PUBLIC SECTOR SUMMIT ONLINE

Improving your organization's security posture with AWS

Tim Rains

Regional Leader

Security and Compliance Business Acceleration

Amazon Web Services

aws PUBLIC SECTOR SUMMIT ONLINE

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Ten places your security group should spend time

Related breakouts

- Defending your data against ransomware threats with secure storage
- Using AWS security services to achieve advanced threat detection
- CI/CD at scale: Best practices with AWS DevOps services

Ten places your security group should spend time

AWS CISO Steve Schmidt: The top ten list

Ten places your security group should spend time

1. Accurate account info
2. Use MFA
3. No hard-coding secrets
4. Limit security groups
5. Intentional data policies
6. Centralize AWS CloudTrail logs
7. Validate IAM roles
8. Take action on GuardDuty findings
9. Rotate your keys
10. **Being involved in dev cycle**

"I really want people to focus on those elements that I think give them the biggest bang for the buck and also represent the areas where people stub their toe the most in the security space… "

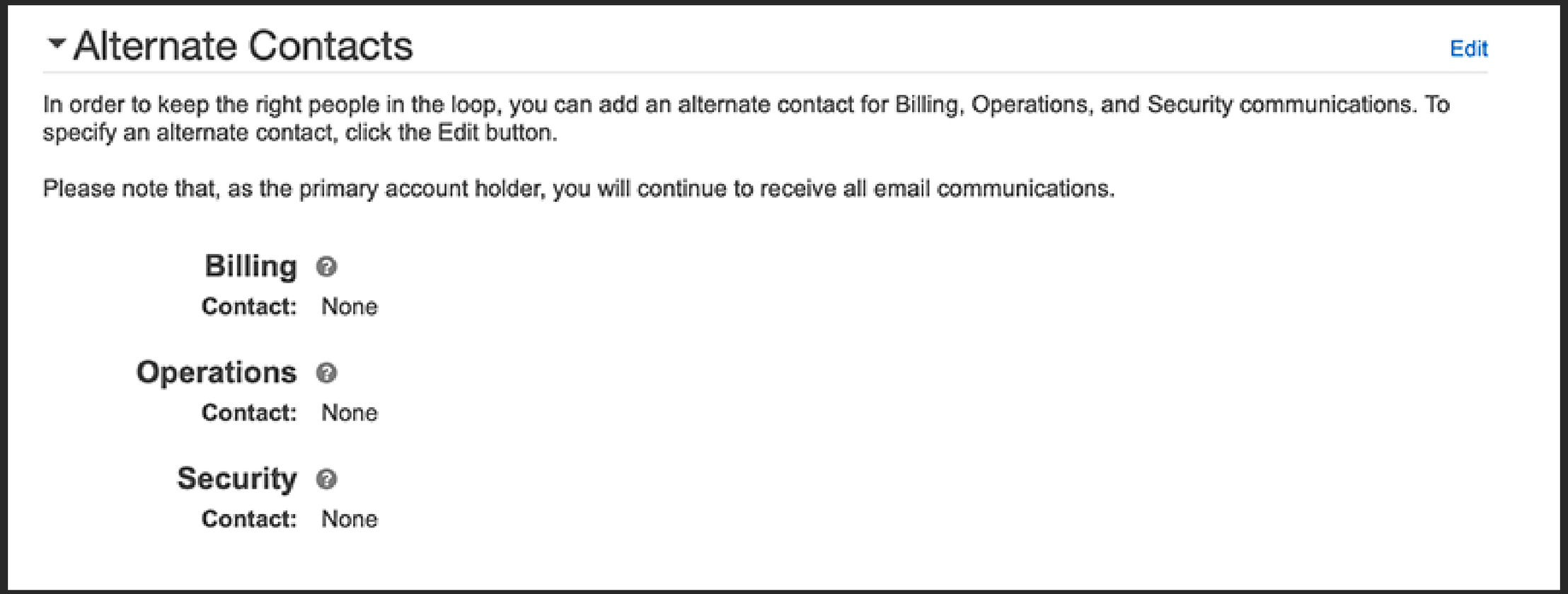
– Steve Schmidt
Vice President and Chief
Information Security Officer
Amazon Web Services

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ten places security teams should spend time

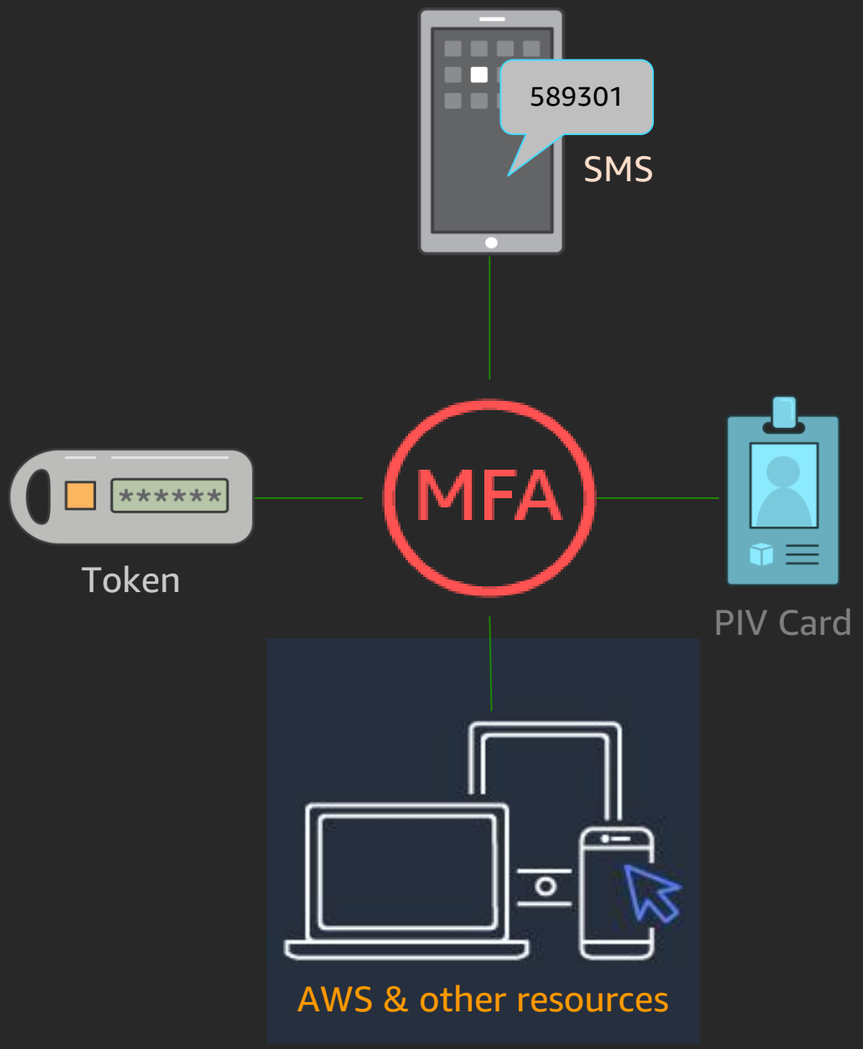
1. Account contact info
2. Use MFA
3. No hard-coding secrets
4. Limit security groups
5. Intentional data policies
6. Centralize AWS CloudTrail logs
7. Validate IAM roles
8. Take action on security findings
9. Rotate your keys
10. Involve security in the development lifecycle

1. Accurate account information



https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-account-payment.html

2. Use multi-factor authentication (MFA)



MFA adds an extra layer of protection on top of name and password for root, interactive IAM users

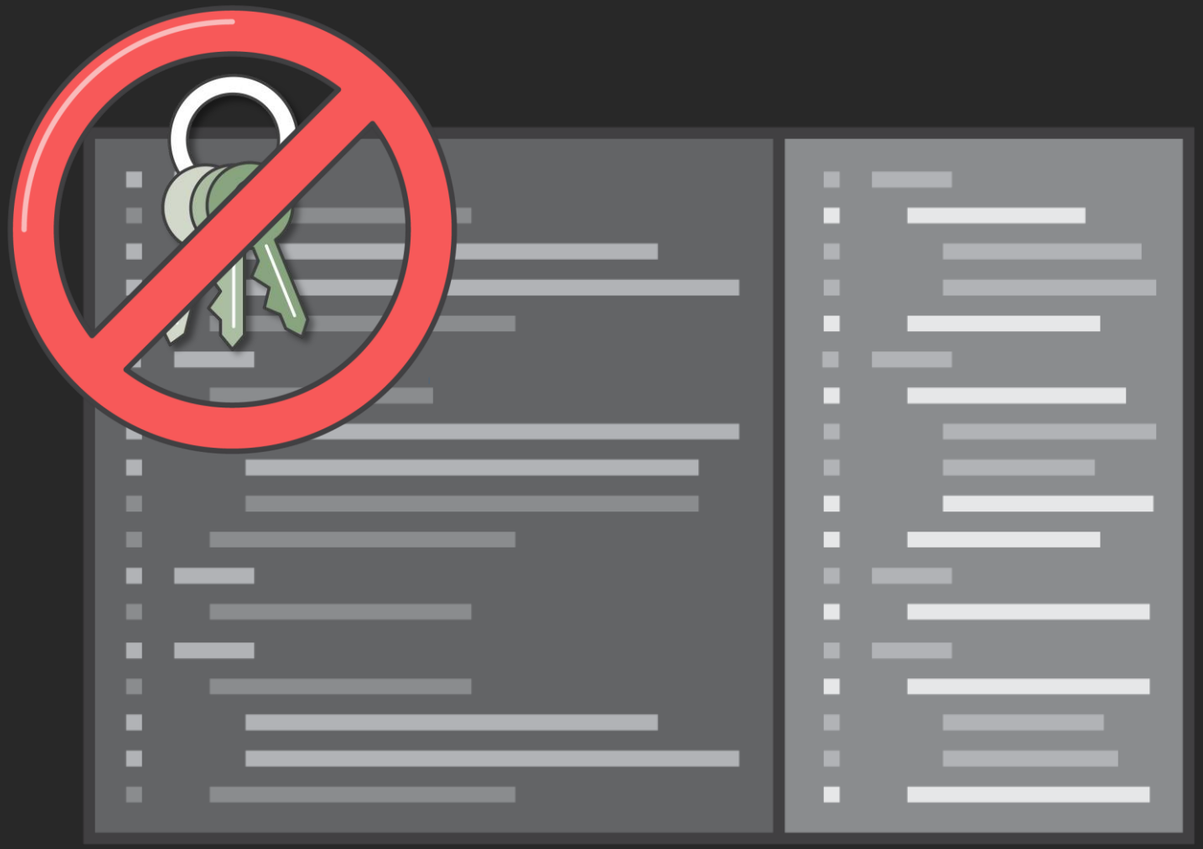
- Virtual MFA devices
- U2F security key
- Hardware MFA device
- SMS text message-based MFA (in preview)

Identity federation changes the approach, but not the best practice

- Use MFA at your identity provider
- Also works with AWS CLI (version 2)

