



{Everything}-as-Code

an introduction to managing multiple Cloud Accounts
with Infrastructure-as-Code and CICD

Ross Wickman

Senior Principal Systems Engineer / GDIT
'Cloud Architect'

Tactful.Cloud

AWS CSA, Sec+, Net+, A+

A man with a beard and mustache, wearing a light blue button-down shirt and a brown and white striped tie, stands in front of a wall covered in papers and red string. He is holding a cigarette in his right hand and pointing with his left hand towards a document on the wall. The wall is cluttered with various papers, photos, and red string tied in a complex web. The man has a surprised or intense expression on his face. The background is a chaotic office environment with a shopping cart visible in the foreground.

Cloud Architecture

Define relationship(s) between components to accomplish business objective.

GENERAL DYNAMICS

Information Technology



FedRAMP
Governance
Standardized
A&A
Monitoring

NIST
ITL
800-53
IAM
Guidelines

DHS
NSA
US-CERT
FBI
InfraGard

FOUNDATION

Minutia

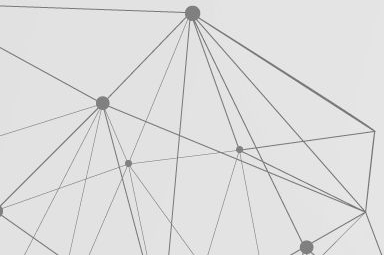
proof is in the puding

AWS

concepts for all CSPs

Git


assumes you know it...and are better than I





Multiple Account Configuration

Why you should. When to implement. What to do.


