CLOUD DAY 2020

29 OTTOBRE • #CLOUDDAY2020

GOVERNANCE IN THE AWS CLOUD

A BALANCE BETWEEN AGILITY AND SAFETY

Paolo Latella
Claranet Italia

@LatellaPaolo

Kudos

Microsoft

managed/designs

AWS User Group - Italy

GDG Cloud Milano

Cloud Adoption – New rules

The right Cloud adoption start with identifying the gaps in **process** and **skills** between the traditional IT environment and the cloud environment.

People

Process

Agility

Ability to rapidly introduce new technologies and adapt the processes to market changes.

People

Process

Safety

Ability to maintain control over cost, compliance and security and define design principles

Cloud Governance Functions

Tecnologies

Cloud Resources

Dynamic infrastructure that provides disposable resources with pay-per-use model

Tecnologies

claranet

CLOUD DAY 2020
29 OTTOBRE 2020
ONLINE CONFERENCE

*Governance (in the Cloud) is a mix of processes, people and technologies that drive the Cloud adoption with goal to improve the enterprise's **Agility** without compromise the **Safety***

Governance – principles and challenges

Principles:

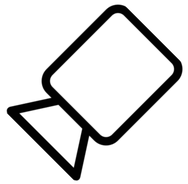
- Align Cloud strategy to Business objectives and IT strategies
- Identify and maintain required policies and compliances
- Create a CCoE (Cloud Center of Excellence) and delegate actions
- Define contracts with internal and external stakeholders
- Adapt career path

Challenges

- Identify the right KPI and ROI
- Risk Management
- Technologies proliferation
- **Balance Agility and Safety**