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

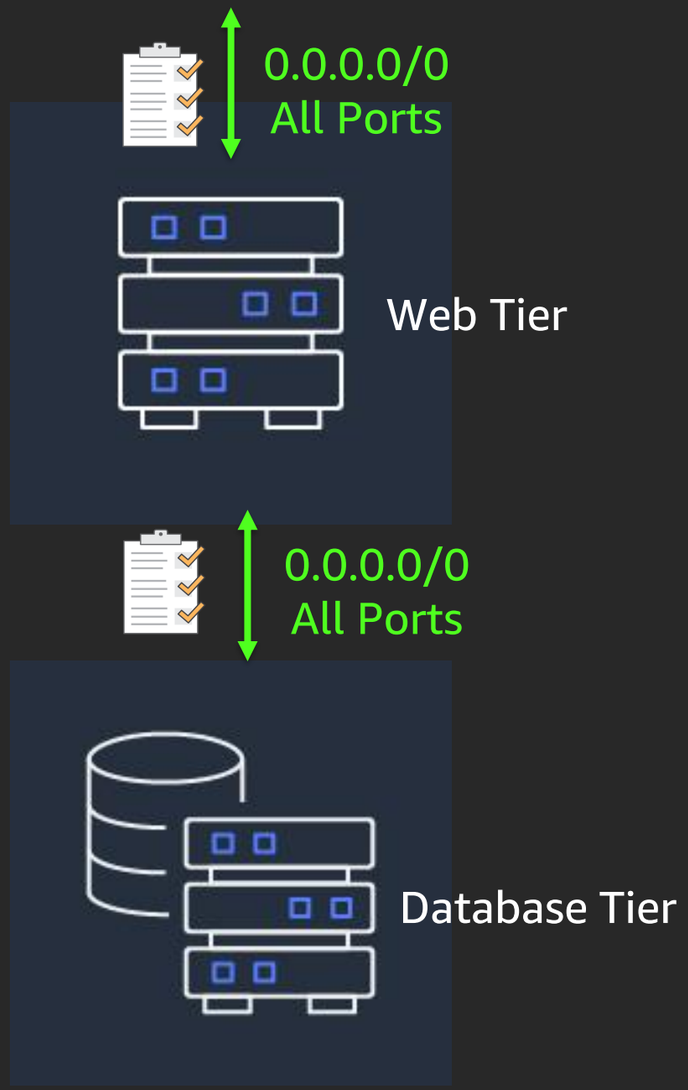
3. No hard-coding secrets



- What are secrets?
  - AWS keys or secret keys
  - UID/Password
- Why?
  - Risk of compromise
  - Impact of compromise
- How do I protect my secrets
  - Avoid long lived credentials where possible
  - Create AWS IAM roles to deliver temporary, short-lived credentials for calling AWS services
  - Use Secrets Manager to securely store and manage database credentials, API keys, and other secrets through their lifecycle

https://aws.amazon.com/secrets-manager/

4. Limit security groups



Ensuring that only the required ports are open and the connection is enabled from known network ranges is a foundational approach to security

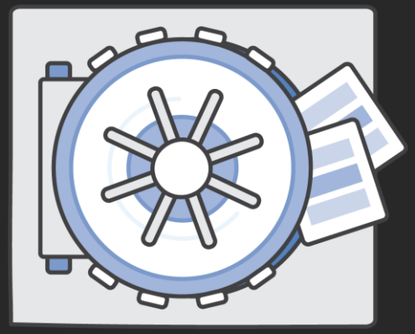
- Use AWS Config or Firewall Manager to programmatically ensure security group configuration is what you intended
- Network reachability rules package analyzes your Amazon VPC network configuration to determine whether your Amazon EC2 instances can be reached from external networks
- Firewall Manager can also be used to automatically apply AWS WAF rules to internet-facing resources across your AWS accounts

https://aws.amazon.com/blogs/security/how-to-monitor-aws-account-configuration-changes-and-api-calls-to-amazon-ec2-security-groups/

5. Intentional data policies

Data

Policies



Protected Data

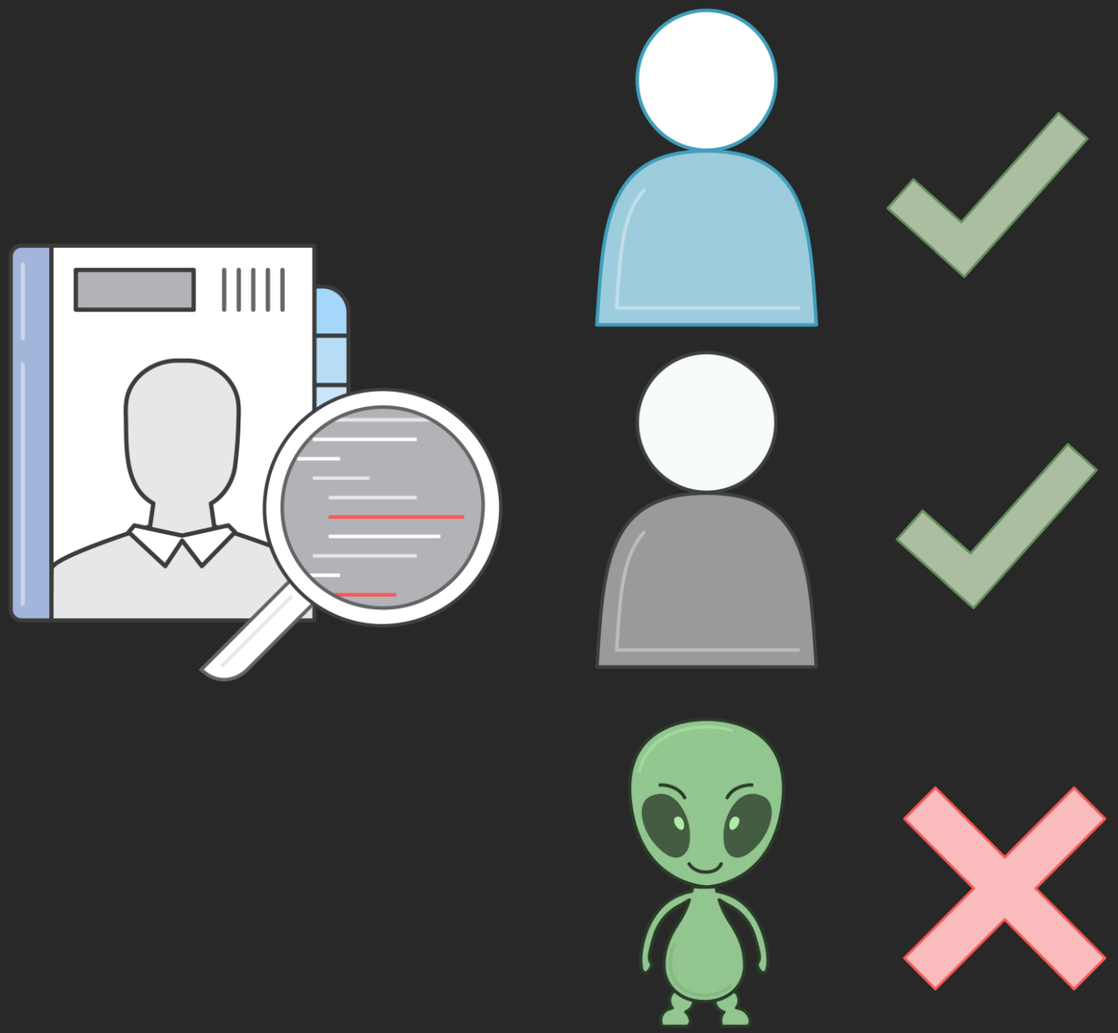
What is an intentional data policy?

- Specific – e.g.
  - Data type
  - Storage service
  - Encryption method
  - Access control
  - Audit/logging
- Guides decision making
- Ideally
  - Can be expressed as code
  - Enables governance and compliance automation

6. Centralize CloudTrail logs

https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html

7. Validate IAM roles



Look for overly permissive roles

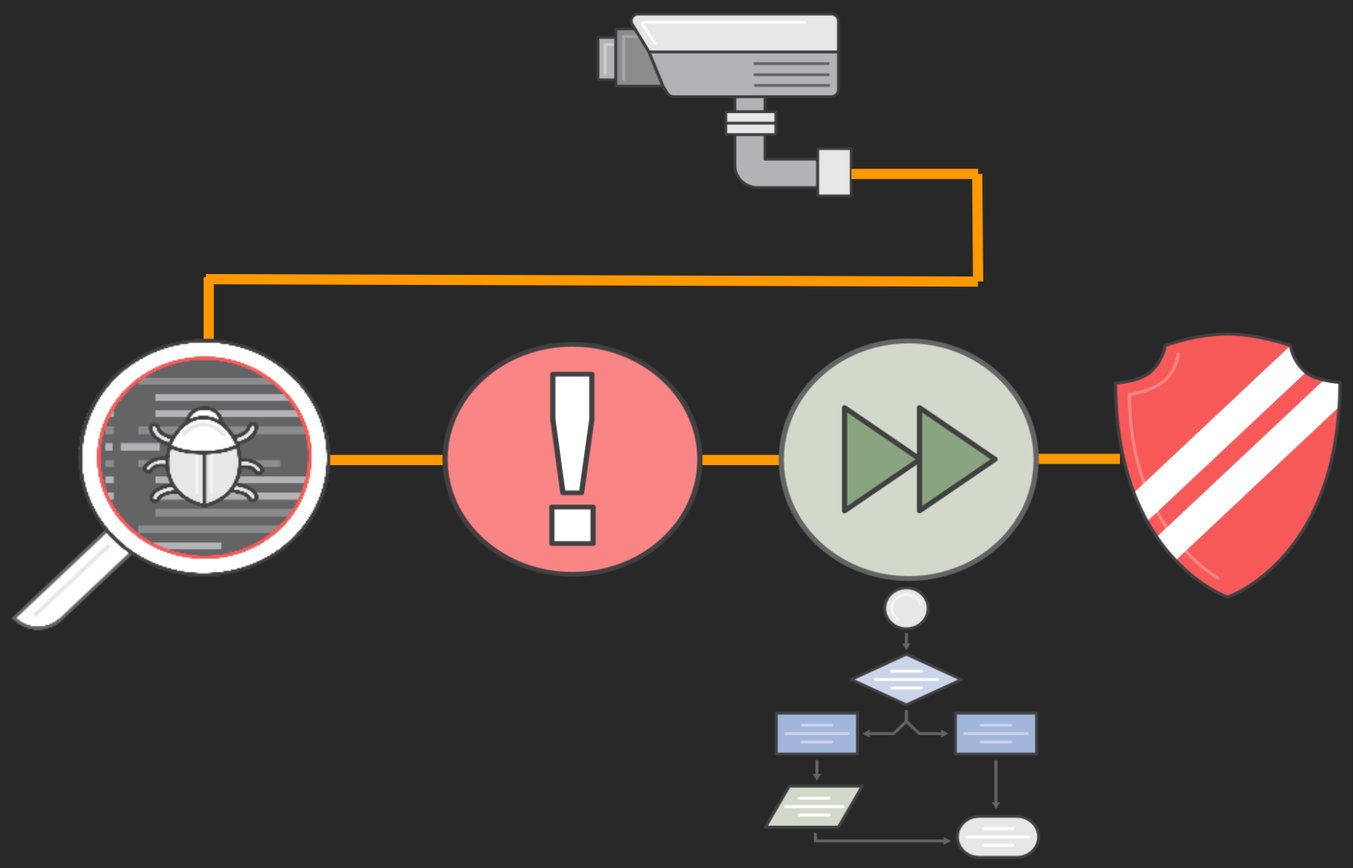
- Use IAM Access Analyzer
- Security Hub
- Third-party/open source tools

