OET405

Threat modelling to evaluate the security and resilience of your generative AI workloads

Atul Dambalkar

Senior Solutions Architect
AWS India

Ankush Agarwal

Solutions Architect
AWS India

What is a threat model?

SHOSTACK'S 4-QUESTION FRAME

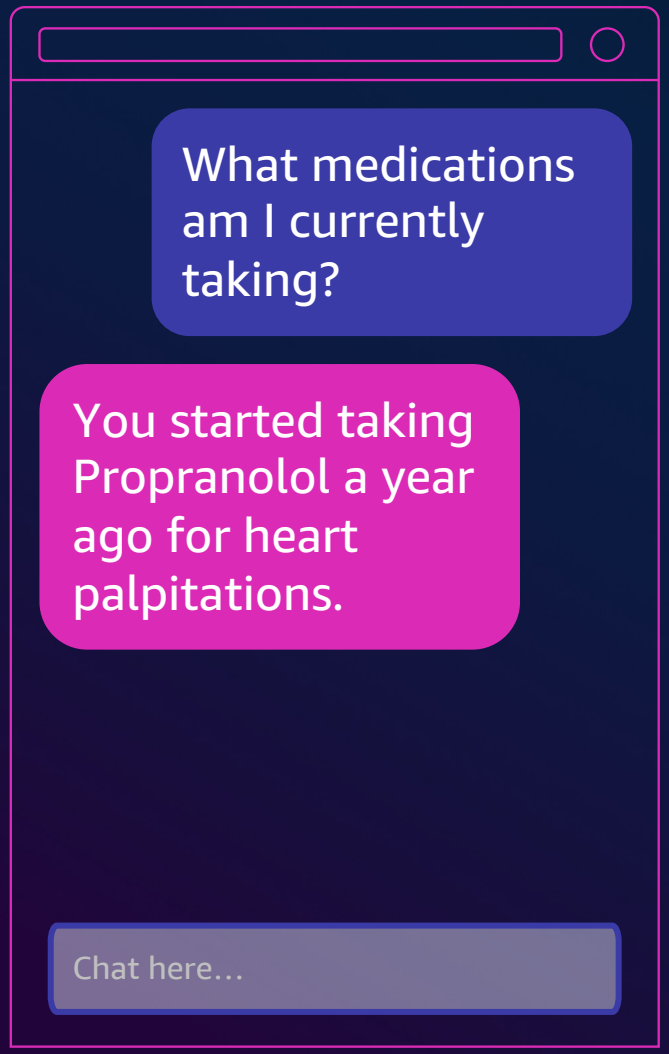
What are we working on?

What can go wrong?

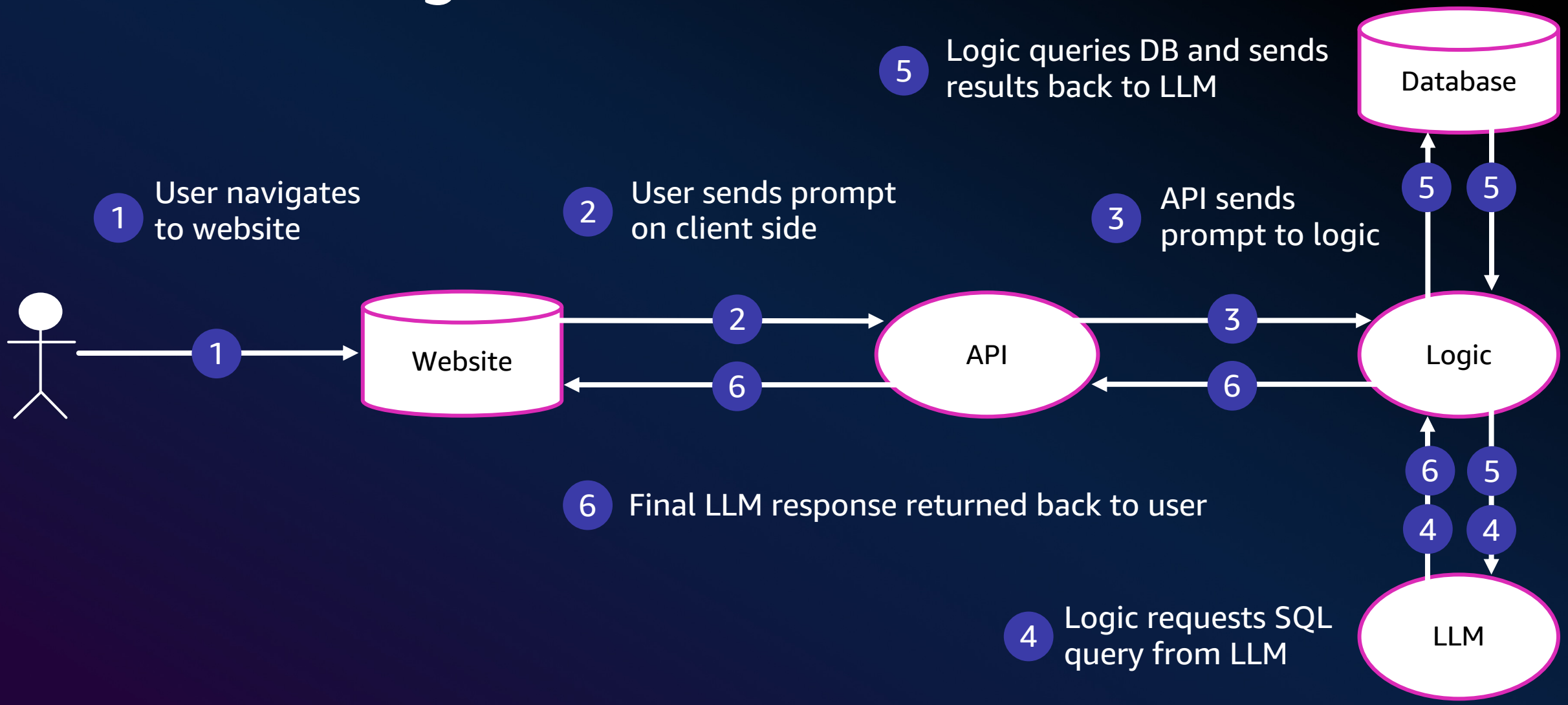
What are we going to do about it?