Safety - is not only (cyber) security

Responsive Control



Preventive Control

SAFETY

Knowledge

Centralize and Automate

Security Automation

Account Automation

Shared Services

SECURITY

Threat Detection

Data Protection and Encryption

Compliance regulations

Host and Endpoint Security

Infrastructure Protection

Operational auditing

Budget & Cost Management

Budget Planning

Budget Enforcement

Cost Monitoring

Guidance

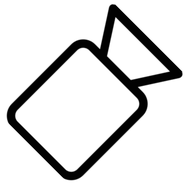
Best practices

Design principle

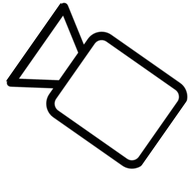
Configuration drift

Configuration Monitoring

Configuration Enforcement



Detective Control



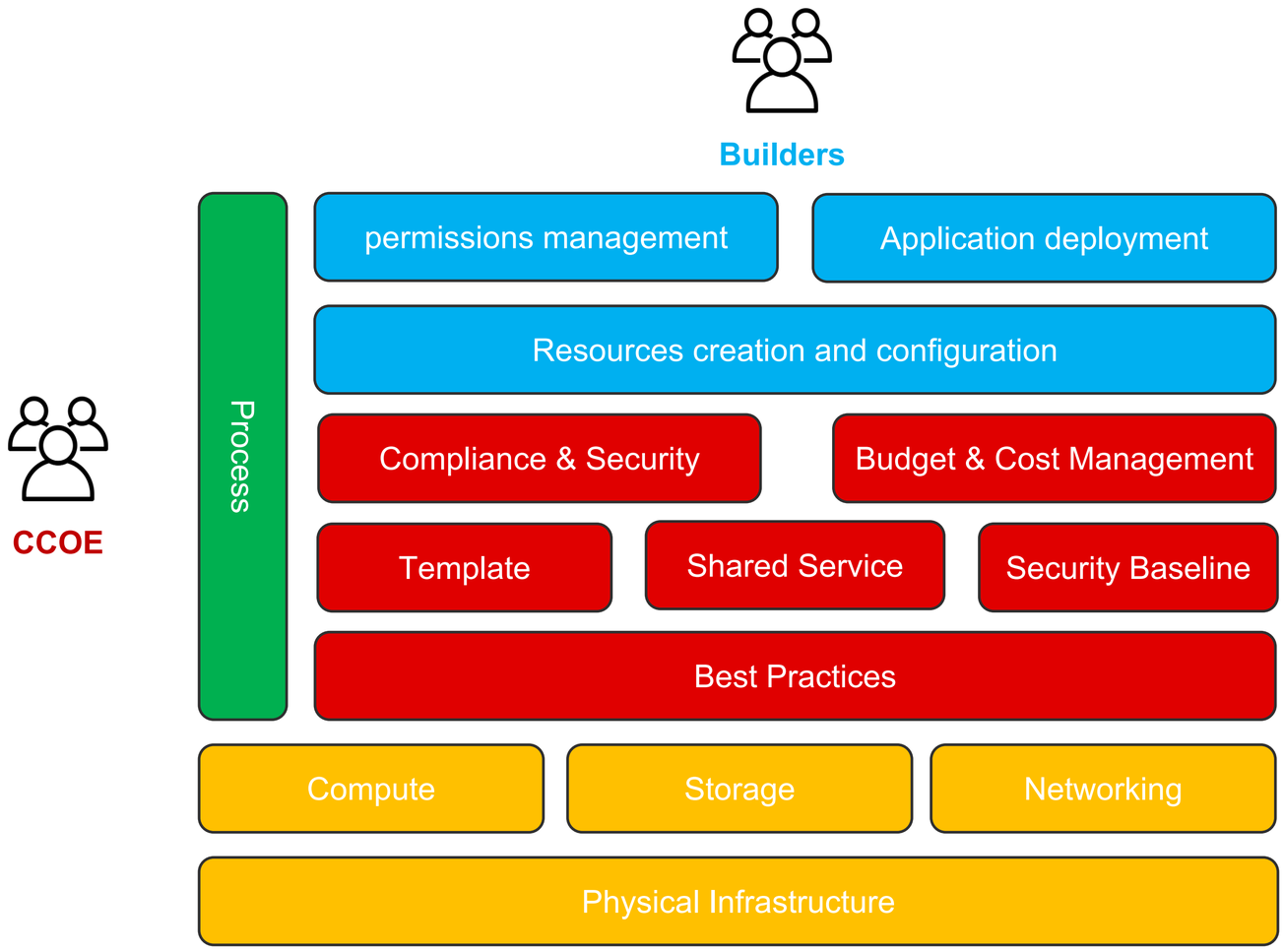
Directive Control

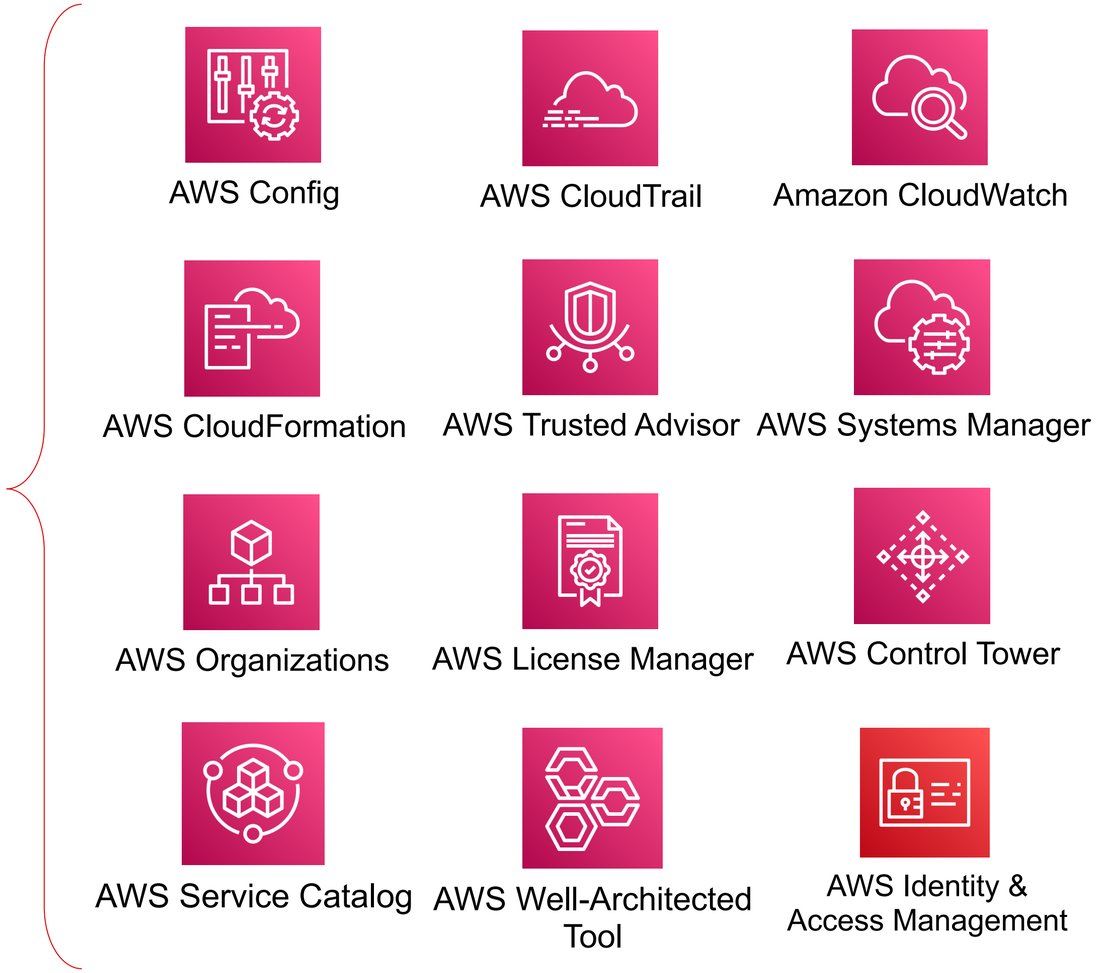
claranet

*Create a **Decentralized Governance** permit a great control over standards and costs (Safety) and allow better responsiveness to business needs (Agility)*

Photo by Mirko Blicke on Unsplash

Decentralized Governance



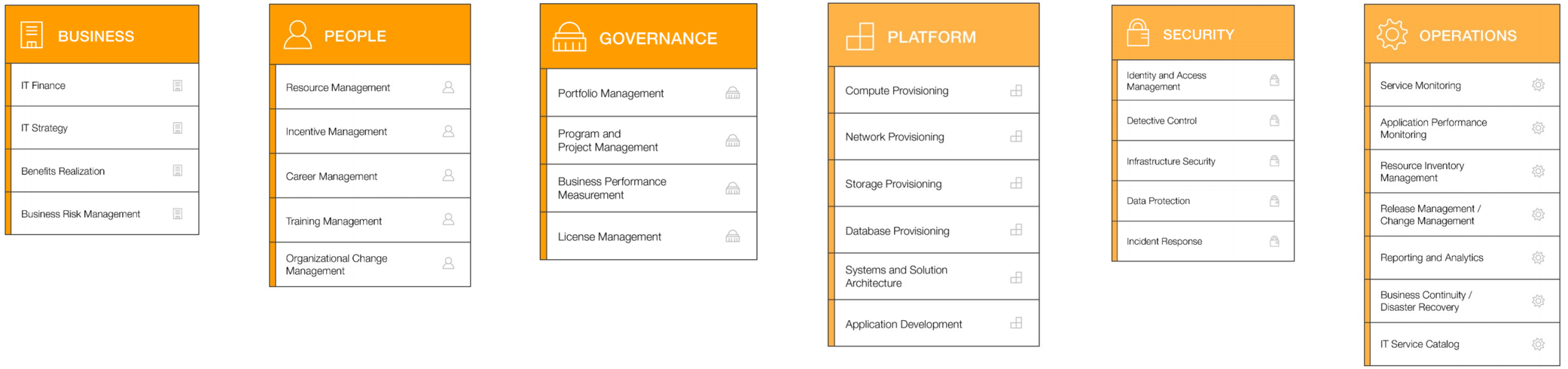


claranet

CLOUD DAY 2020
29 OTTOBRE 2020
ONLINE CONFERENCE

Establish Best Practices - CAF

- The **AWS Cloud Adoption Framework** helps organizations understand how cloud adoption transforms the way they work, and it provides structure to identify and address gaps in skills and processes.