Detect and remove unused roles

- Implement continuous monitoring of role activity using AWS Config
  https://aws.amazon.com/blogs/security/continuously-monitor-unused-iam-roles-aws-config/

https://aws.amazon.com/iam/features/analyze-access/

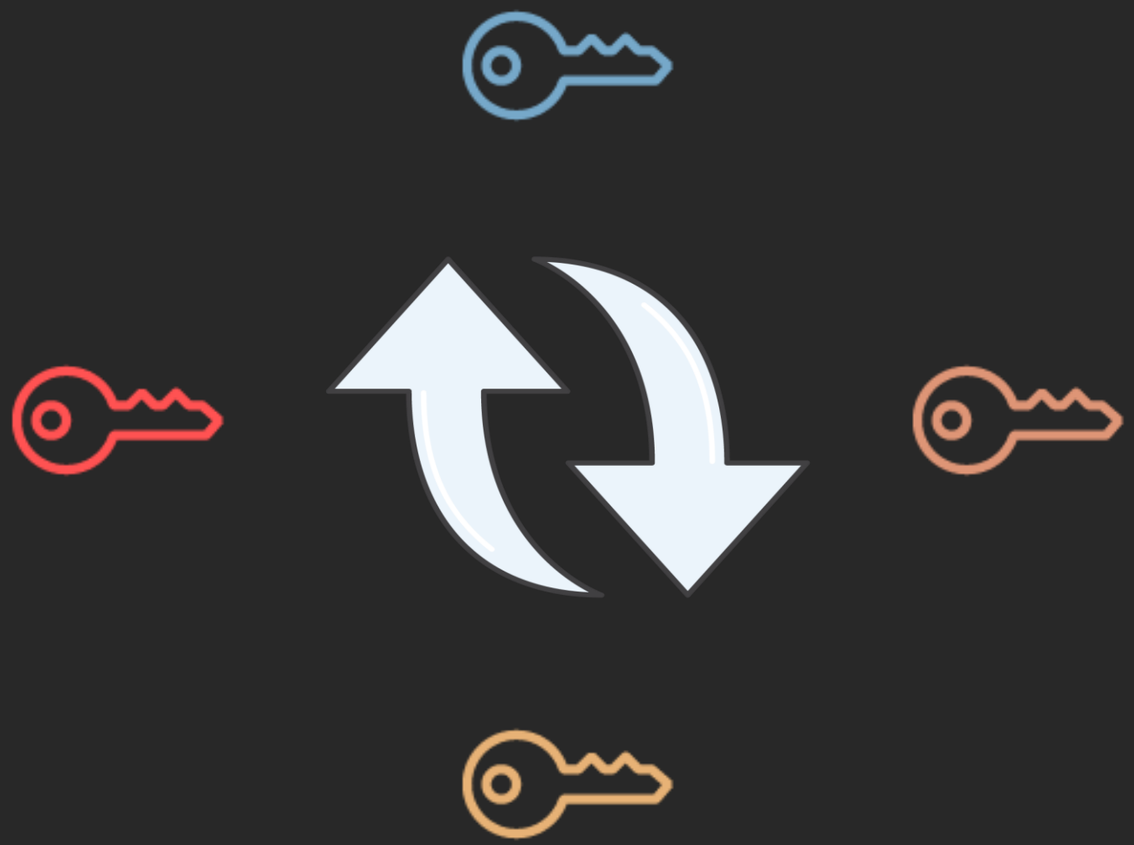
8. Take action on security findings



- GuardDuty
- Security Hub
- IAM Access Analyzer

https://aws.amazon.com/blogs/security/automated-response-and-remediation-with-aws-security-hub/

9. Rotate your keys



- Avoid using long-term access keys
- Use IAM roles and federation
- If you need to use access keys rather than roles, you should rotate them regularly
  https://aws.amazon.com/blogs/security/how-to-rotate-access-keys-for-iam-users/
- Security Hub can check for IAM users with access keys that are long lived and haven't been rotated regularly

https://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html

10. Be involved in the dev cycle

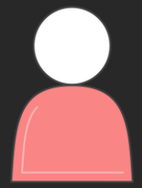
"I guarantee you'll find interesting places where you can look, to see where you can do better as an organization."