 AWS Organizations Acct



OAM

 Security & Logging

 IAM

 Enforcement

 Shared Resources

 Enterprise Infrastructure

 ACCT6

R&D

 Current Program Dev

 APP2 Dev

 APP3 Dev

 Sandbox

Production

 Current Program

 APP2

 APP3

Legacy

 Program Today

LANDING ZONES

Because AWS said so.
re:Invent 2018
Control Tower & Orgs

01

SHARED SERVICES

Single location management
Configure once for multiple uses

02

SECURITY

Auditing best practice
Keep log integrity

03

WHY

04

BILLING

Tagging can only go so far
Cap and track spending per
division or project

05

ISOLATION

Eliminate or significantly
minimize blast radius

06

RECOVERY

Limit the downtime of
resources

AWS Multi-account Strategy: rwick.it/AWS-MAS

WHEN



FEDERATION

Access control
One-to-many
Many-to-many roles
SSO
Credentials

Centralized management and
deployment of approved resources
and services

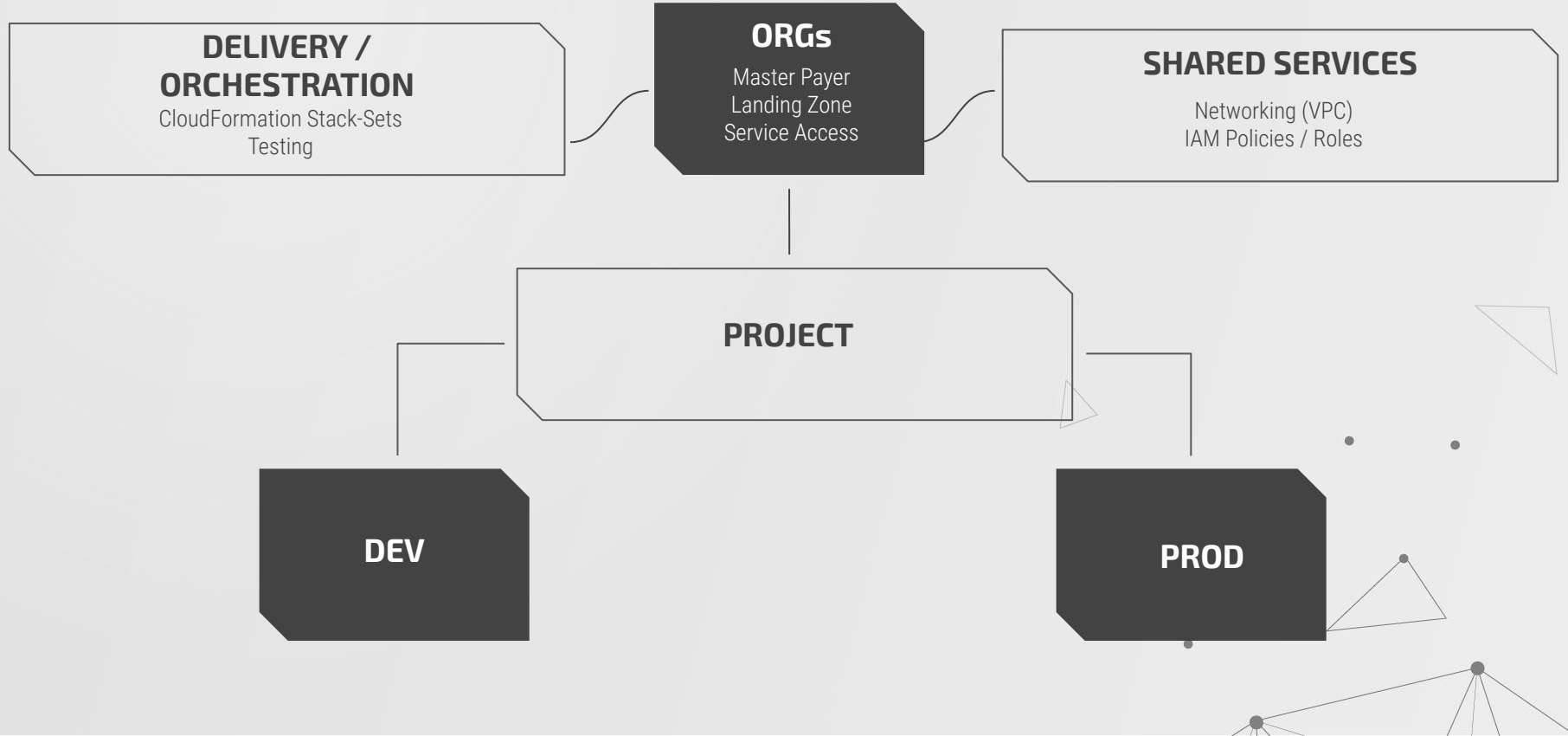
BASELINE



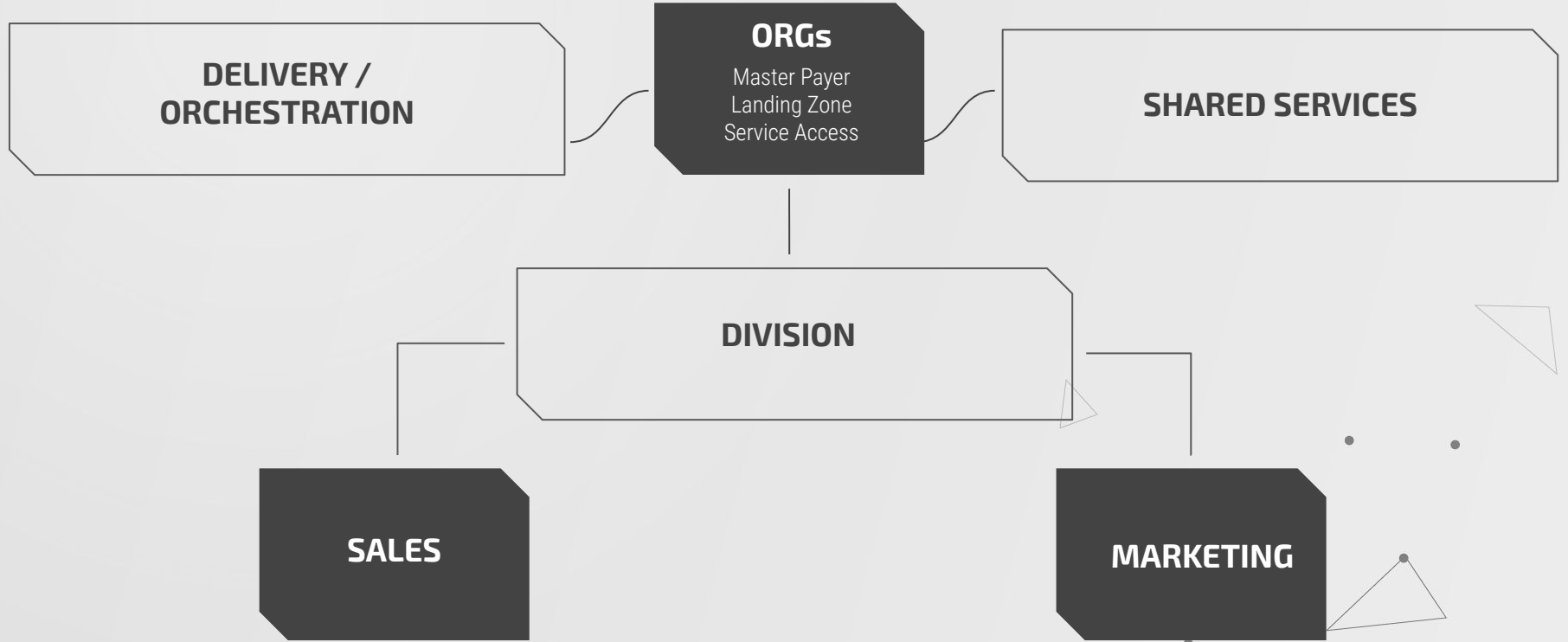
LOGGING

Archive for official records
HIPAA / PCI Compliance
Security Audit

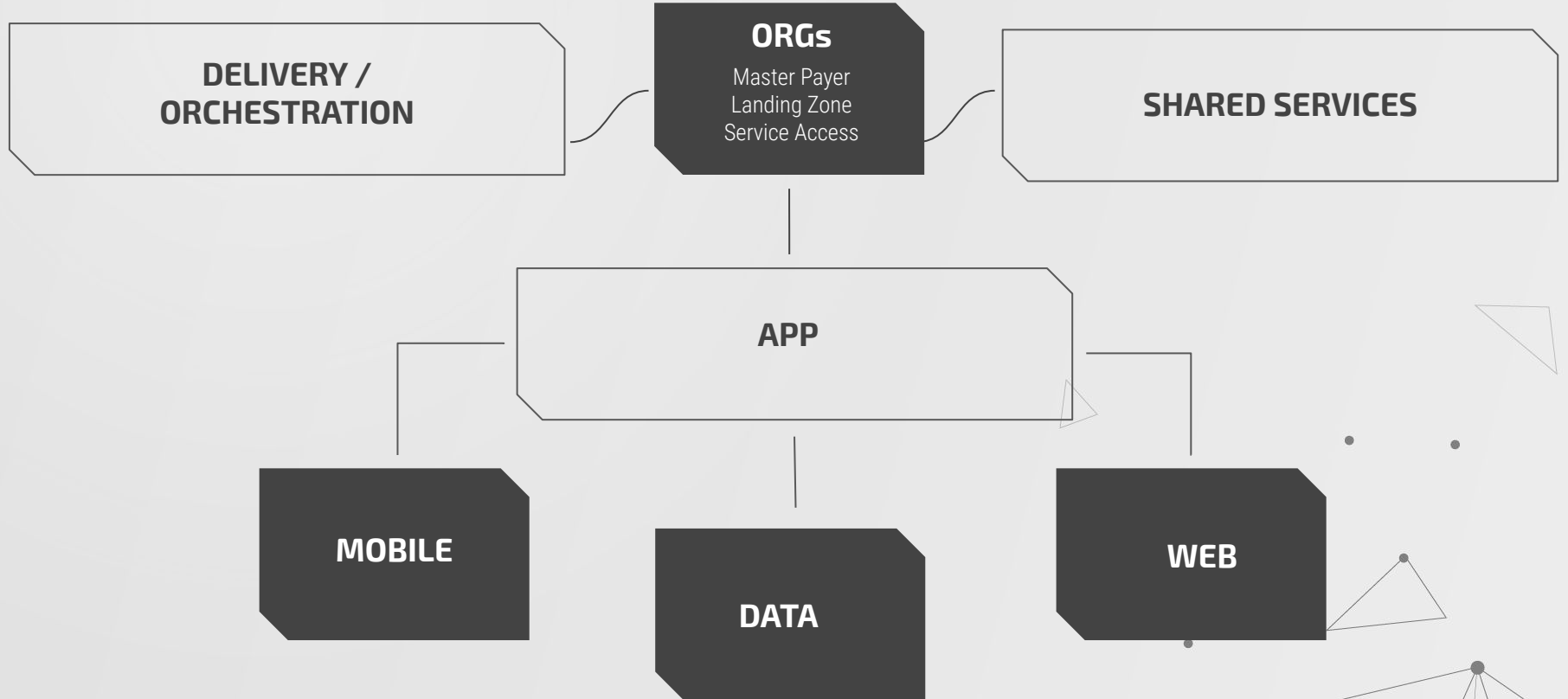
WHAT



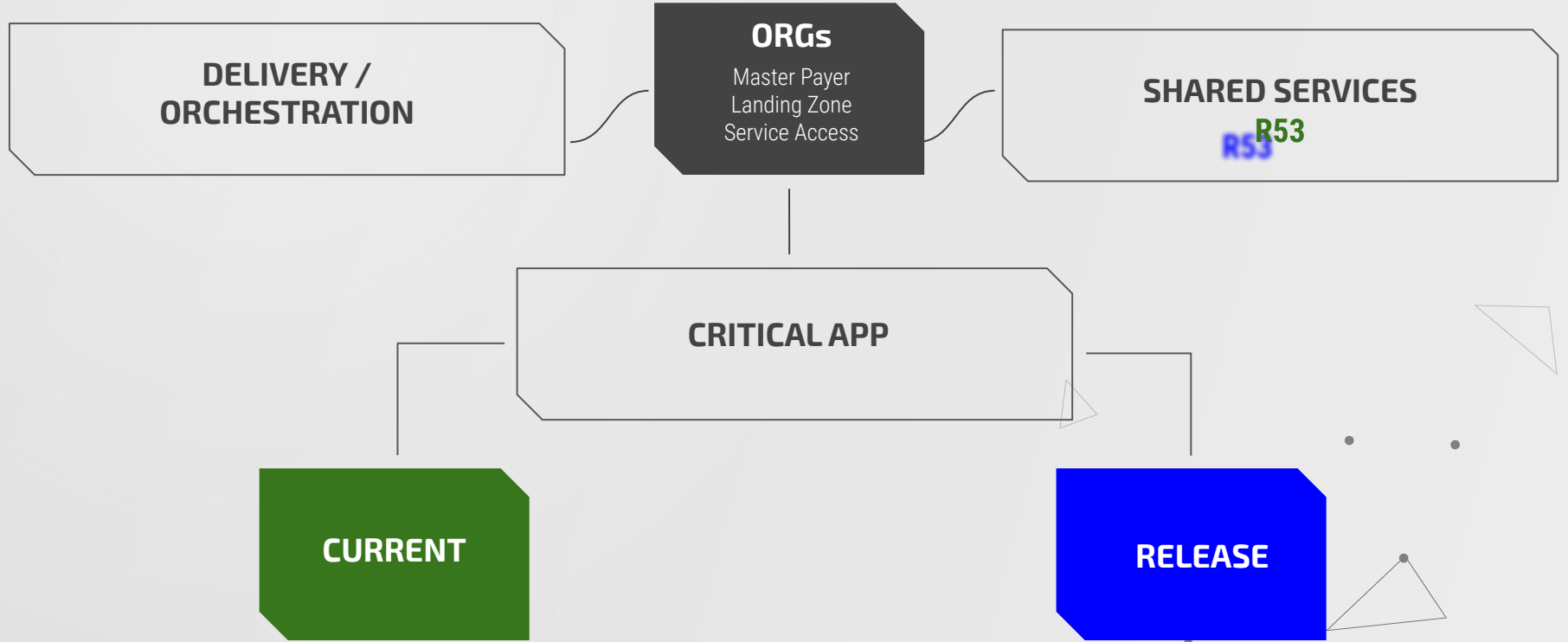
BILLING



ISOLATION



RECOVERY



WE DID & YOU CAN TOO

	ACTIVE ACCOUNTS	TIME TO DEPLOY	POLICIES UNDER SC	CAB REVIEW
Q2 '17	~12	2+ Wks	1	2 Wks
Q2 '18	~30	3-4 Days	~20	~1 Wk
Q2 '19	66	~30 min.	3	IRT




Everyone gets an AWS Account





 AWS Organizations Acct





OAM


 Security & Logging

 IAM


 Enforcement


 Shared Resources


 Enterprise Infrastructure


 ACCT6

R&D


 Current Program Dev


 APP2 Dev


 APP3 Dev

 Sandbox


Production

 Current Program

 APP2

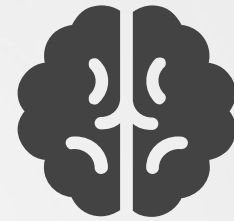
 APP3

Legacy

 Program Today



&



CCM for the people

Phase 1. Delegate change and configuration to lowest level

Phase 2...