Establish Best Practices - WAF

- The **AWS Well-Architected Framework** helps you understand the pros and cons of decisions you make while building systems on AWS. By using the Framework you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud.

OPS 4 How do you design your workload so that you can understand its state?

Design your workload so that it provides the information necessary across all components (for example, metrics, logs, and traces) for you to understand its internal state. This enables you to provide effective responses when appropriate.

SEC 8 How do you protect your data at rest?

Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.

REL 9 How do you back up data?

Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO).

PERF 7 How do you monitor your resources to ensure they are performing?

System performance can degrade over time. Monitor system performance to identify degradation and remediate internal or external factors, such as the operating system or application load.

COST 4 How do you decommission resources?

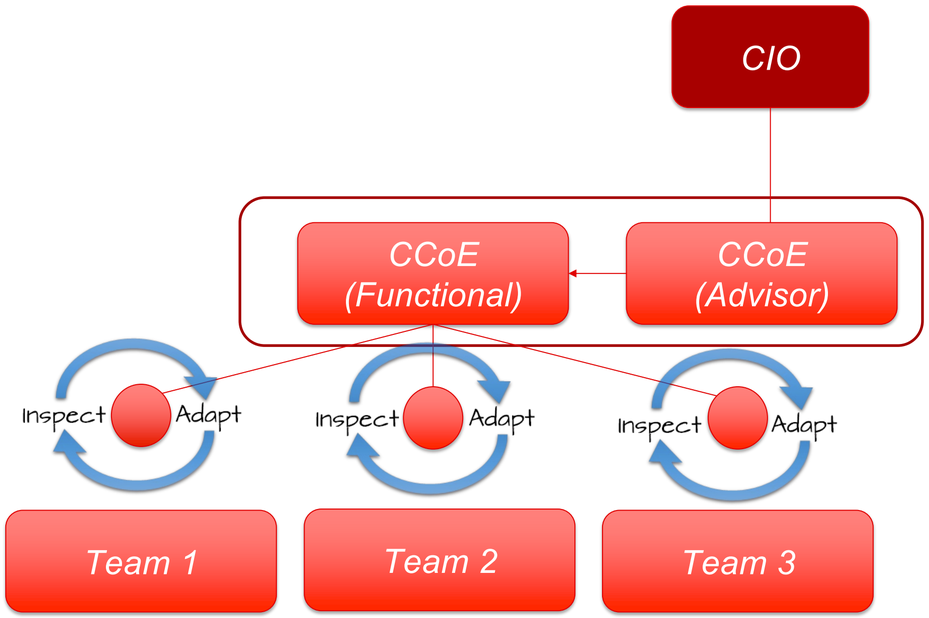
Implement change control and resource management from project inception to end-of-life. This ensures you shut down or terminate unused resources to reduce waste.

*It's important to develop a critical mass of people with AWS experience, establish operational processes and form a **Cloud Center of Excellence** (CCoE) that's dedicated to provide the right building blocks and best practices.*

Photo by Randy Fath on Unsplash

Cloud Center of Excellence (CCoE)

A CCoE develop and implement the solutions under the processes and principles that Governance has defined



Principles

- Drive Cloud Culture
- Engage and Evangelize
- Scale and Re-Organize
- Build Reference Architectures
- Improve agility and security

*Leave your builders to experiment and innovate in a safe environment leveraging the **security baseline** and related controls*

Photo by Science in HD on Unsplash

Security baseline

- It is important to define a security baseline, a set of security policy that must be met, and then ensure that they are being always applied.
  - Adopt principle of least privilege
  - Mix preventive and detective controls
  - Create baseline as a Service
  - Implement separation-of-duties
- Use “Security as Code” and “Compliance as Code” to maintain security without sacrificing business agility.
  - Define and codify security policies
  - Build, Test and Run your security policies in a DevOps approach

Security baseline – Organization and IAM

- AWS Organizations enables you to centrally manage and govern multiple accounts using Service Control Policies
  - Policies to centralize control over the AWS services and API - Preventive Controls
- AWS Identity and Access Management enables you to manage access to AWS services and resources in a specific account
  - Create and manage users and groups, and use permissions to allow and deny their access to AWS resources using least privileges principles
  - Exsplicit Deny on Identity based policy or Resource bases policy – Preventive Controls

Preventive Controls - SCP

Secure Control Policy (AWS Organization)

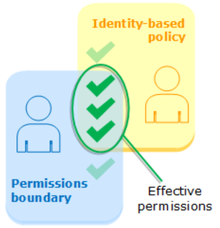
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunBigInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals":{
          "ec2:InstanceType":["r5.16xlarge","r5.24xlarge"]
      }
    }
    }
  ]
}
```

Identity Policy (AWS IAM)

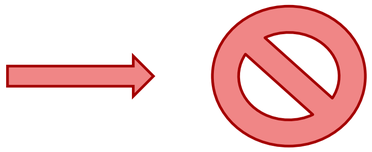
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

Preventive Control – Permission boundaries

```
aws iam put-user-permissions-boundary --permissions-boundary
arn:aws:iam::123456789012:policy/intern-boundary --user-name paolo.latella
```



Action = IAM: CreateUSer



```
aws iam attach-user-policy --policy-arn arn:aws:iam:ACCOUNT-
ID:aws:policy/AdministratorAccess --user-name paolo.latella
```

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "cloudwatch:*",
                "ec2:*"
            ],
            "Resource": "*"
        }
    ]
}
```

```json
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "iam:CreateUser",
    "Resource": "*"
  }
}
```