Steve Schmidt

Vice President and
Chief Information Security Officer
Amazon Web Services

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traditional governance flow



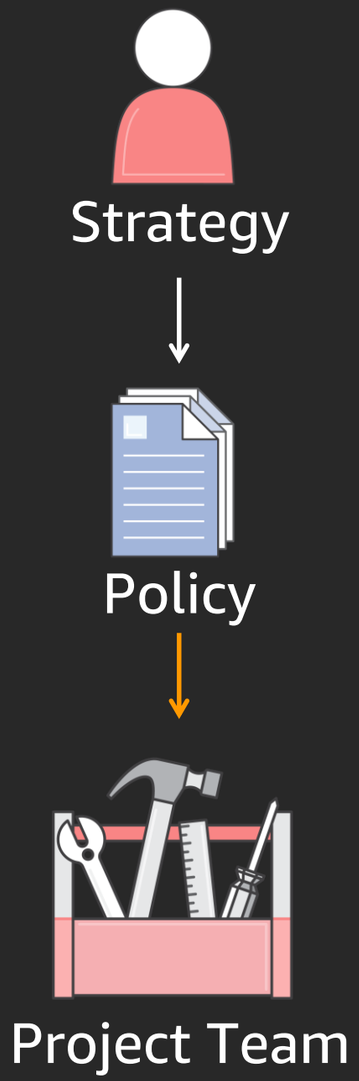
Strategy

Traditional governance flow

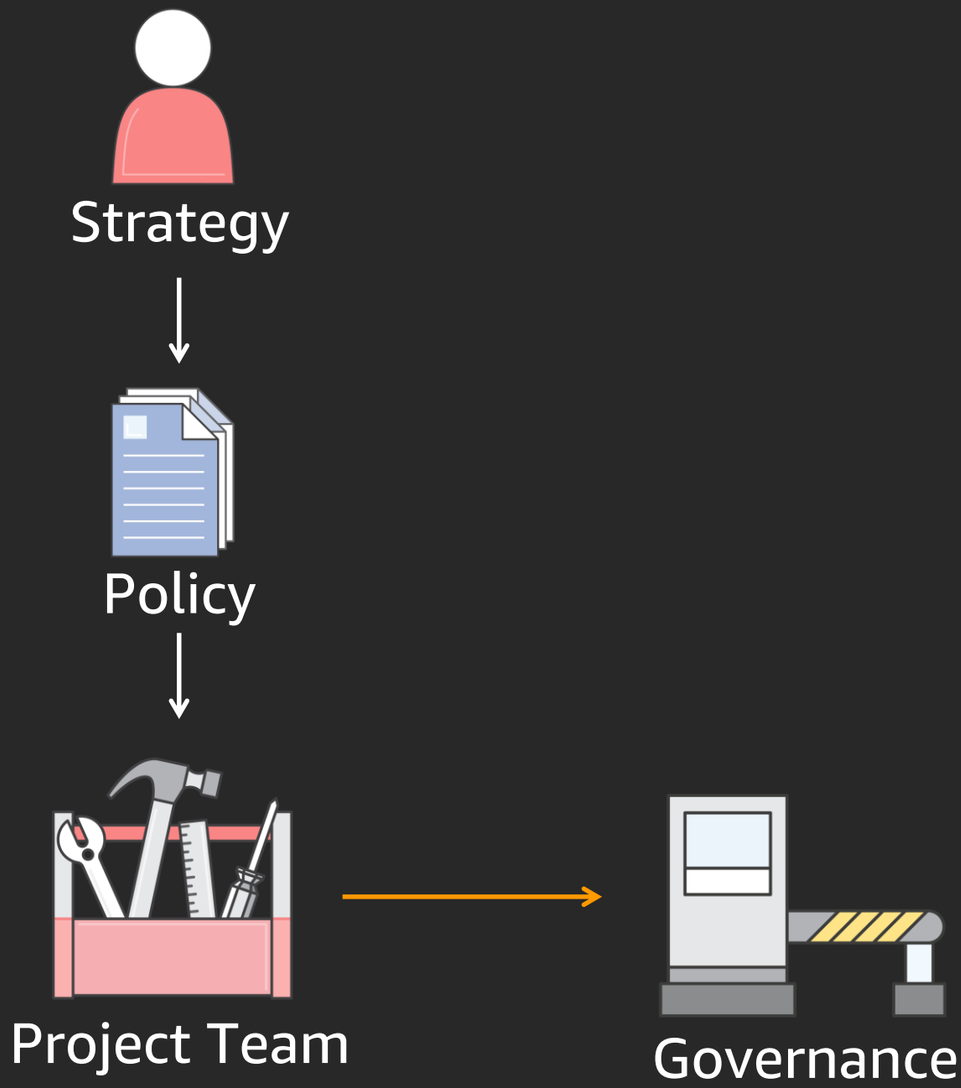
Strategy

Policy

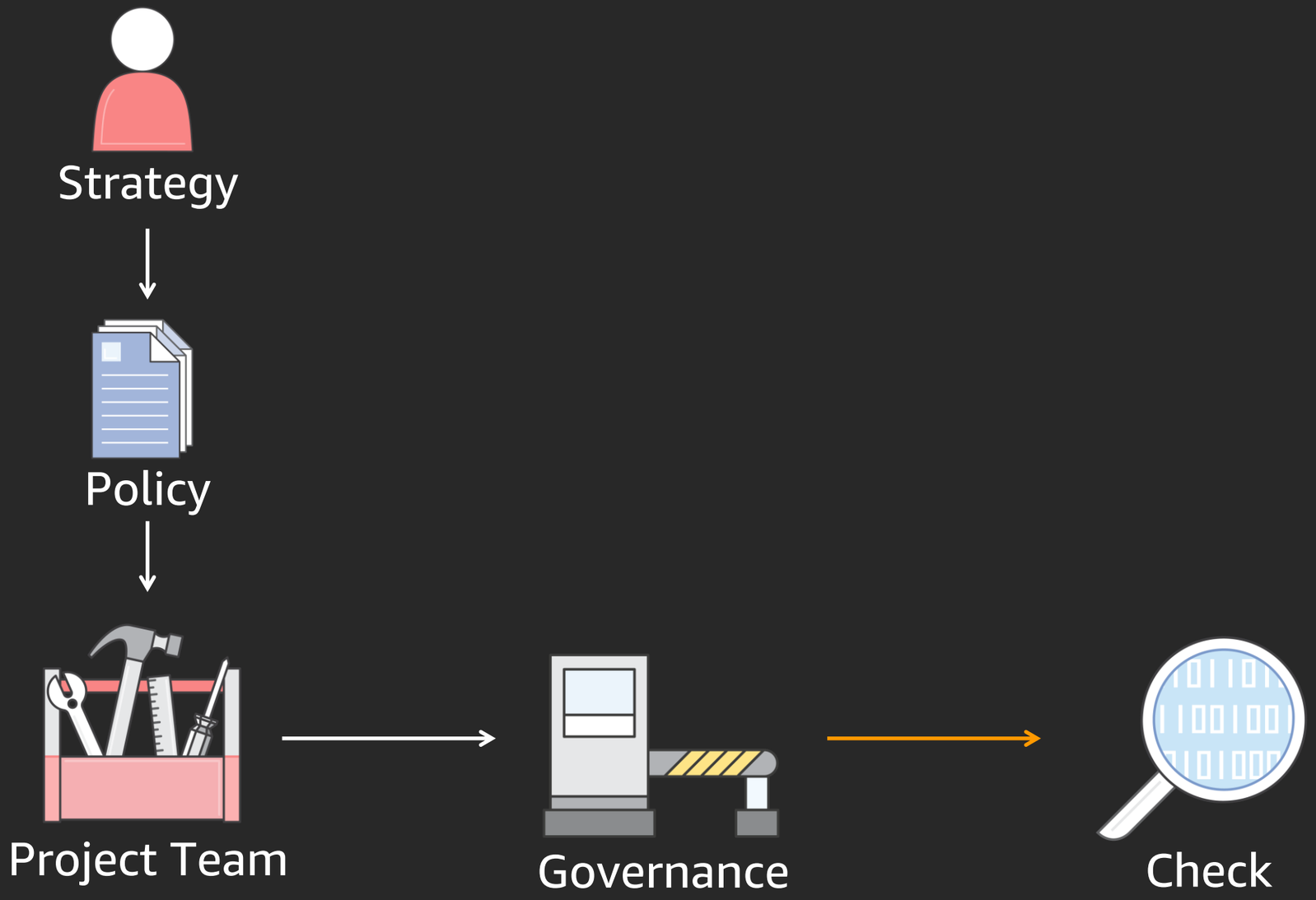
Traditional governance flow



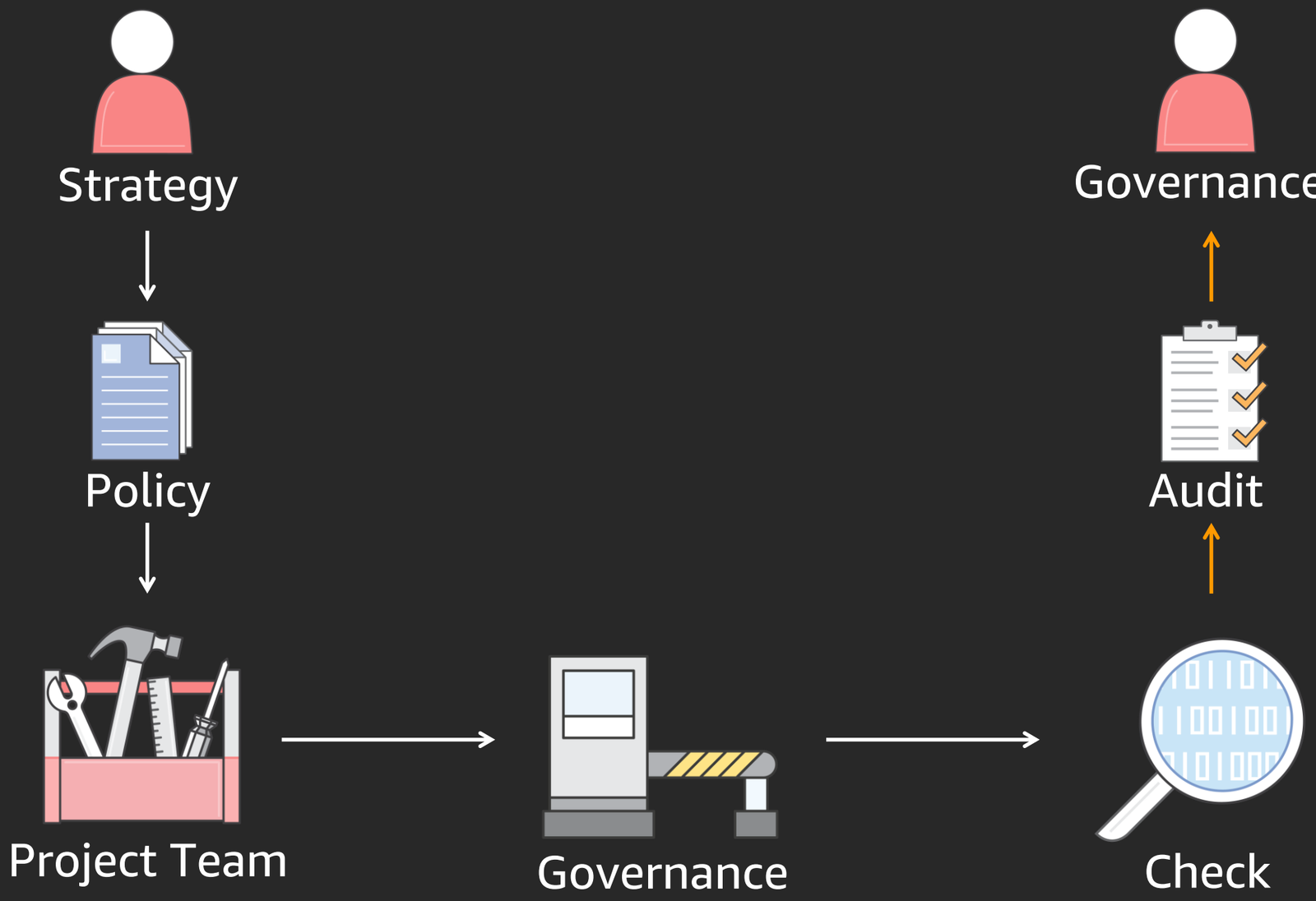
Traditional governance flow



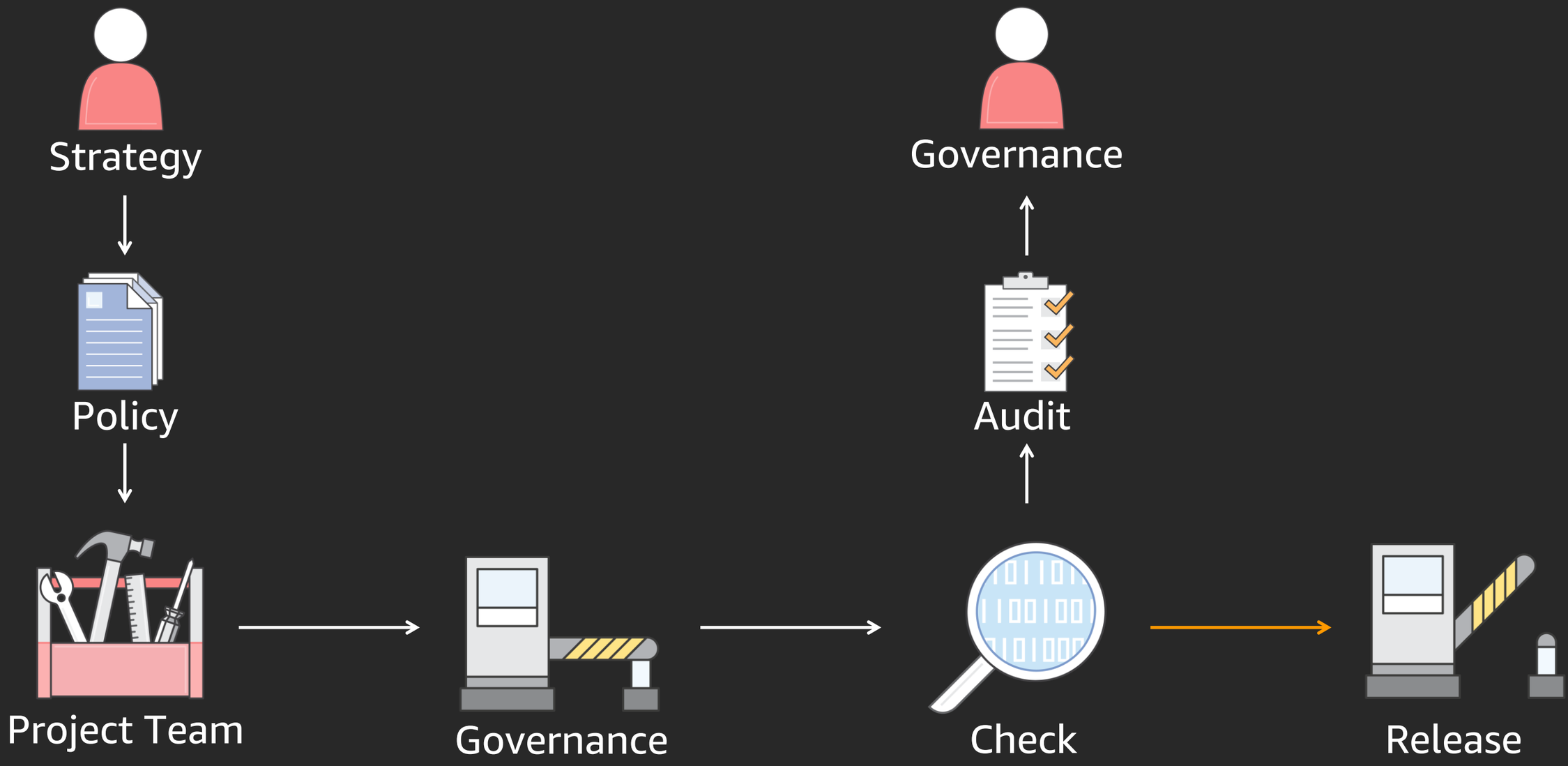
Traditional governance flow



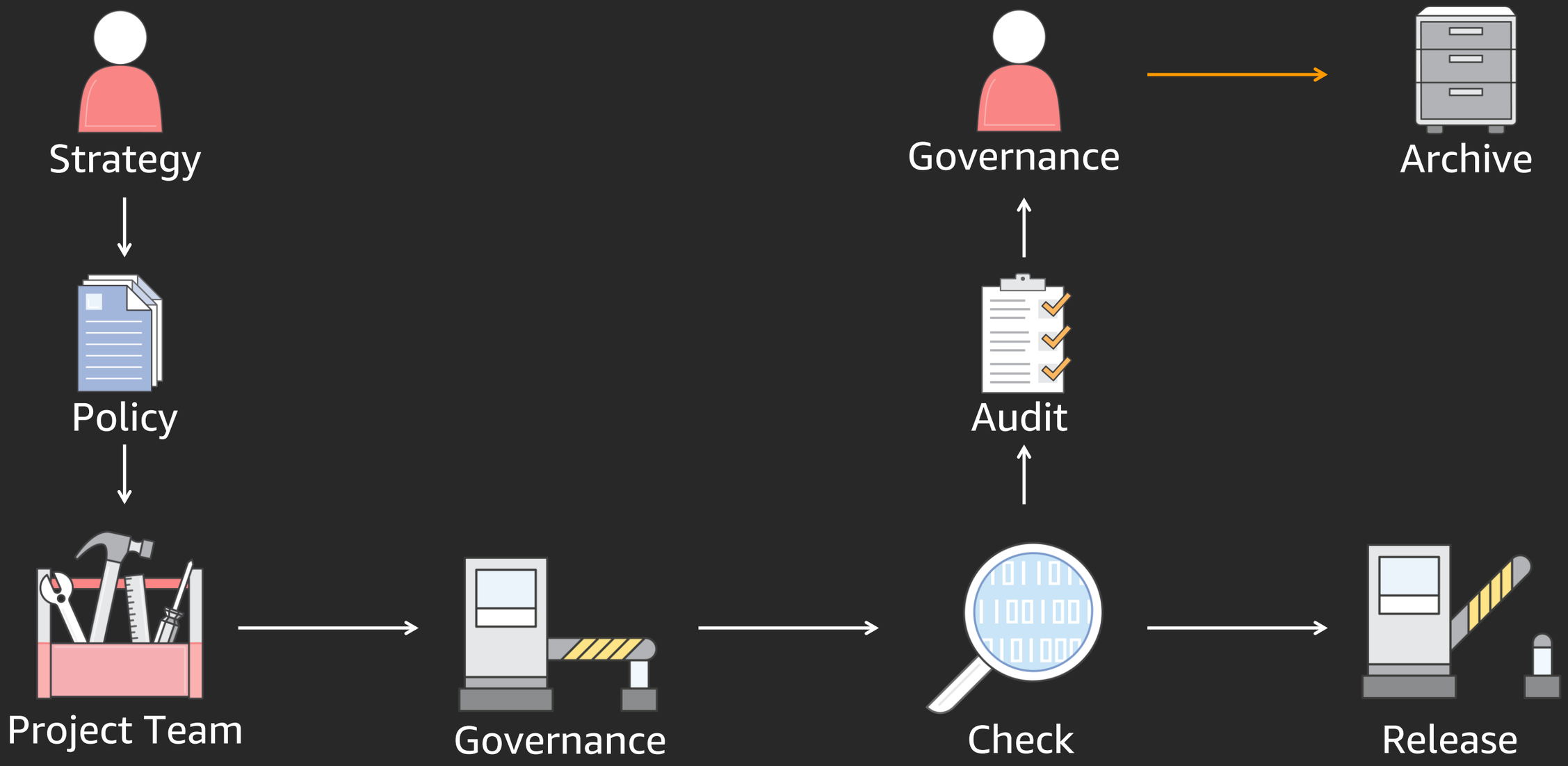
Traditional governance flow



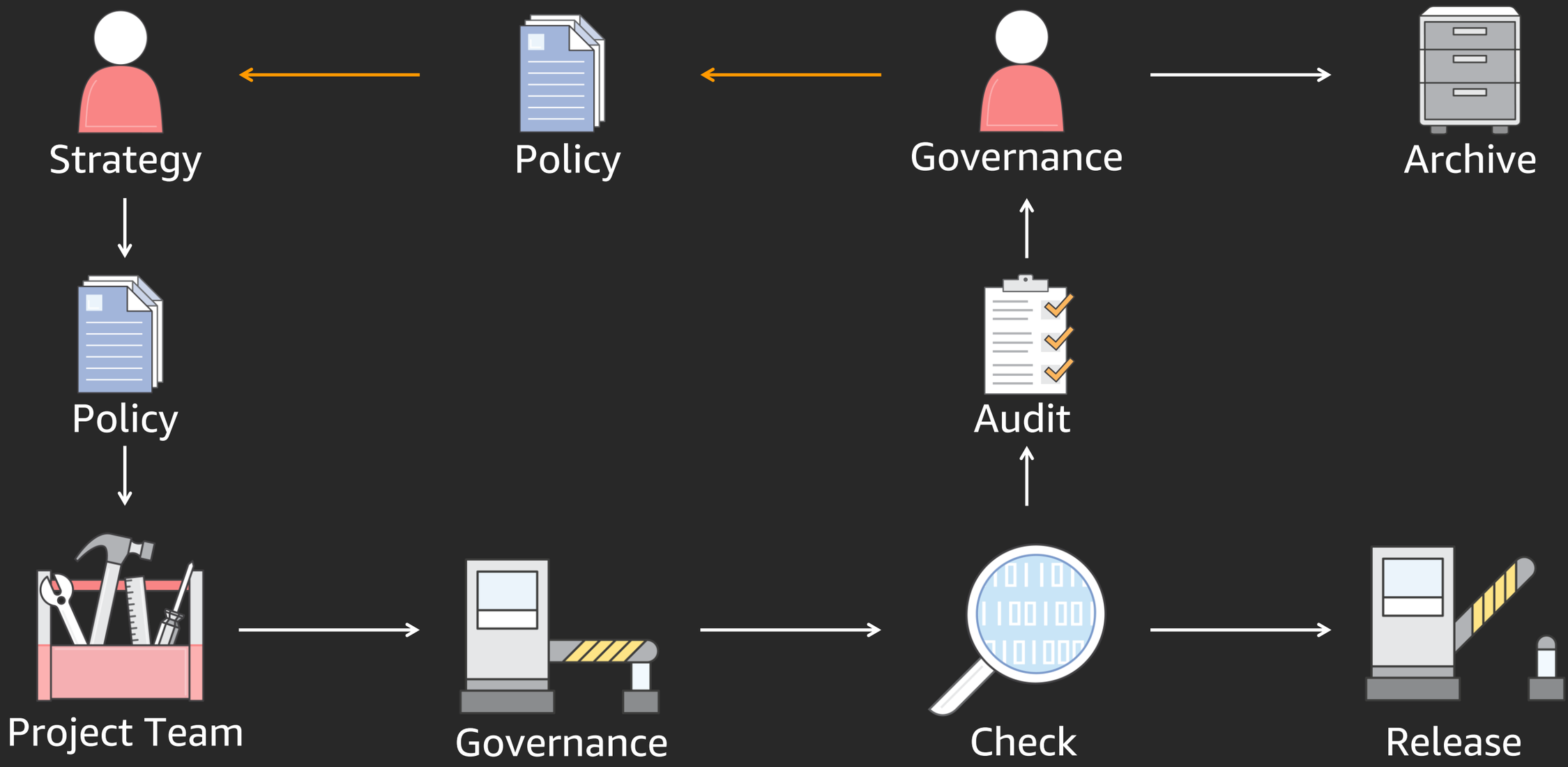