Did we do a good enough job?

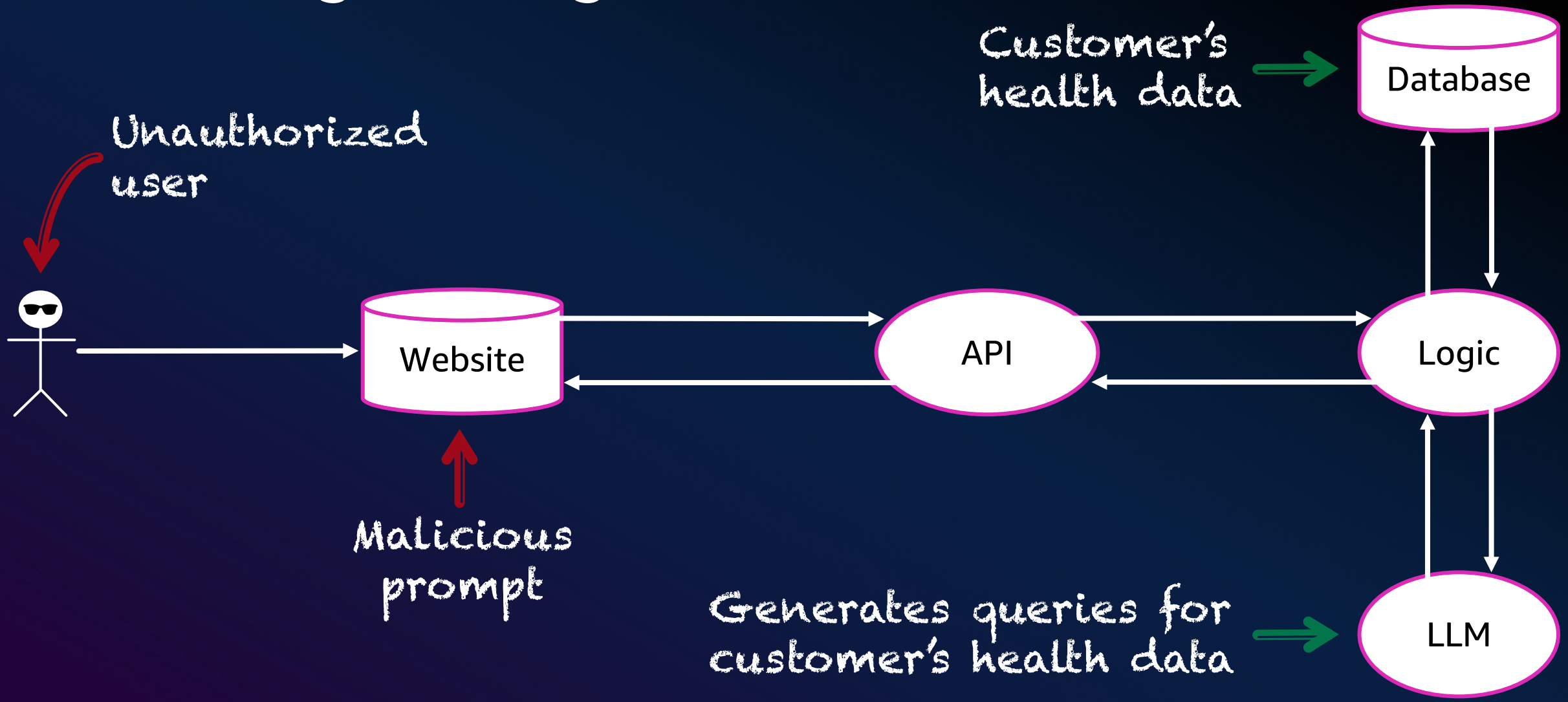
What are we working on?