Permission boundaries – delegate responsability

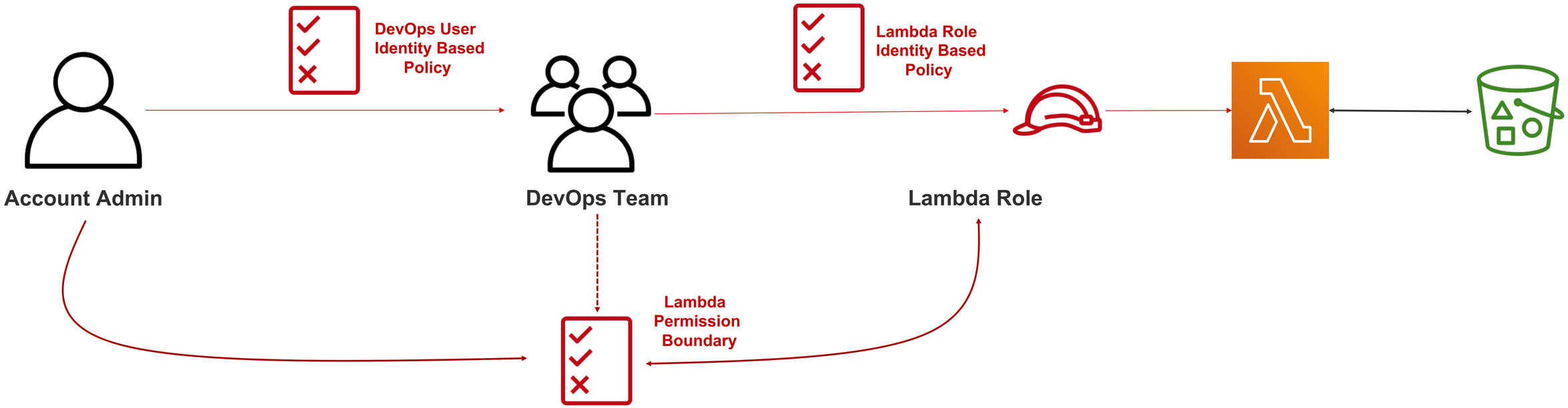
How I can delegate my DevOps team to create and attach role to AWS Lambda ?

Permission boundaries – delegate responsability

How I can delegate my DevOps team to create and attach role to AWS Lambda ?

```
"Effect": "Allow",
"Action": "iam:CreateRole”
"Condition": {"StringEquals": {"iam:PermissionsBoundary":
"arn:aws:iam::123456789012:policy/RolesBoundaries"}}
```

```
"Effect": "Allow",
"Action": ”S3:*"
```



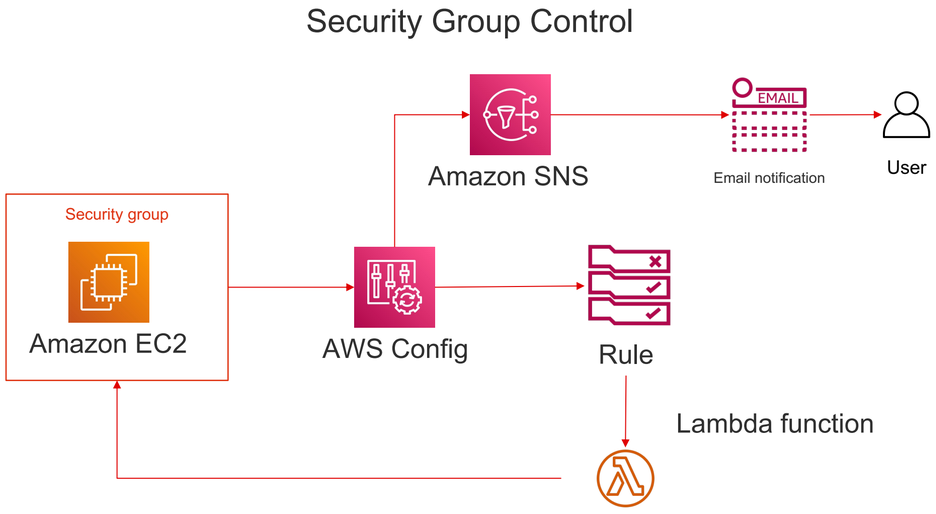

```
"Effect": ”Allow",
"Action": ”S3:GetObject"
```