Phase 3. Celebrate success

I DON'T ALWAYS TEST
MY CODE



BUT WHEN I DO,
I DO IT IN PRODUCTION

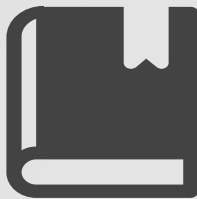
DevOps

“

~~GEOLOGY~~ IS THE STUDY
OF PRESSURE AND TIME.
THAT'S ALL IT TAKES,
REALLY. PRESSURE AND
TIME. THAT AND A BIG
GODDAMN POSTER.

ELIAS WEDDING

WHAT'S IN IT FOR ME



DOCUMENTATION

Environmental Configuration
Custom Settings
Deployment Requirements

SUPPORT TICKETS

Increase resolution time
Reduced outages

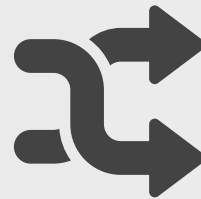


HUMAN ERROR

No more typos
Naming convention
Required elements (tags)

BASELINE

Cookie cutter environment
Compliance
Historical





What do you want?

CLONE / FORK

Bring down current state
Permission caveats for reviewer

01

FEATURE BRANCH

Purposeful commits
WIP for discussion

02

MERGE / PULL

Document modification
Request deployment by CM

03

CAB
-
AS
-
CODE

04

REVIEW

No pipeline failures
Approve, prioritize & schedule

05

DEPLOY

Merge into env. Branch
Monitor for rollback

06

CLOSE ISSUE / CRQ

Formal request closed
Revert if needed



CHANGE ?

'GIT' IT

TRACK

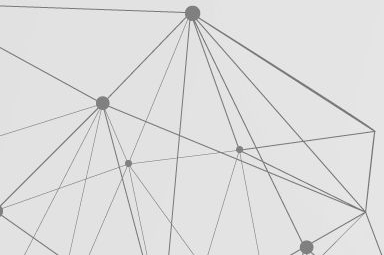
how has this evolved?

BLAME

what happened? when?

HOOKS

leverage more automation







CICD/D

'Agile' Account Development

Using GitLab for a complete 'DevOps' platform tool-chain

WHAT IF I TOLD YOU

YOU DON'T HAVE TO USE JENKINS

PIPELINE



BUILD



TEST



QA

DEV

PROD



REVIEW



STAGE



DELIVER / DEPLOY

QUALITY CODE



LINTING

Templates
SCA
Validation
Bugs

Port
CIDRs
Actions
Services

SECURITY



REQUIREMENTS

Tagging
Naming convention (prefix)
Documentation

SYSTEMIZED DEPLOYMENT

REVIEW

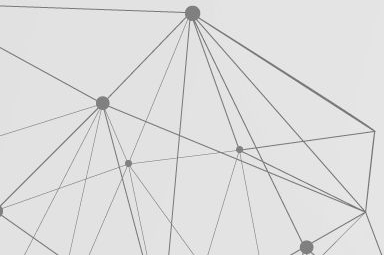
what's going to break?

STAGE

prepare to ship / known rollback

DELIVER

auto / schedule / manual



A woman with short, curly brown hair and glasses is clapping her hands. She is wearing a yellow and brown patterned top. The background shows a window with light curtains on the left and a doorway leading to another room on the right. The room in the background has patterned wallpaper and a lamp.