Data flow diagram



What can go wrong?



Threat statement

→ A [threat source] with [pre-requisites],

can [threat action],

which leads to [threat impact] ,

negatively impacting [goal] of [impacted assets].

Threat statement

An external threat actor with access to the public facing application,

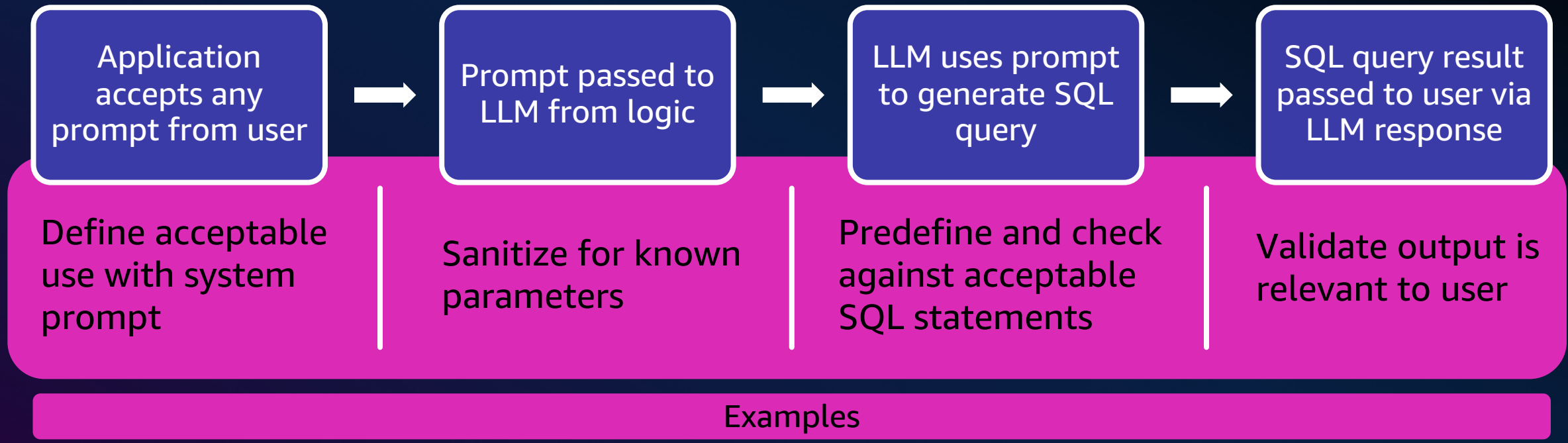
can inject malicious prompts which overwrite existing system prompts,

resulting in healthcare data from other patients being returned,

impacting the confidentiality of the data in the database.

Demo

Develop mitigations



Did we do a good enough job?