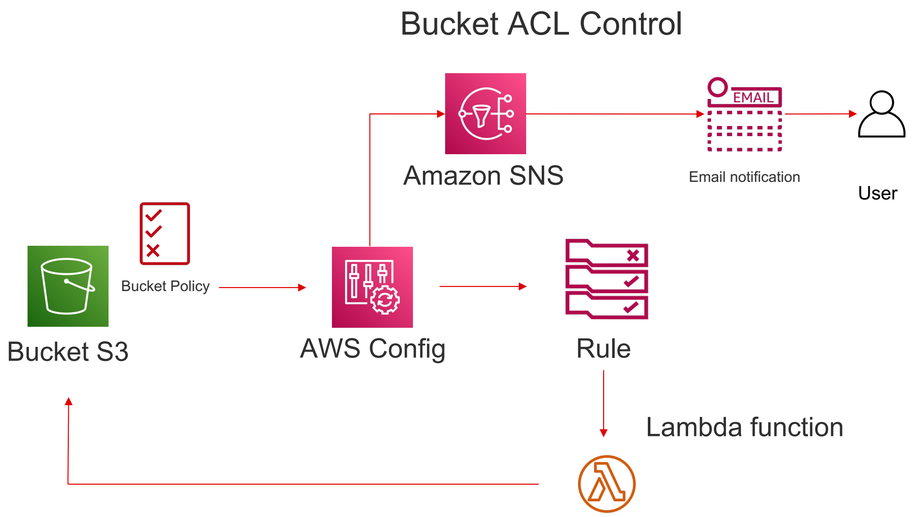
claranet

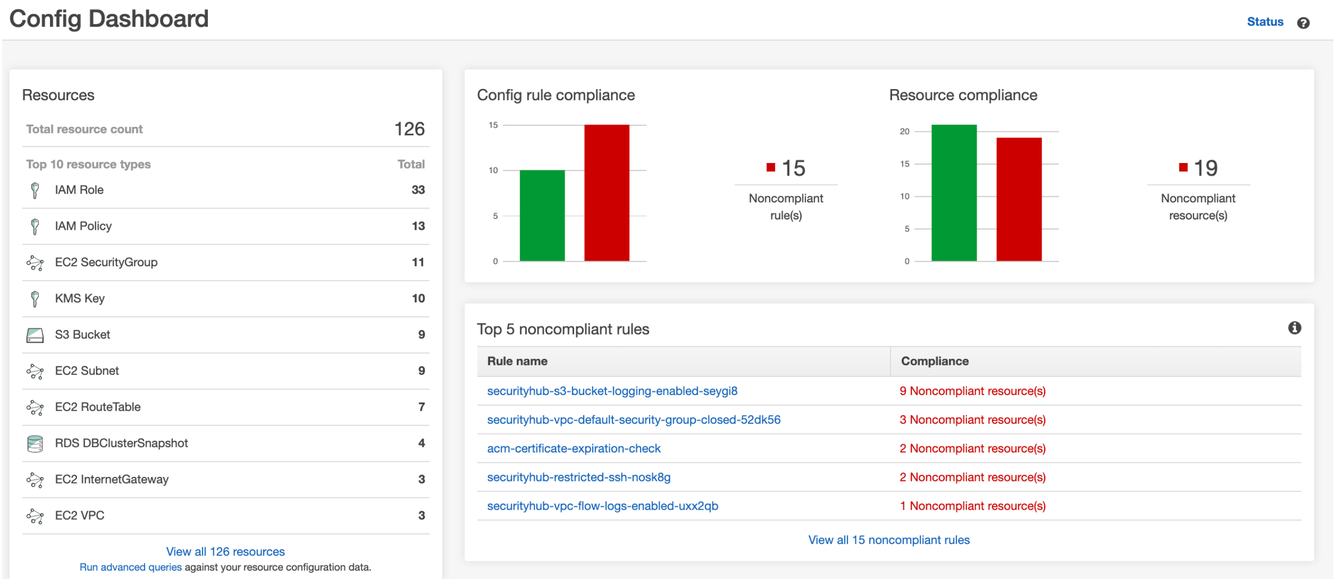
Security Baseline - AWS Config

- AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.
  - You can implement detective controls by processing events from your resources with goal to continuously audit and assess the overall compliance of your AWS infrastructure
  - You can implement “Compliance as code” defining your compliance requirements as AWS Config rules nd author remediation actions using AWS Systems Manager or AWS Lambda
- We can implement more detective control using CloudTrail and Cloudwatch Logs Insight together wit SNS / Lambda

Detective Controls – Config rules







Centralized and Aggregated Dashboard
- multi-account
- mullti-regions

claranet

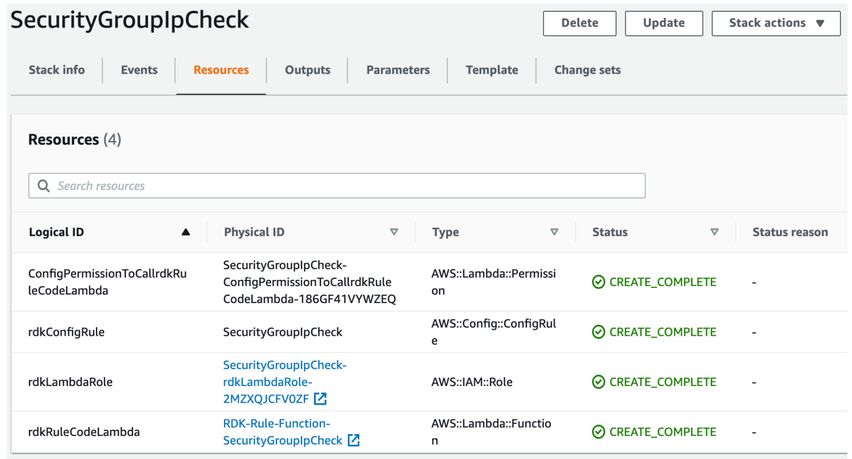
CLOUD DAY 2020
29 OTTOBRE 2020
ONLINE CONFERENCE

Config Rules – Compliance as Code

The RDK (Rules Development Guide) is designed to support a "Compliance-as-Code" workflow

```
rdk create SecurityGroupIpCheck --runtime python3.7 --
resource-types AWS::EC2::SecurityGroup --input-parameters
'{"allowedIP":"192.168.10.10"}'
Running create!
Local Rule files created.

rdk deploy SecurityGroupIpCheck
Running deploy!
Found Custom Rule.
Zipping SecurityGroupIpCheck
Uploading SecurityGroupIpCheck
Upload complete.
Creating CloudFormation Stack for SecurityGroupIpCheck
Waiting for CloudFormation stack operation to complete....
CloudFormation stack operation complete.
Config deploy complete.

rdk test SecurityGroupIpCheck
Running local test!
Testing SecurityGroupIpCheck
Debug!
test_sts_access_denied ... ok
test_sts_unknown_error ... ok
Ran 3 tests in 0.001s - OK
```

```python
def evaluate_compliance(event, configuration_item, valid_rule_parameters):
    """Form the evaluation(s) to be return to Config Rules

    Return either:
    None -- when no result needs to be displayed
    a string -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    a dictionary -- the evaluation dictionary, usually built by build_evaluation_from_config_item()
    a list of dictionary -- a list of evaluation dictionary , usually built by build_evaluation()

    Keyword arguments:
    event -- the event variable given in the lambda handler
    configuration_item -- the configurationItem dictionary in the invokingEvent
    valid_rule_parameters -- the output of the evaluate_parameters() representing validated parameters of the Config Rule

    Advanced Notes:
    1 -- if a resource is deleted and generate a configuration change with ResourceDeleted status, the Boilerplate code will put a NOT_APPLI
    2 -- if a None or a list of dictionary is returned, the old evaluation(s) which are not returned in the new evaluation list are returned
    3 -- if None or an empty string, list or dict is returned, the Boilerplate code will put a "shadow" evaluation to feedback that the eval
    """

    ##############################
    # Add your custom logic here. #
    ##############################

    return 'NOT_APPLICABLE'
```



claranet

https://github.com/awslabs/aws-config-rdk

CLOUD DAY 2020
29 OTTOBRE 2020
ONLINE CONFERENCE

Provide centralized and preconfigured services or resources to your builders with goal to simplify infrastructure, speed up a release of new products and adopt a separation of duties mindset.

