainty



Back on track...

It's the culture (obviously)

1. Get executive buy-in
2. Choose enthusiasts
3. Choose cross- functional team
 - (Security folks are people too!)
4. Consider who might put obstacles in your way
5. Small feature sets per cycle

It's the culture (obviously)

1. Get executive buy-in
2. Choose enthusiasts
3. Choose cross- functional team
 - (Security folks are people too!)
4. Consider who might put obstacles in your way
5. Small feature sets per cycle
6. Expect to fail ... and then succeed

It's the culture (obviously)

1. Get executive buy-in
2. Choose enthusiasts
3. Choose cross- functional team
 - (Security folks are people too!)
4. Consider who might put obstacles in your way
5. Small feature sets per cycle
6. Expect to fail ... and then succeed



Summary

Summary

- DevOps allows and forces you to integrate security
 - It has to part of the story, because you can't bolt it on later
- Get the experts in
 - Allow responsibilities to live in the right places
- Plan for cultural change
 - Tools and processes *are* important too

Summary

- DevOps allows and forces you to integrate security
 - It has to part of the story, because you can't bolt it on later
- Get the experts in
 - Allow responsibilities to live in the right places
- Plan for cultural change
 - Tools and processes *are* important too

Q. But where's the definition of DevSecOps?

Summary

- DevOps allows and forces you to integrate security
 - It has to part of the story, because you can't bolt it on later
- Get the experts in
 - Allow responsibilities to live in the right places
- Plan for cultural change
 - Tools and processes *are* important too

Q. But where's the definition of DevSecOps?


A. There isn't one: it's a change in mindset.

Thank you


Blog: <https://aliceevebob.com/>

LinkedIn: <https://www.linkedin.com/in/mikebursell/>

Twitter: @MikeCamel

 [linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)

 [facebook.com/redhatinc](https://www.facebook.com/redhatinc)

 [youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)

 twitter.com/RedHat