Verify Mitigations

Pentesting
- Per release
- Recurring

Automated Testing
- SAST/DAST

Validate Process

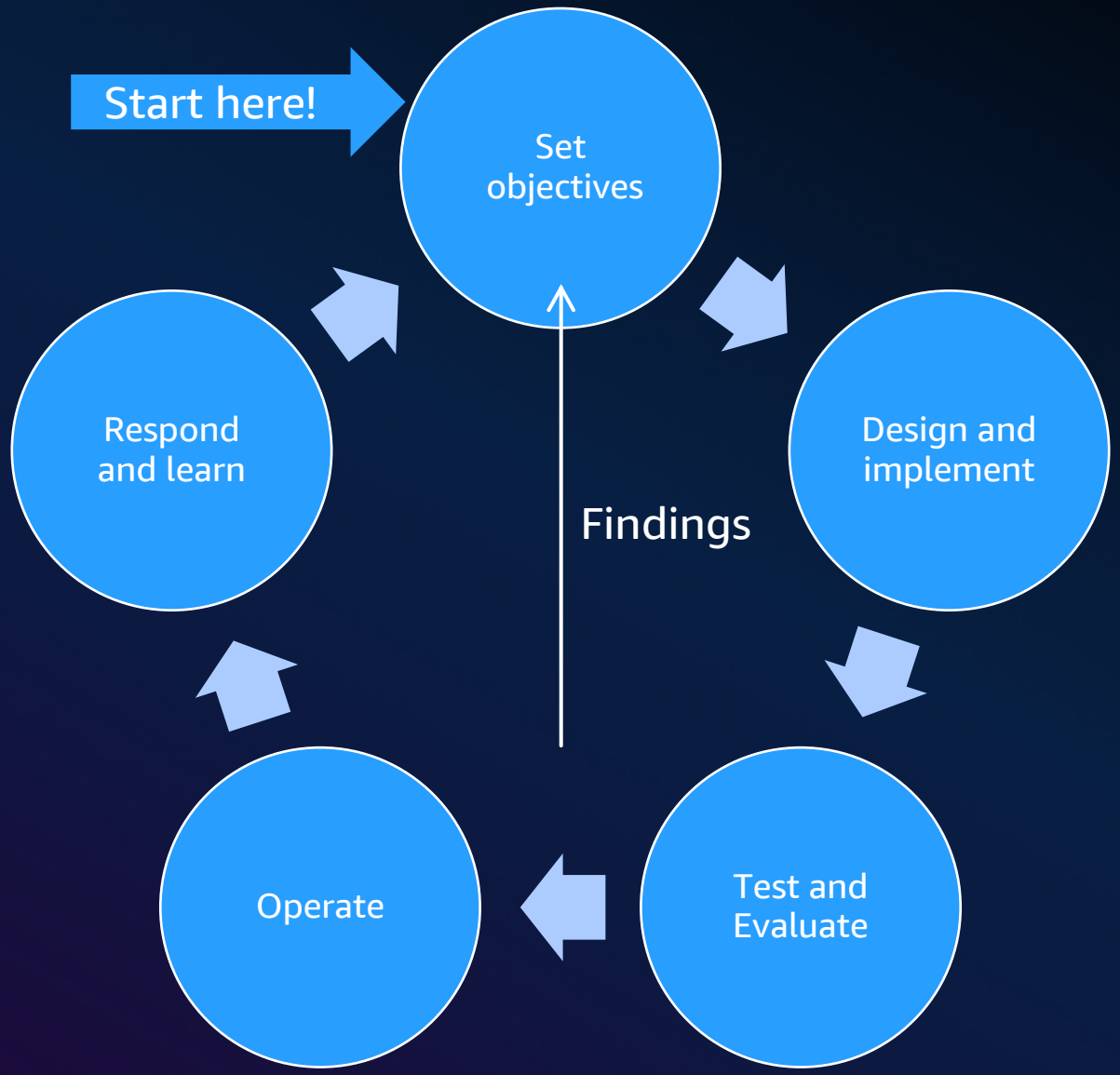
Compare
- Other threat frameworks

Review
- Accuracy
- Completeness
- Clarity

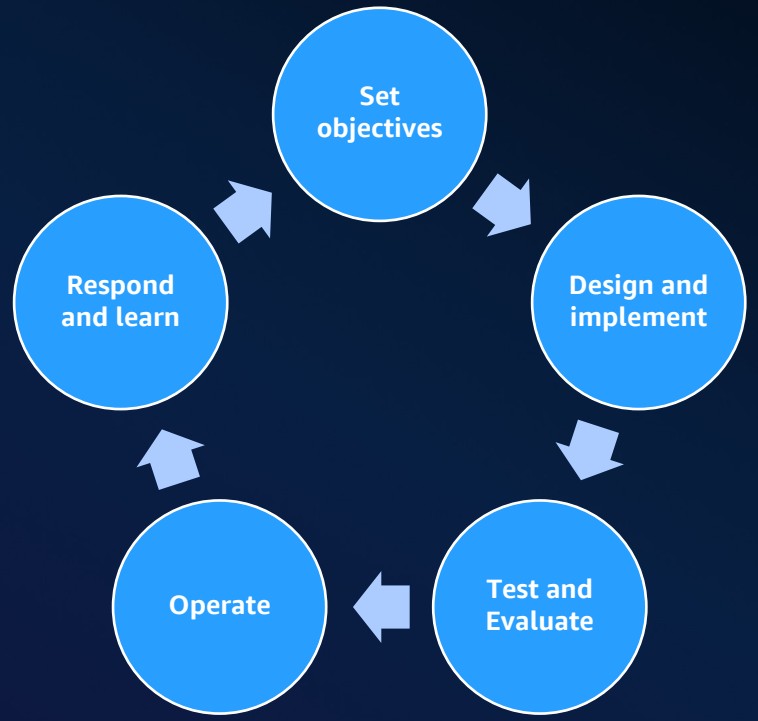
How can we operationalize and continuously improve resilience?