Photo by Agnieszka Kowalczyk on Unsplash

Account Provisining – Control Tower

- A multi-account environment is an AWS best practice that permit
  - Administrative boundary
  - Workload boundary
  - Billing entity
- AWS Control Tower provides the easiest way to set up and govern a secure, compliant, multi-account AWS environment
  - Landing Zone
  - Account Factory
  - Guardrails by Secure Control Policies and AWS Config
  - SSO for administrators and end users

Shared Services

- Provide centralized services to your builders with goal to simplify infrastructure, speed up a release of new products and adopt a separation of duties mindset.
  - Create shared services Accounts / VPCs
  - Centralize cross-account services
    - Networking, Security, Logging, Identity, Template, Application Delivery
  - Define a shared responsibility model
- Governance must define the process and principles, CCoE define best practices and implement the solutions.

Templating

- Create and manage catalogs of Cloud resources that are already approved and ready to launch
  - Create template of virtual machine, software and resources
  - Centralize and automate management of this template
  - Define constraint and permission access
- AWS Service Catalog for define your own catalog of AWS services and make them available for your organization
- AWS Cloudformation for provision resources quickly and consistently by treating infrastructure as code
- AWS Systems Manager and Image Builder for creation, maintenance, validation, sharing, and deployment of images for use with Amazon EC2

Costs monitoring

- Cost Explorer is a tool that enables you to view and analyze your costs and usage
  - actual (hourly) and forecast
  - cost by project / service / tag
- AWS Budgets enable a simple cost and usage tracking – preventive control
  - Cost budgets – Plan how much you want to spend on a service.
  - Usage budgets – Plan how much you want to use one or more services
- Anomaly detection is an AWS Cost Management feature that uses machine learning to continuously monitor your cost and usage to detect unusual spends – detective control
  - Analyze and determine the root cause of the anomaly, such as account, service, Region
  - Not in real time

Take away

- Governance (in the Cloud) is a mix of processes, people and technologies that drive the Cloud adoption with goal to improve the enterprise's Agility without compromise the Safety
- Create a Decentralized Governance permit a great control over standards and costs (Safety) and allow better responsiveness to business needs (Agility)
- It's important to develop a critical mass of people with AWS experience, establish operational processes and form a Cloud Center of Excellence (CCoE) that's dedicated to mobilizing the appropriate resources.
- Leave your builders to experiment and innovate in a safe environment leveraging the security baseline and related controls
- Provide centralized and preconfigured services or resources to your builders with goal to simplify infrastructure, speed up a release of new products and adopt a separation of duties mindset.