Traditional governance flow



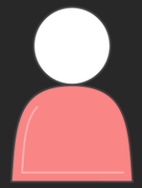
Traditional governance flow



Traditional governance flow



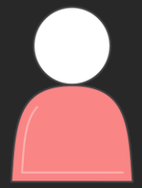
Governance at the speed of cloud



Strategy

Policy

Governance at the speed of cloud

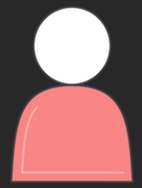


Strategy

Policy

Project team

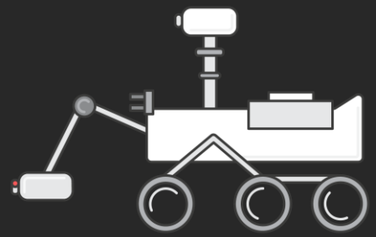
Governance at the speed of cloud



Strategy

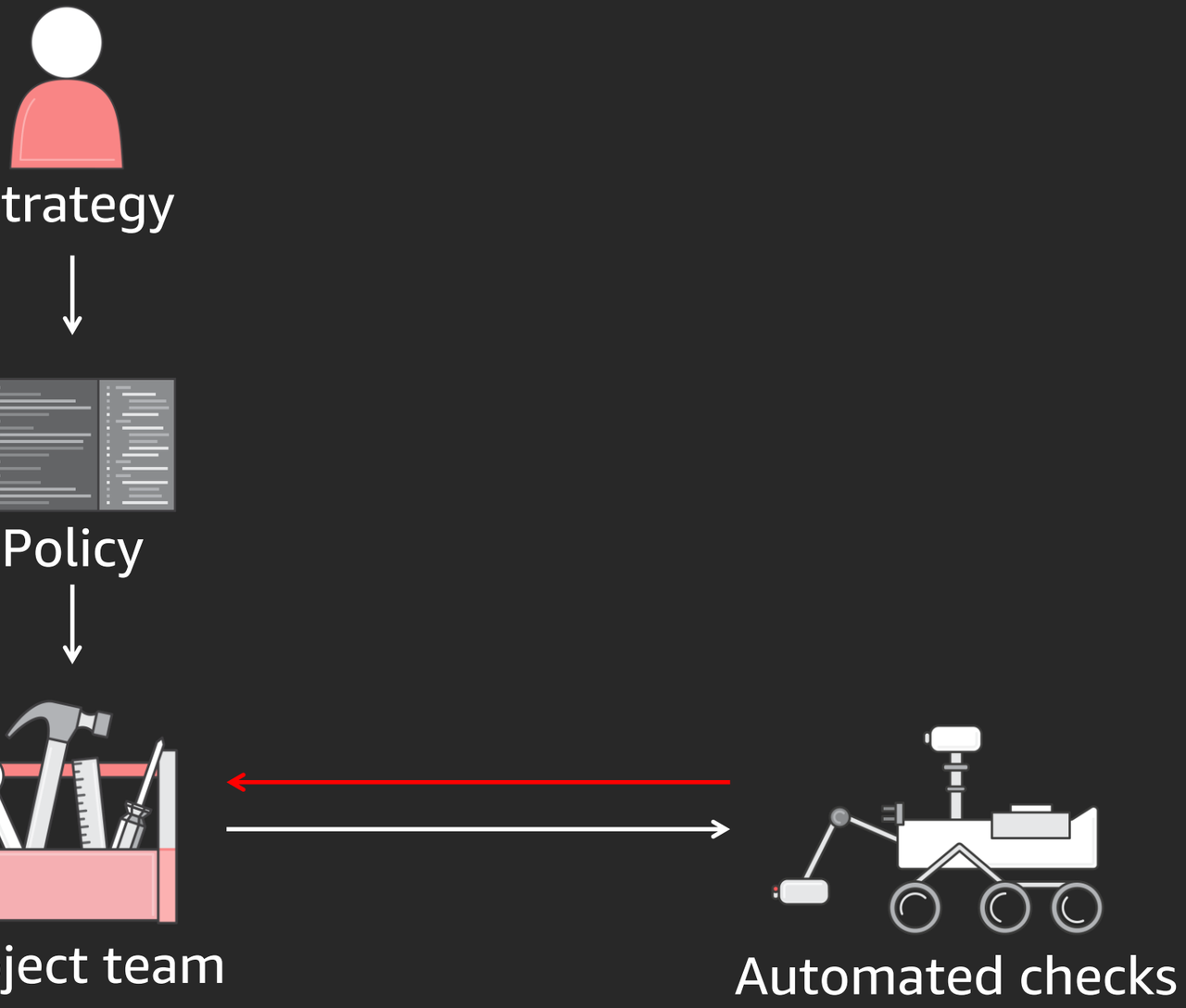
Policy

Project team



Automated checks

Governance at the speed of cloud

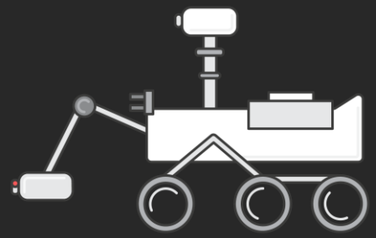


Governance at the speed of cloud