Foundational resilience  **Continuous resilience**

The resilience lifecycle



The resilience lifecycle – Key Outputs



Key outputs

- Identified priorities
- Better operational practices
- Learning/mitigation capabilities

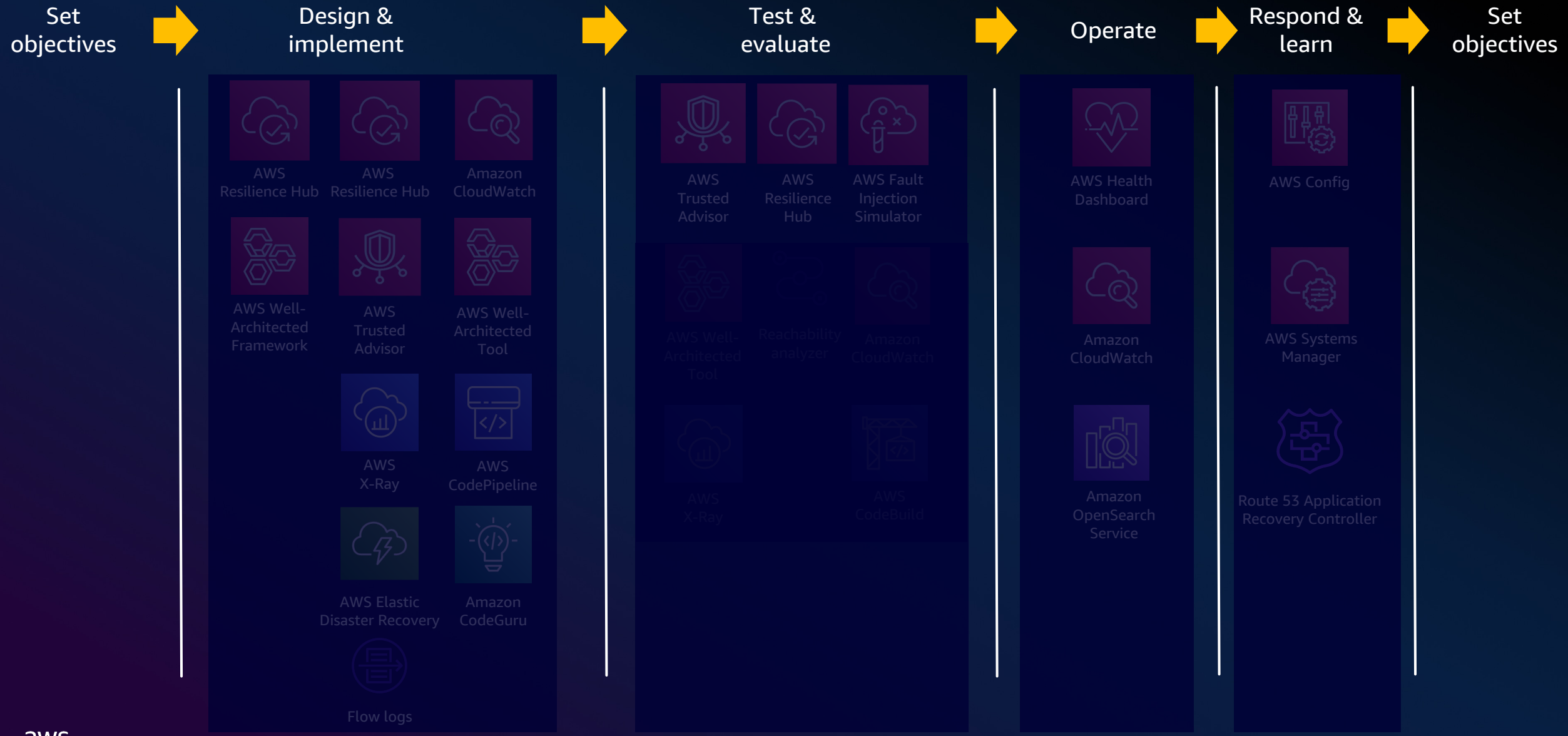
Practices at each step

Setting objectives

Workload prioritization and tiering

Objective metrics identification