paolo.latella@it.clara.net

@LatellaPaolo

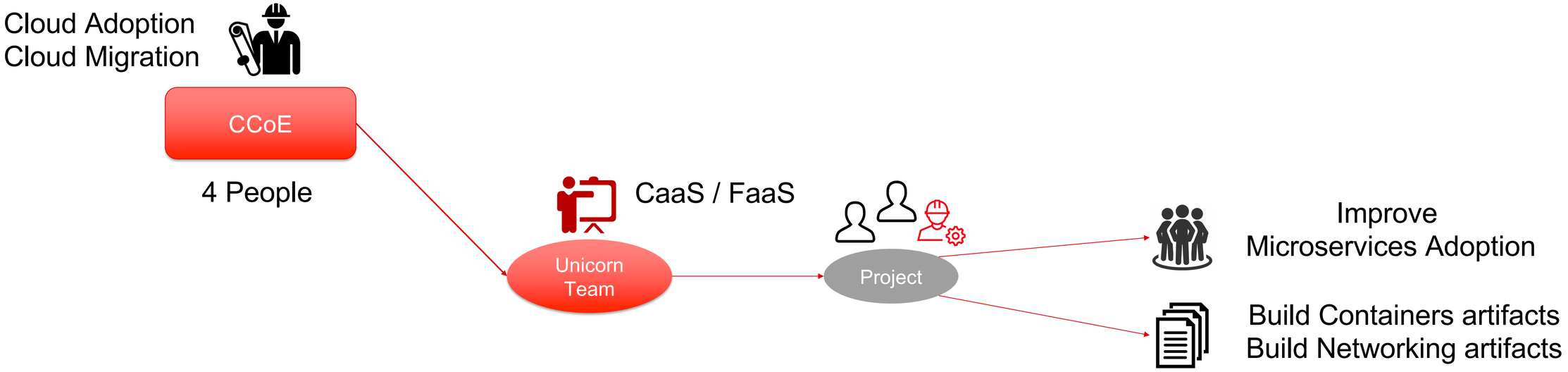
THANK YOU

https://www.meetup.com/Amazon-Web-Services-Rome

Appendix

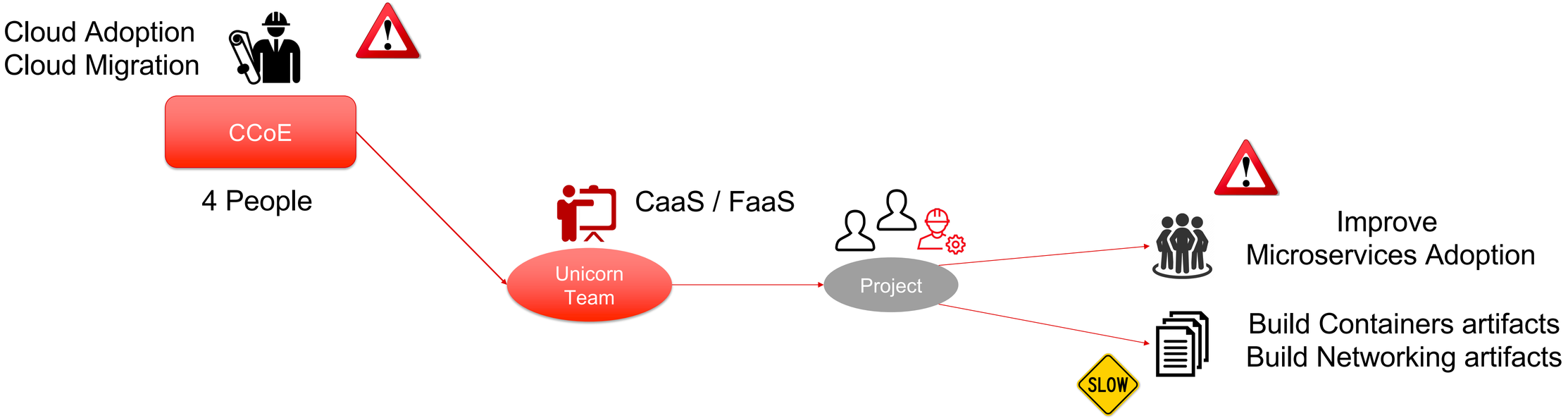
Appendix - CCoE – Use Case

1-2 Months



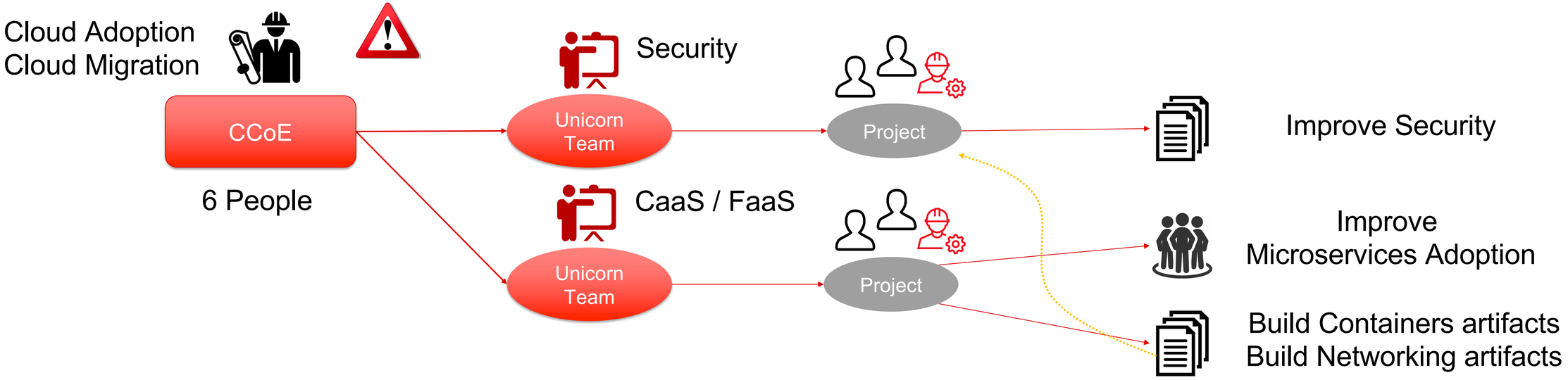