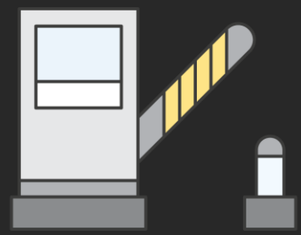
Strategy

Policy

Project team

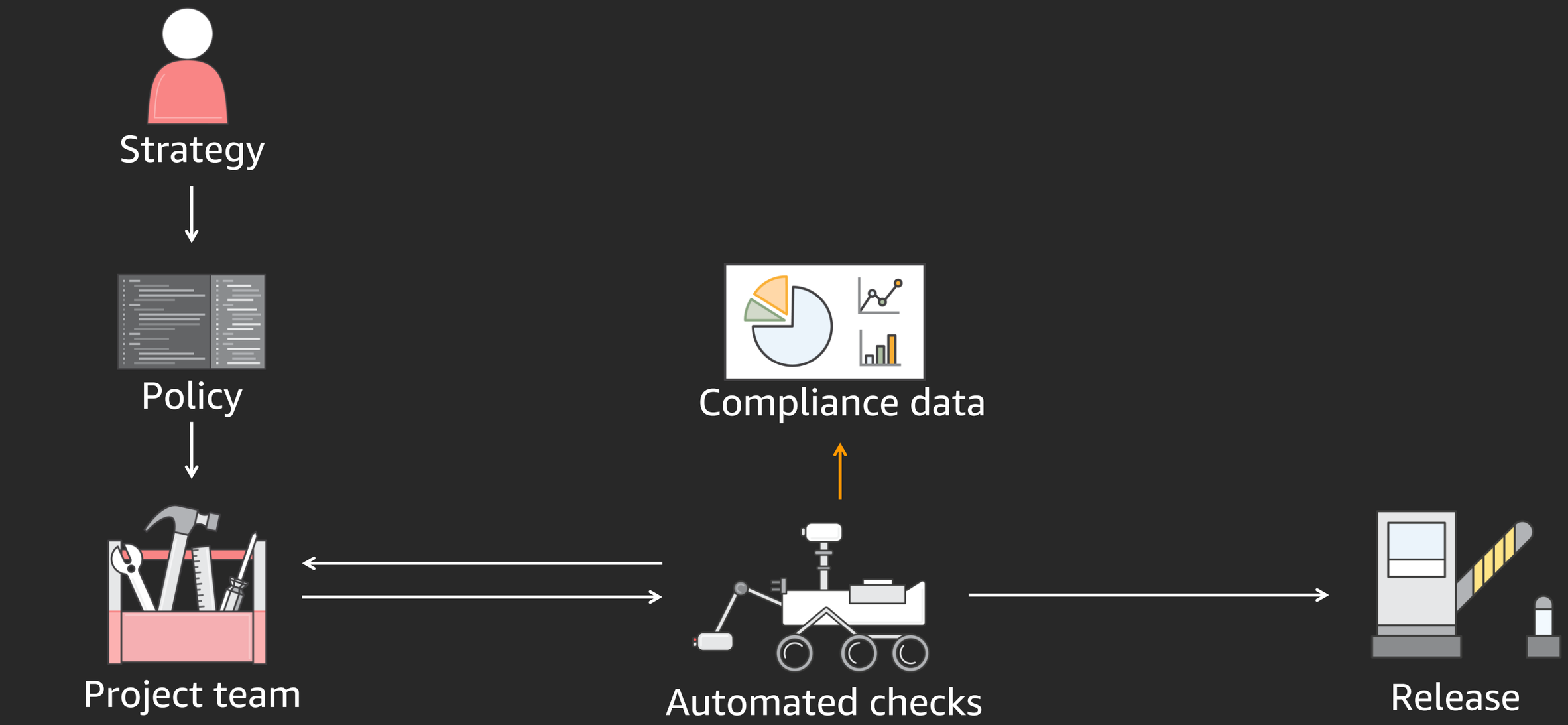


Automated checks

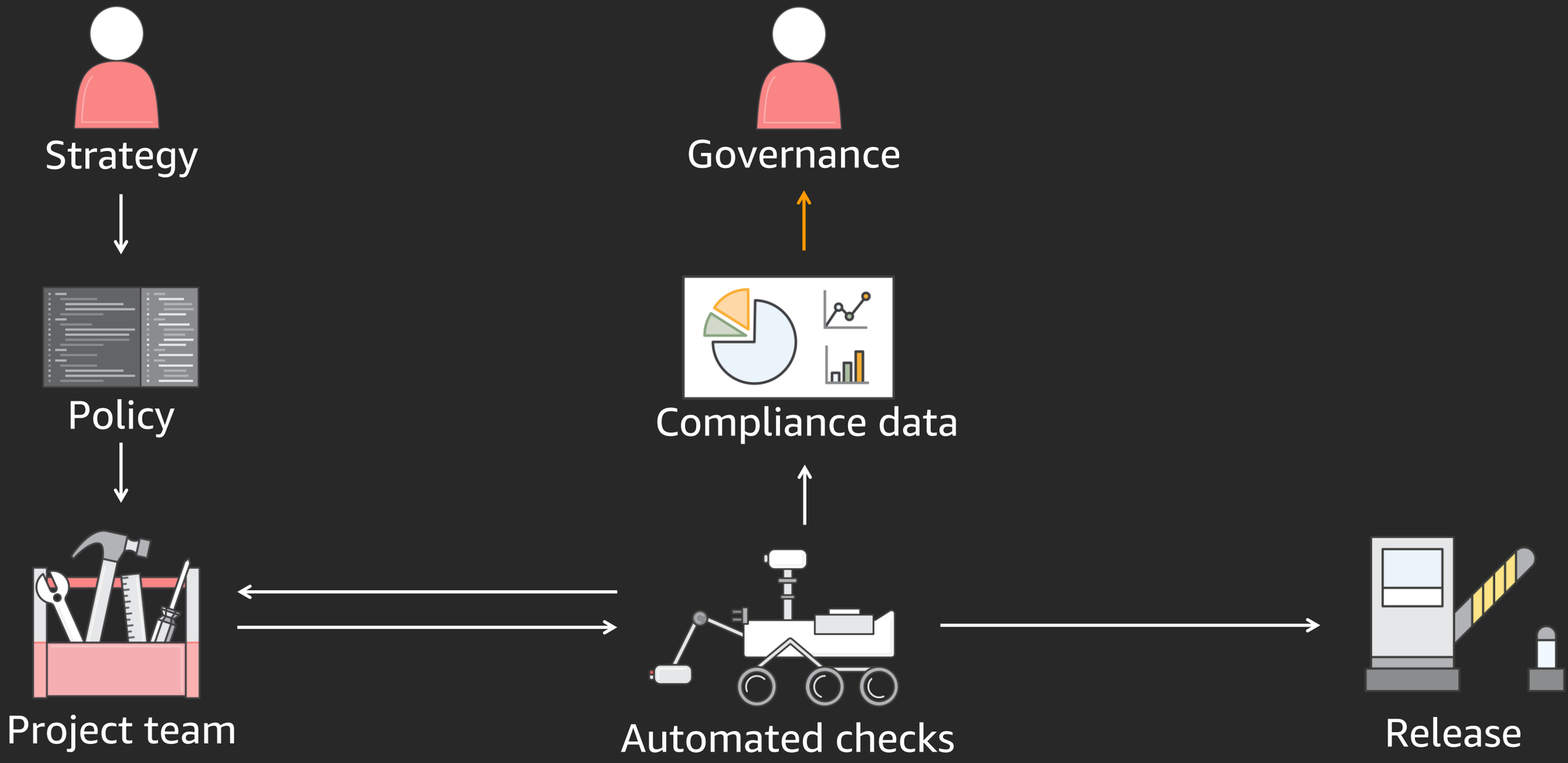


Release

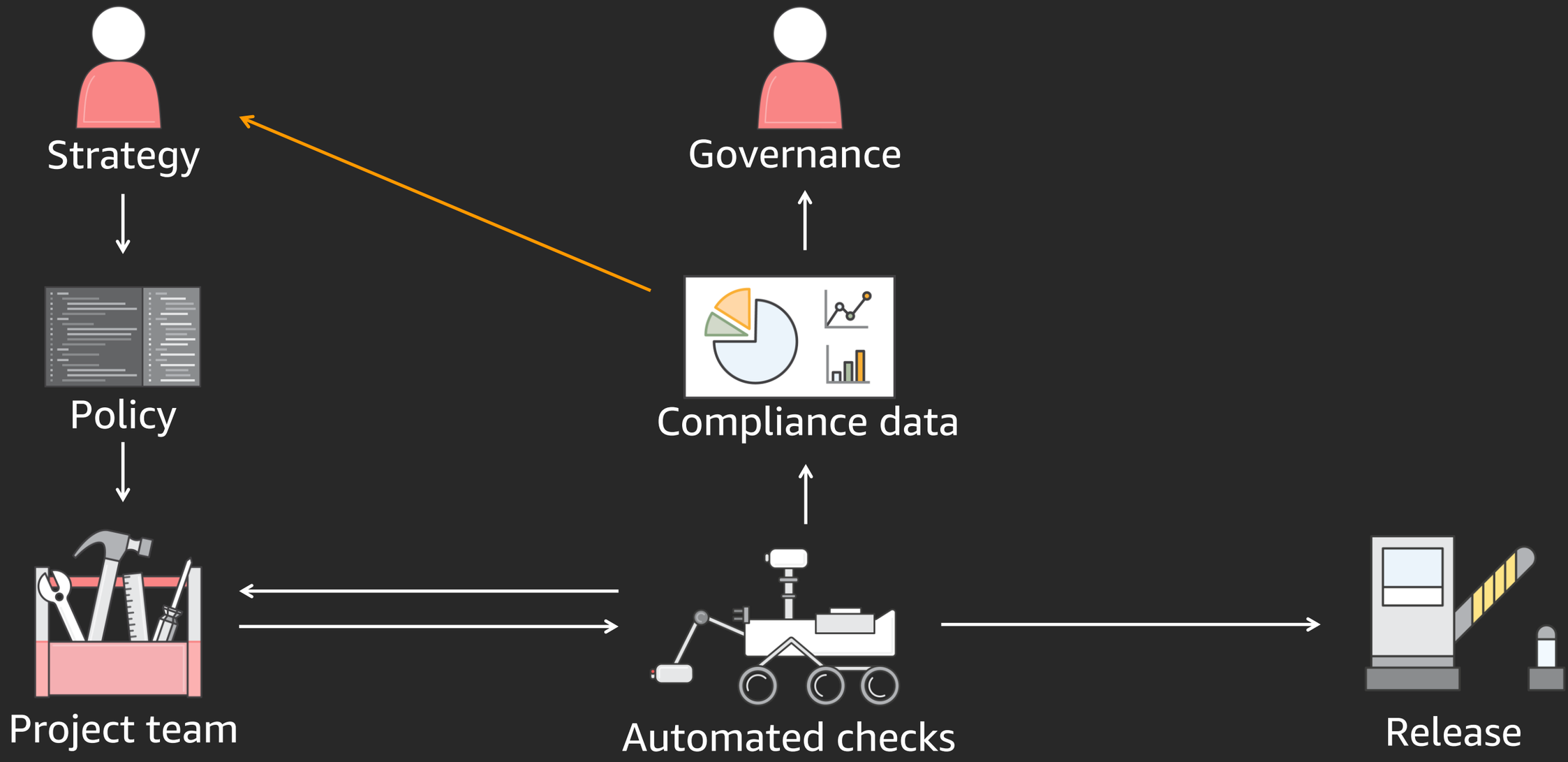
Governance at the speed of cloud



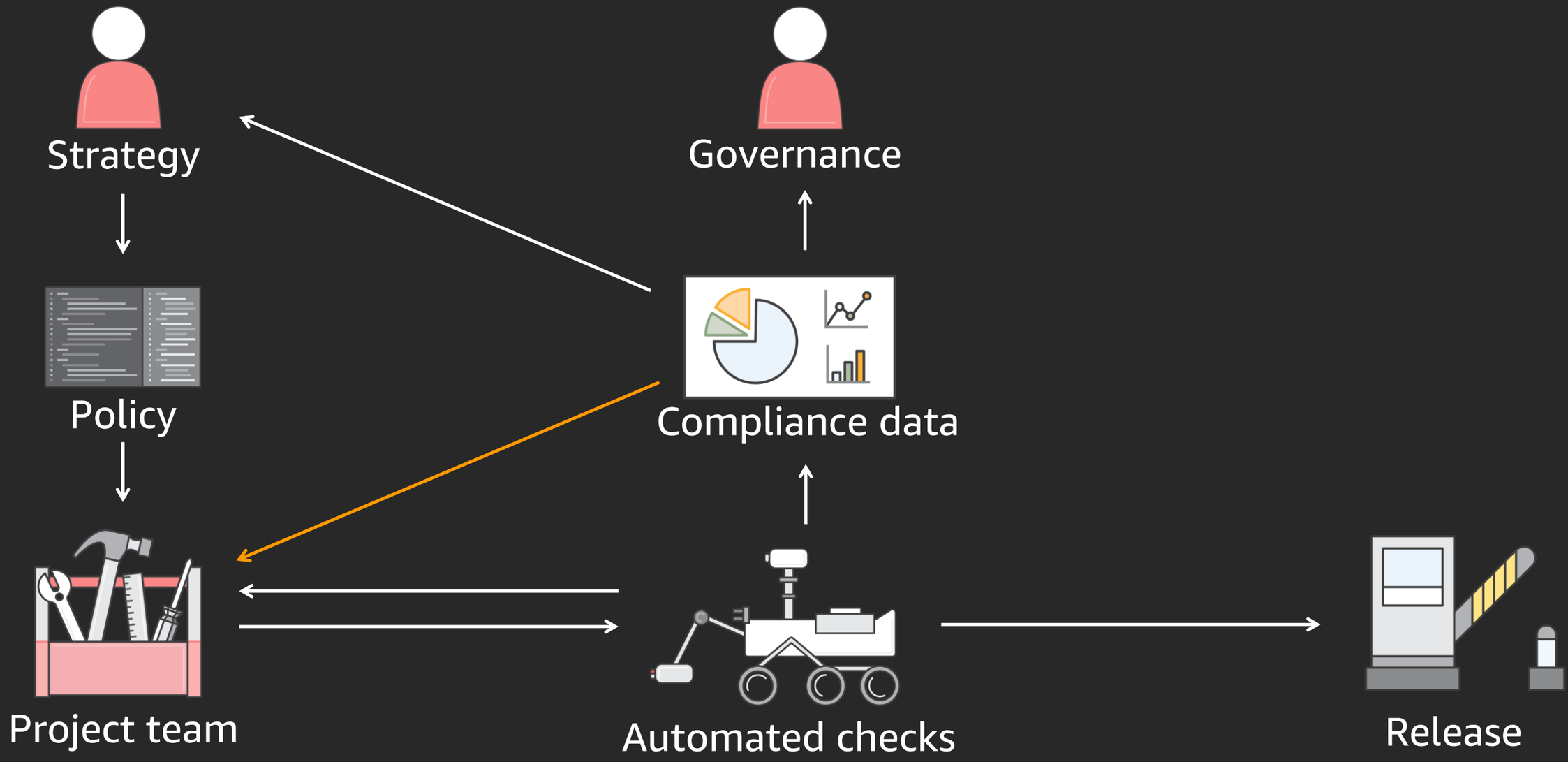
Governance at the speed of cloud



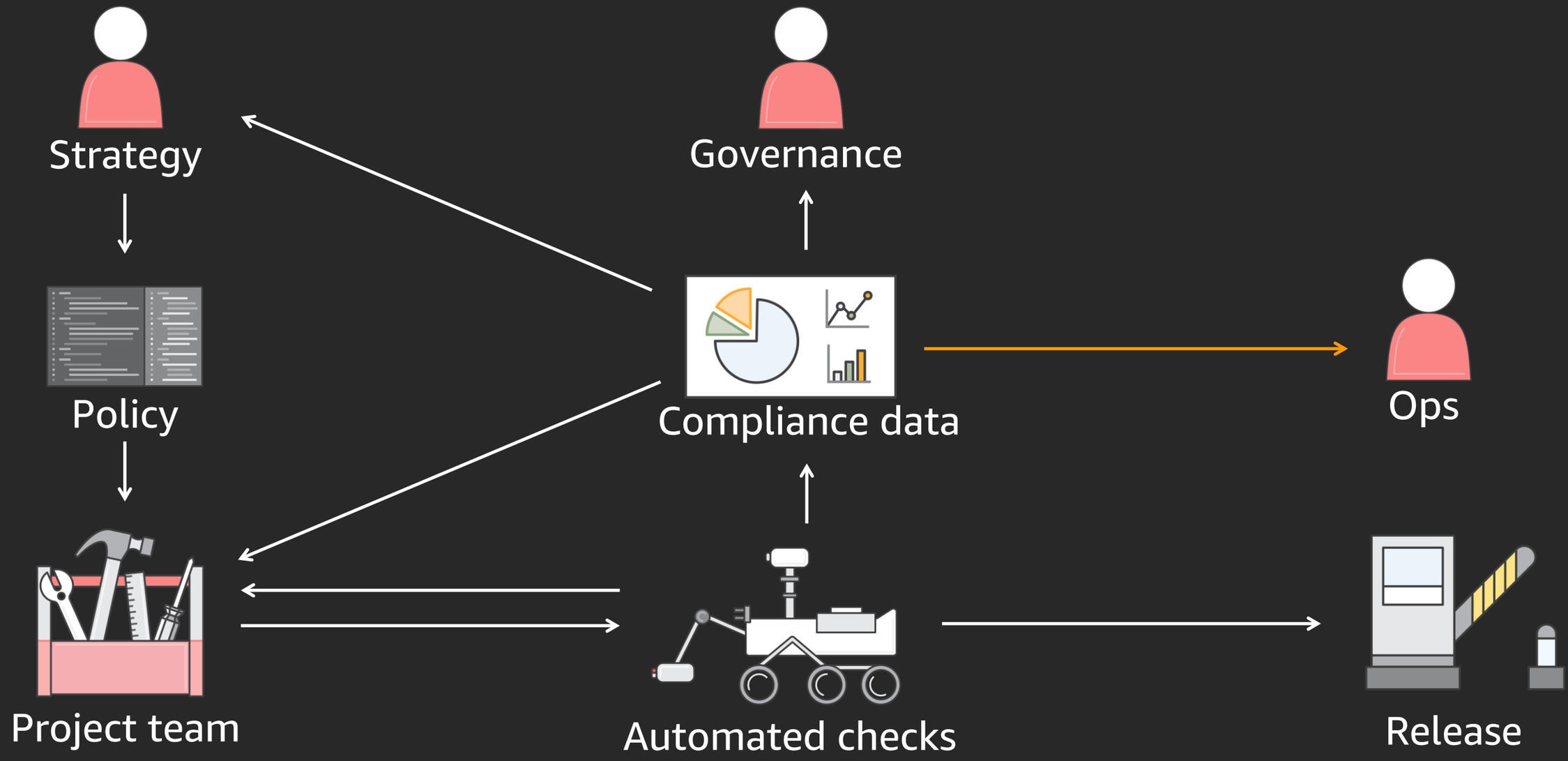
Governance at the speed of cloud



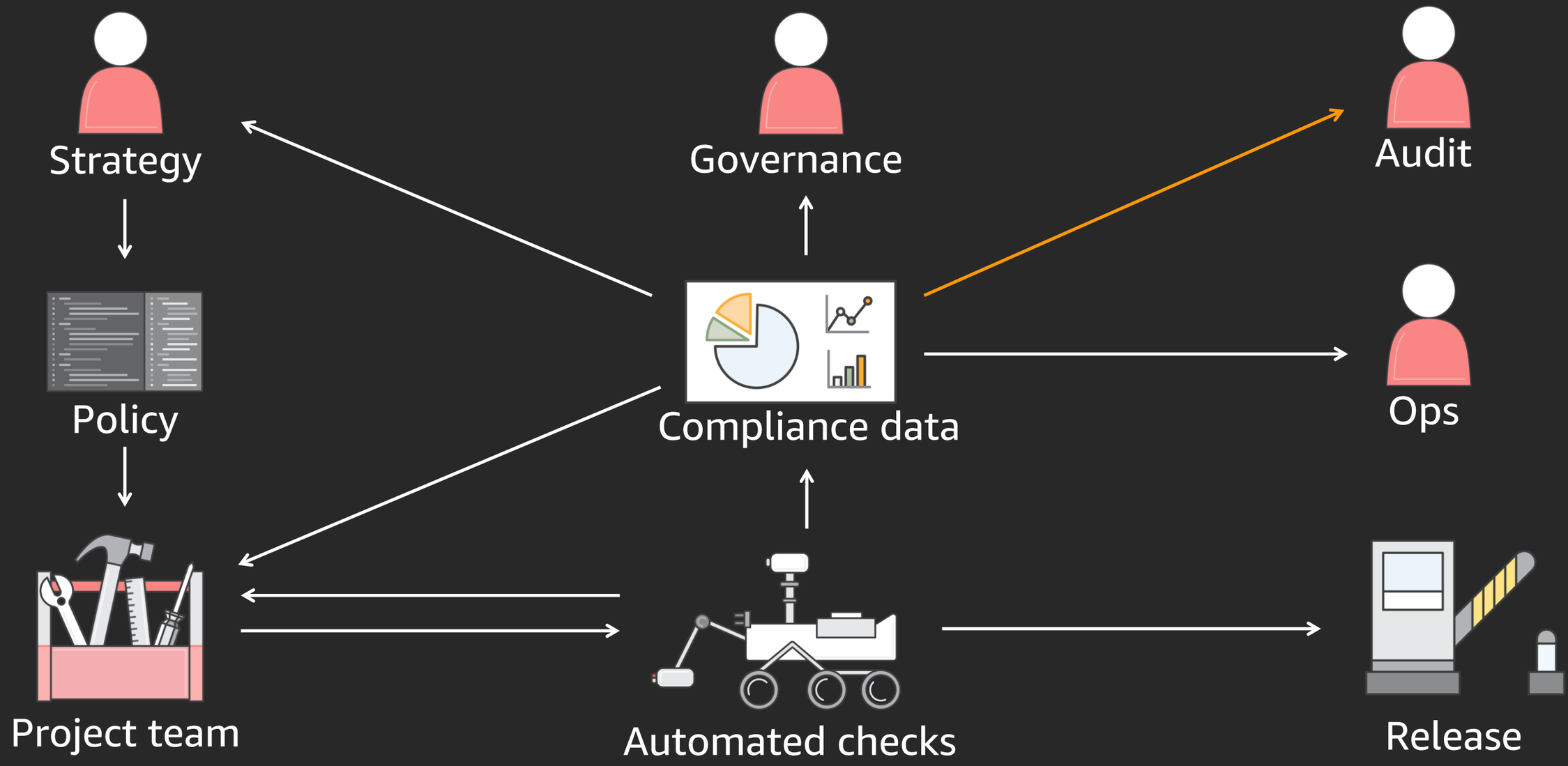
Governance at the speed of cloud



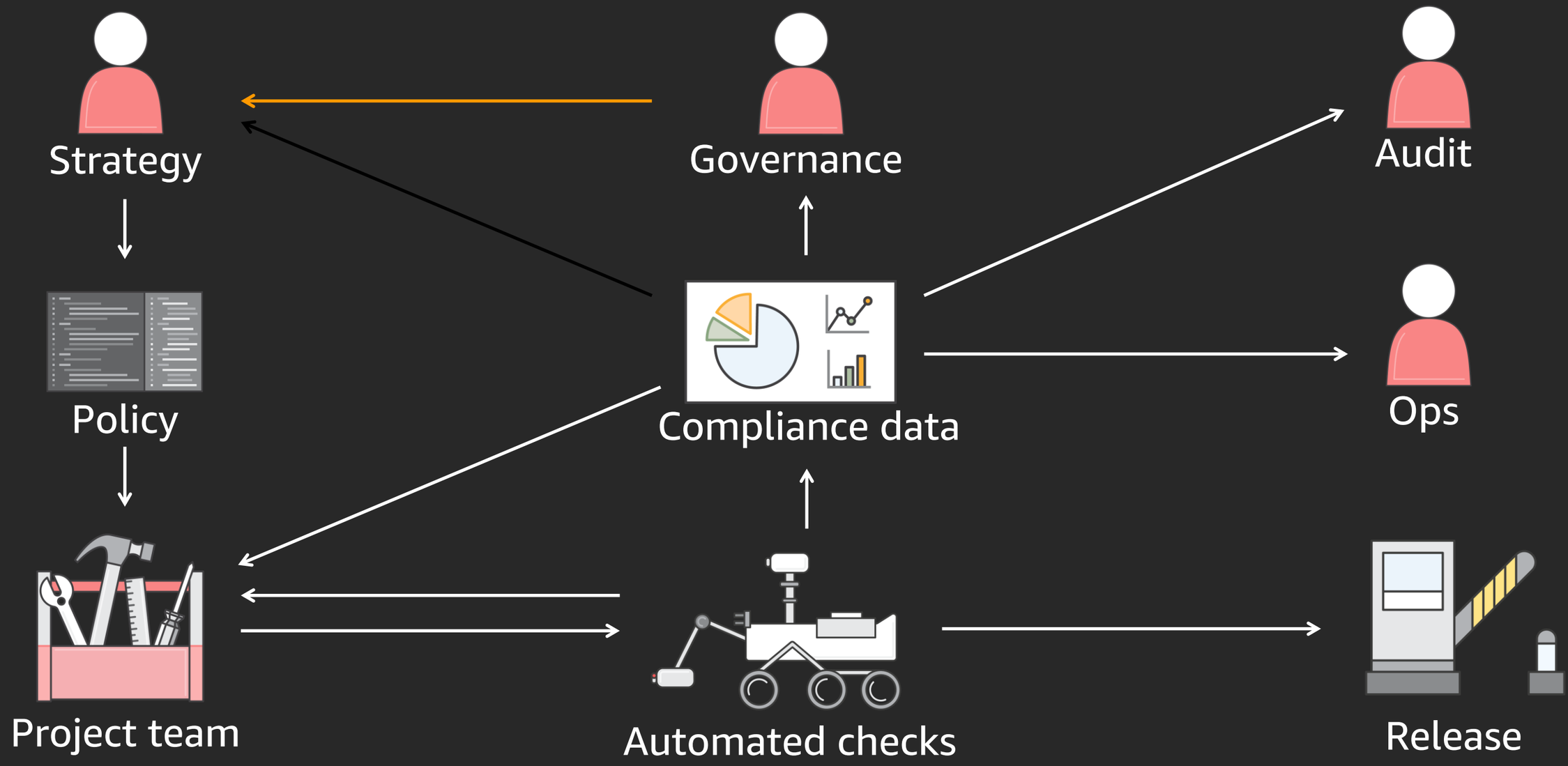
Governance at the speed of cloud



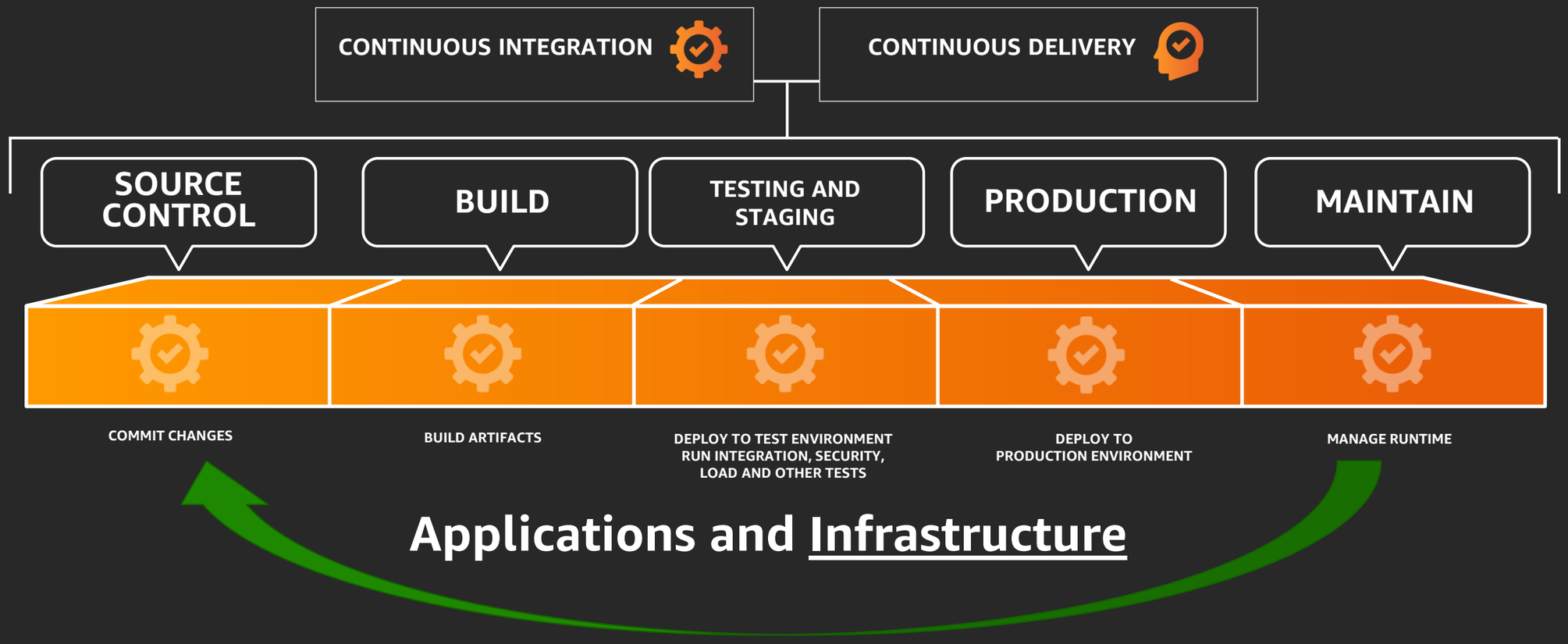
Governance at the speed of cloud