AWS continuous resilience services



Design and implement

Architecture recommendation

Foundational resilience services and features

CI/CD

Logging

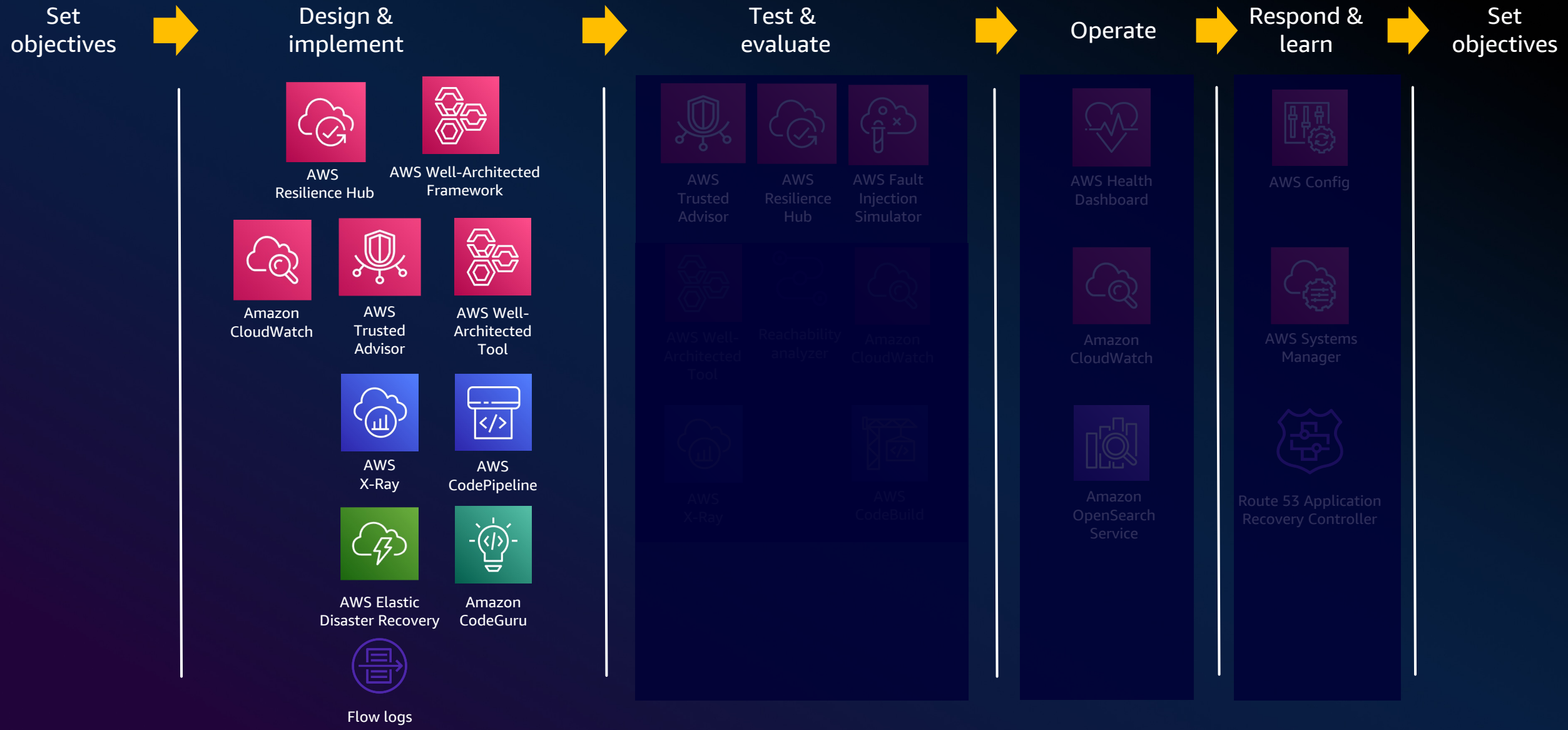
Dependency mapping

Code reviews and frameworks

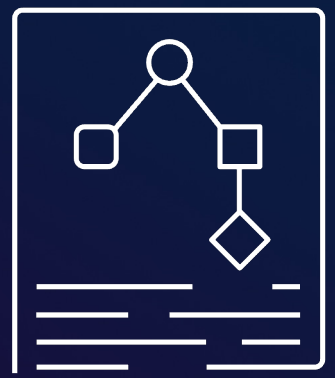
Backup and disaster recovery

Training

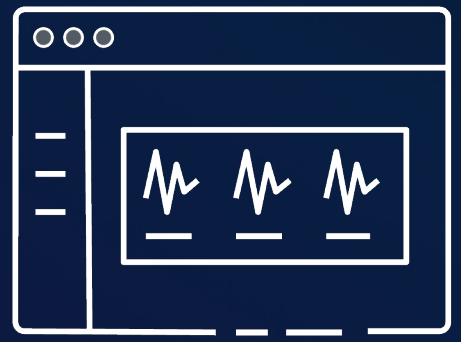
AWS continuous resilience services