DEMO

sdcc2019.rwick.it



Distillation

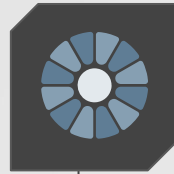
Lessons Learned

What to look out for after two years of implementation

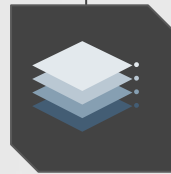
PLAN FOR SCALE



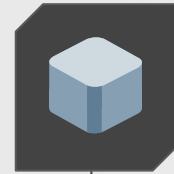
Determine
dependencies



Isolate
resources



Define
standards

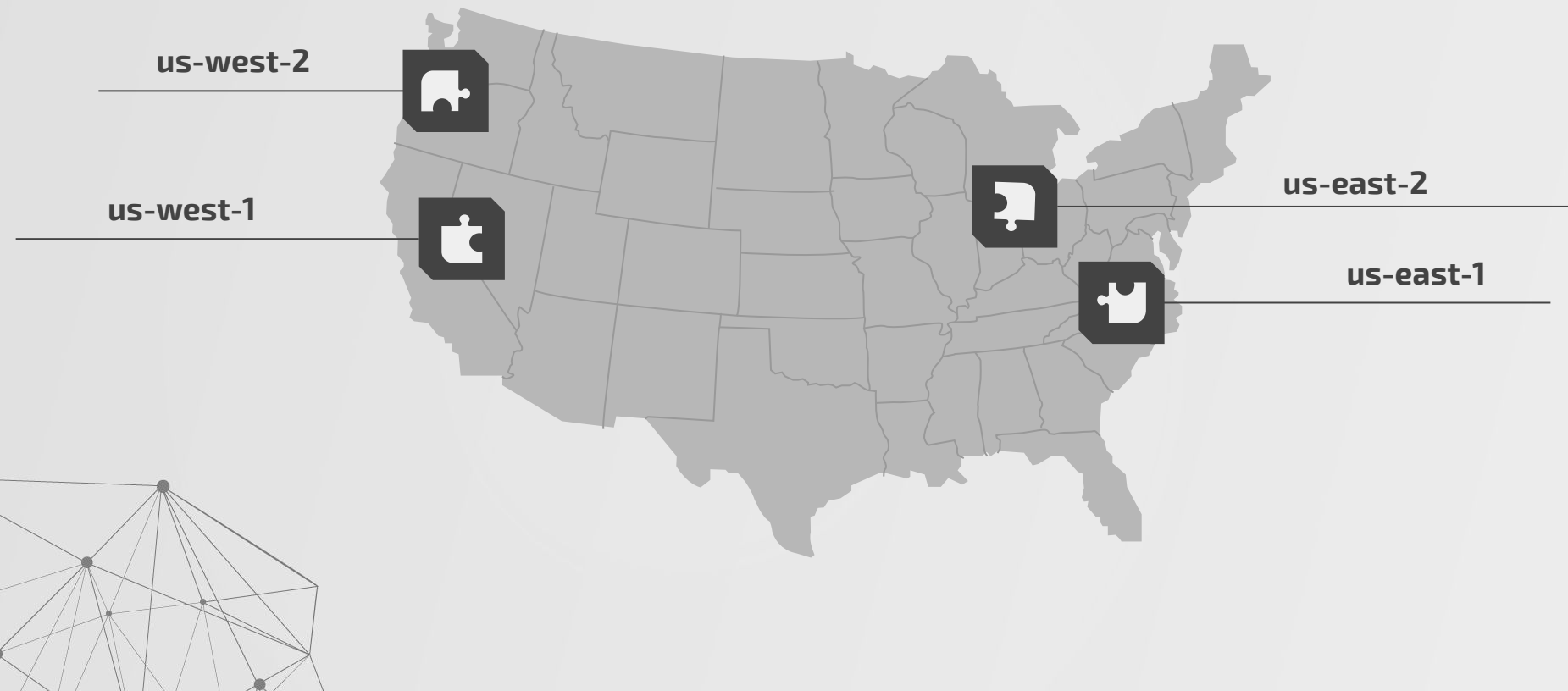


Test
design



Linear
Feedback
Experimentation

MULTI-REGION & GLOBAL RESOURCES





GIT WITH PURPOSE

COMMIT

ISSUE

MERGE

PRUNE

COMMUNICATE

REVIEW



The background of the slide is a light gray color. It features two abstract geometric patterns made of thin gray lines and small dark gray dots. One pattern is on the left side, and another is on the right side. The lines connect the dots in a way that creates a series of overlapping triangles and polygons, giving it a network-like appearance.

THANKS

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

Please keep this slide for attribution.

THANKS TO OUR SPONSORS

GOLD SPONSOR



SILVER SPONSORS



LOCATION SPONSOR



[SOUTHDAKOTACODECAMP.COM](https://southdakotacodecamp.com)

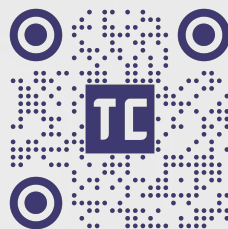


Sfdevs.slack.com

#Cloud

@rosswickman

QUESTIONS?



sdcc2019.rwick.it



@rosswickman
ross@tactful.cloud
<https://tactful.cloud>