Governance at the speed of cloud



10. Be involved in the dev cycle

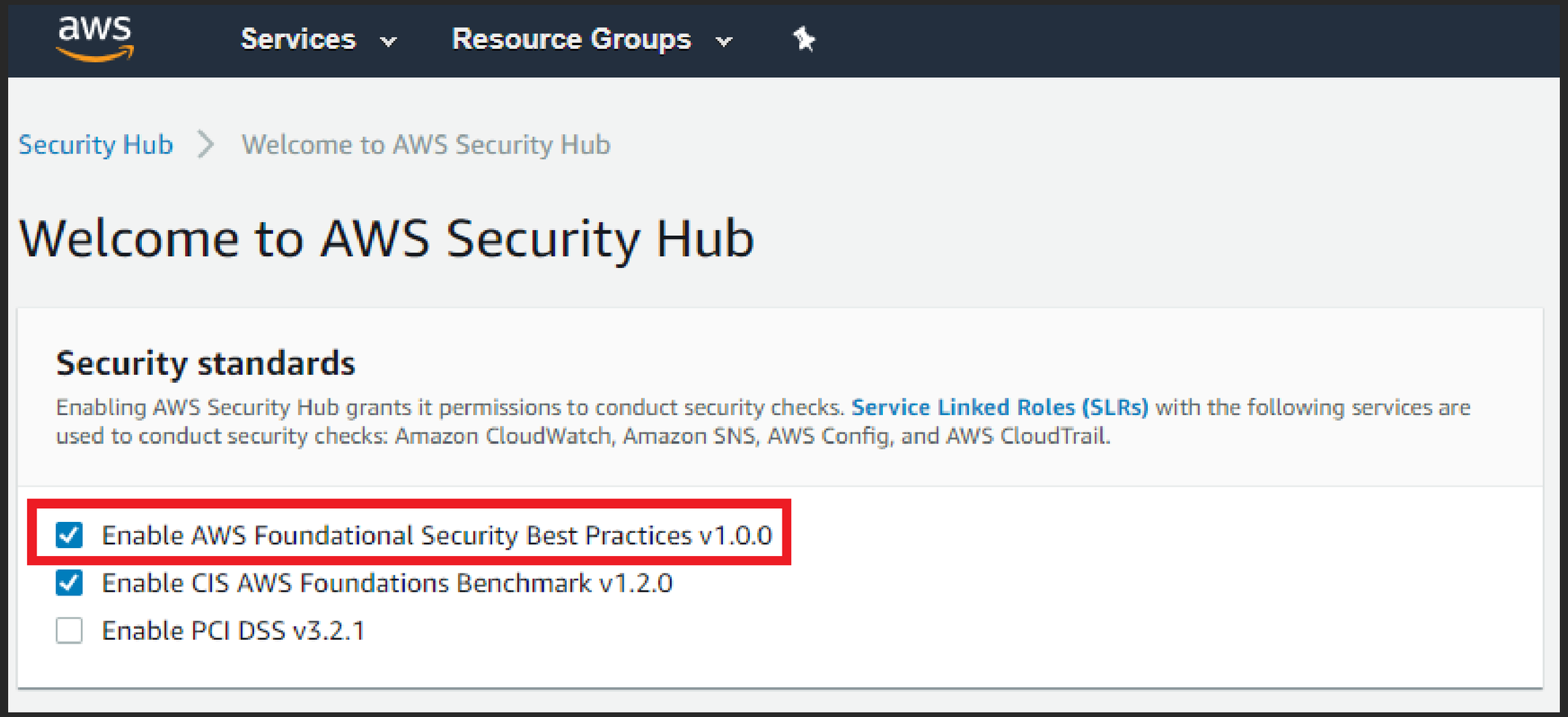


https://d1.awsstatic.com/executive-insights/en_US/ebook-cultivating-security-leadership.pdf

Ten places security teams should spend time

1. Account contact info
2. Use MFA
3. No hard-coding secrets
4. Limit security groups
5. Intentional data policies
6. Centralize AWS CloudTrail logs
7. Validate IAM roles
8. Take action on security findings
9. Rotate your keys
10. Involve security in the development lifecycle

Security Hub



https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-fsbp.html

Learn security with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud security skills

30+ no-cost digital courses cover topics related to cloud security, including Introduction *to Amazon GuardDuty* and *Deep Dive on Container Security*

Take one of the classroom offerings, like *AWS Security Engineering* on AWS, featuring AWS expert instructors and hands-on activities

Validate your expertise with the AWS Certified Security – *Specialty* exam

Visit the Learning Path at **https://aws.training/Security**

Thank you!

Tim Rains

www.linkedin.com/in/timrains

aws PUBLIC SECTOR SUMMIT ONLINE

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.