Test and Evaluate



Tracing



Performance benchmarking

Fault injection and GameDays

Load testing

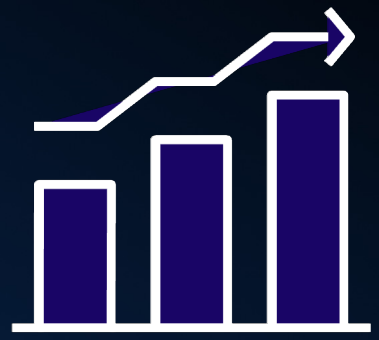
AWS continuous resilience services

Operate

Synthetic traffic

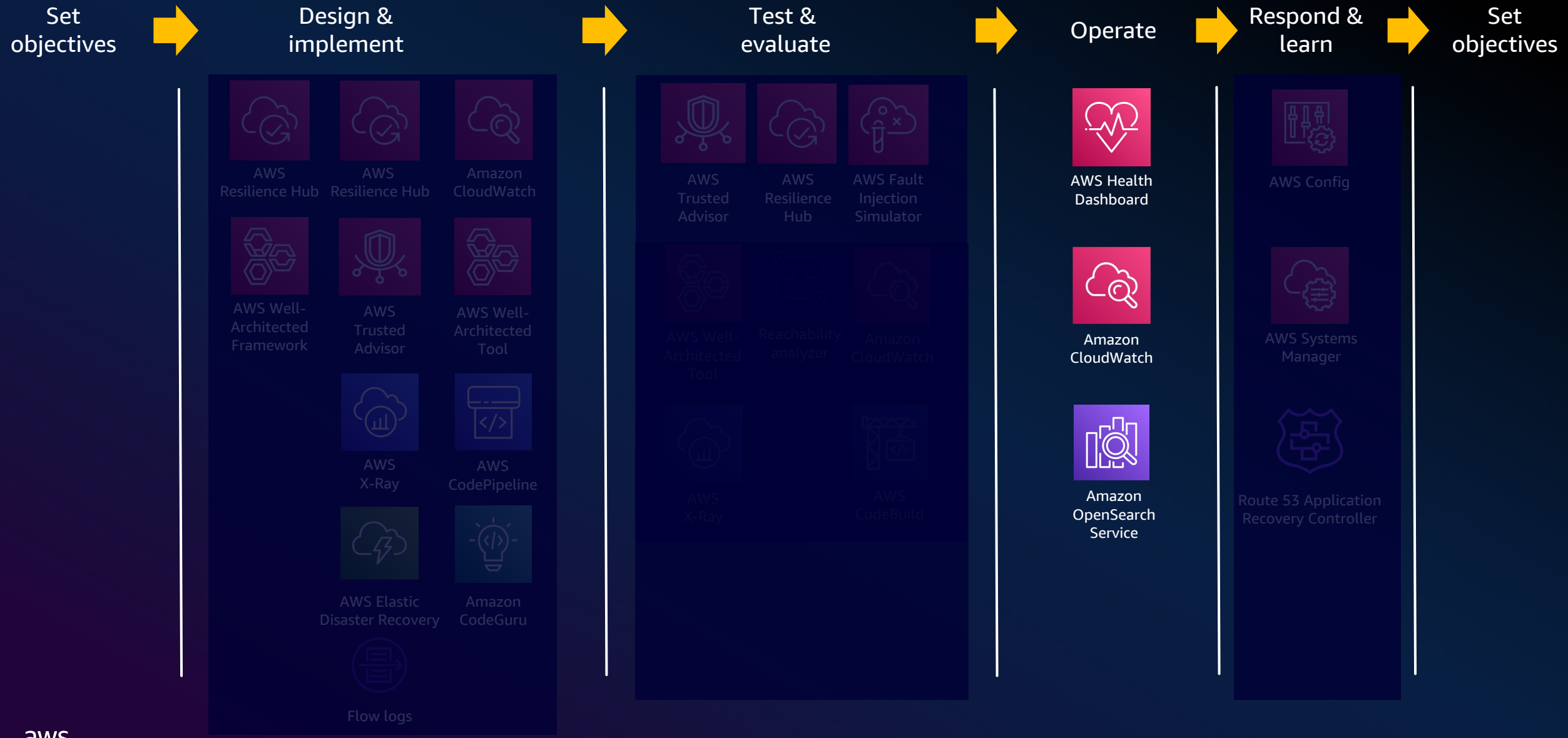
Alarming

Operational reviews



Load testing

AWS continuous resilience services



Respond and learn

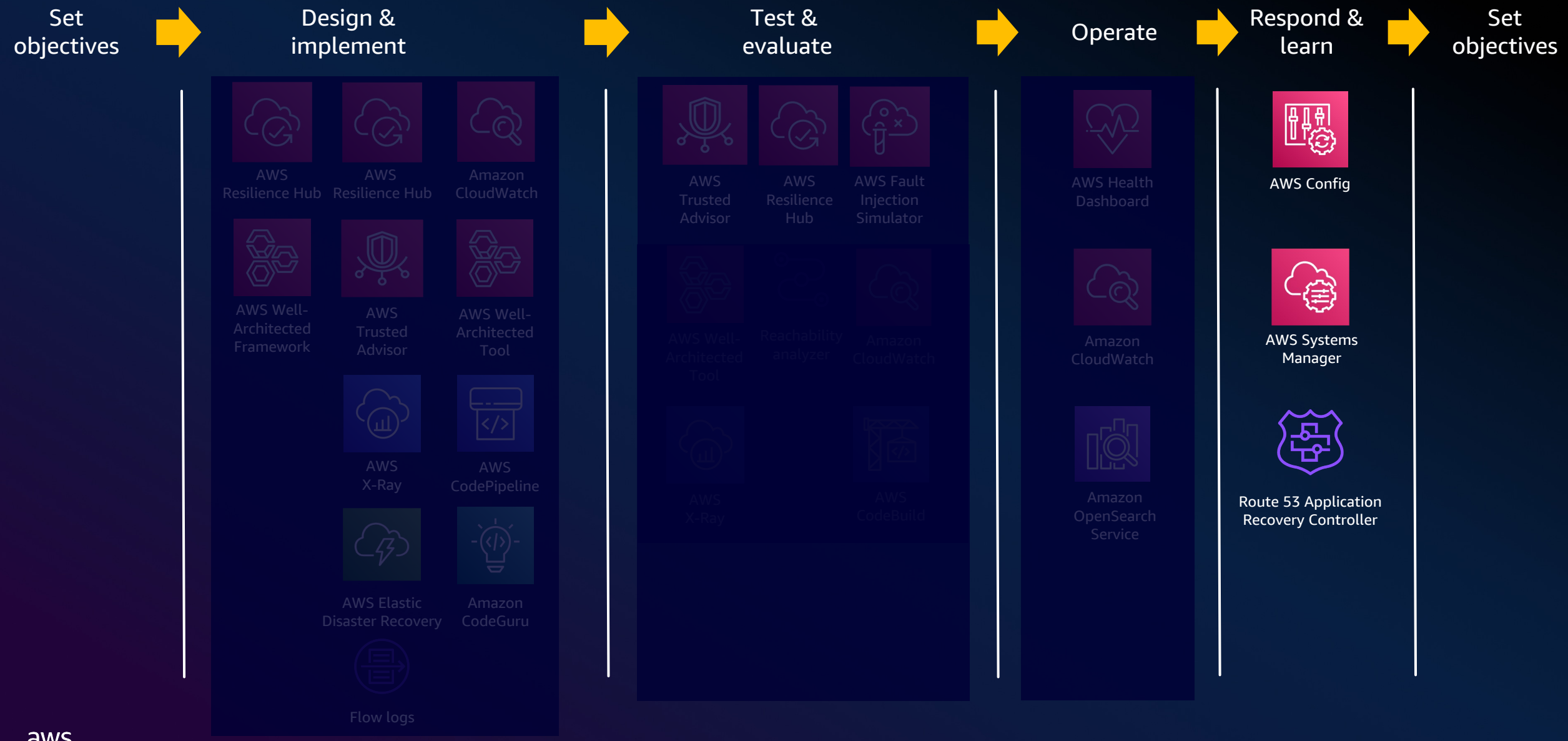
Auto remediation

Escalation paths

Event management

Correction of errors

AWS continuous resilience services



skillbuilder.aws

Build beyond

Redeem your free 7-day trial of AWS Skill Builder

Thank you!

Please complete the session survey in the mobile app

Atul Dambalkar

Senior Solutions Architect
AWS India

Ankush Agarwal

Solutions Architect
AWS India