Appendix - CCoE – Use Case

1-2 Months



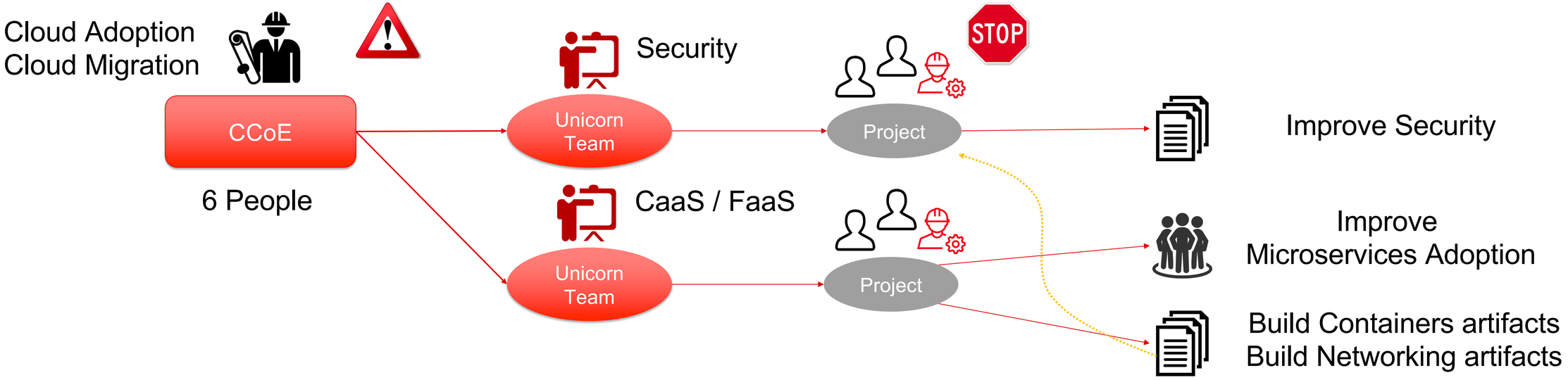
Appendix - CCoE – Use Case

2-4 Months



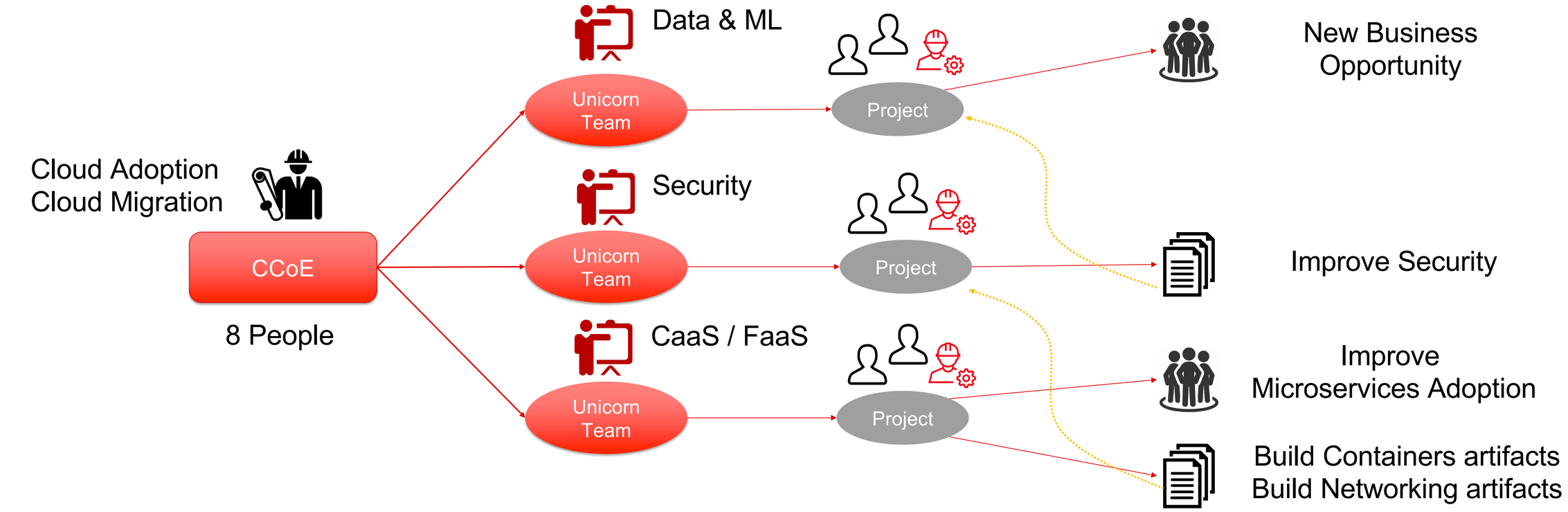
Appendix - CCoE – Use Case

2-4 Months



Appendix - CCoE – Use Case

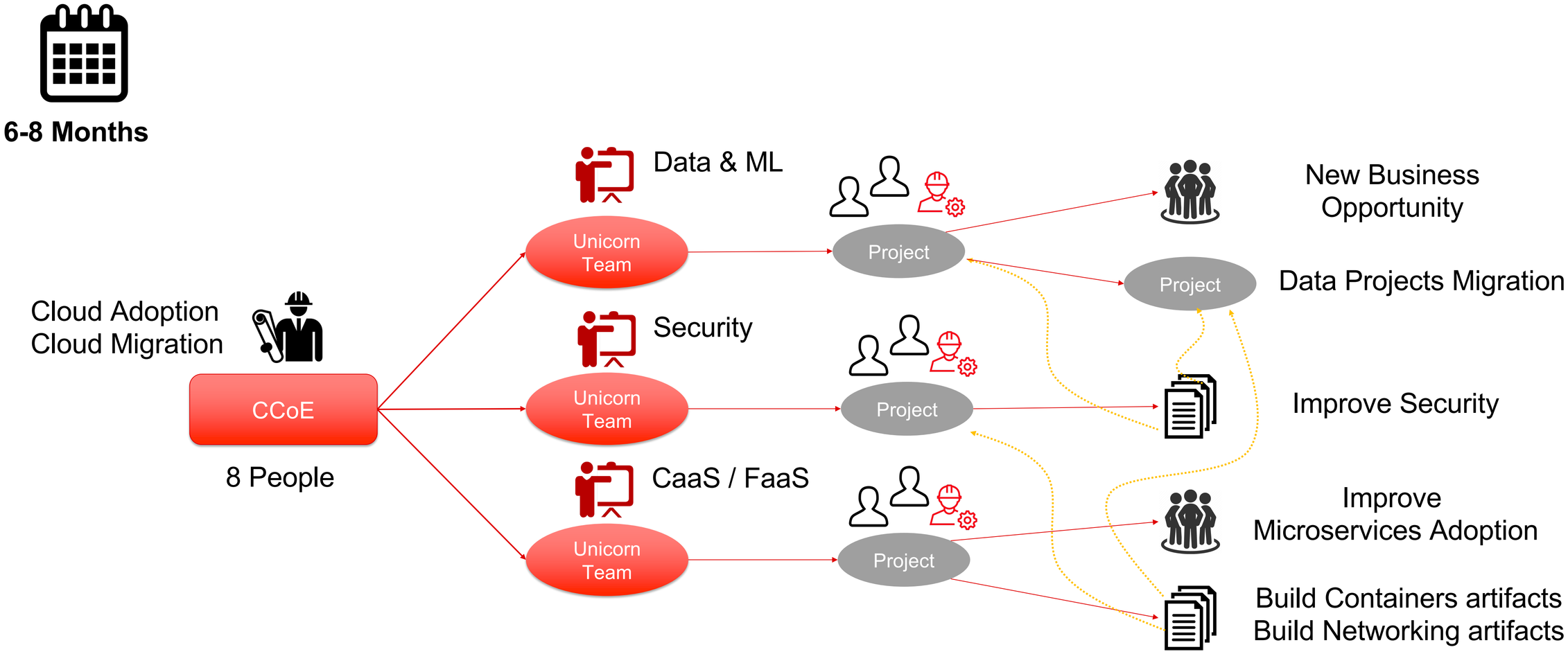
4-6 Months



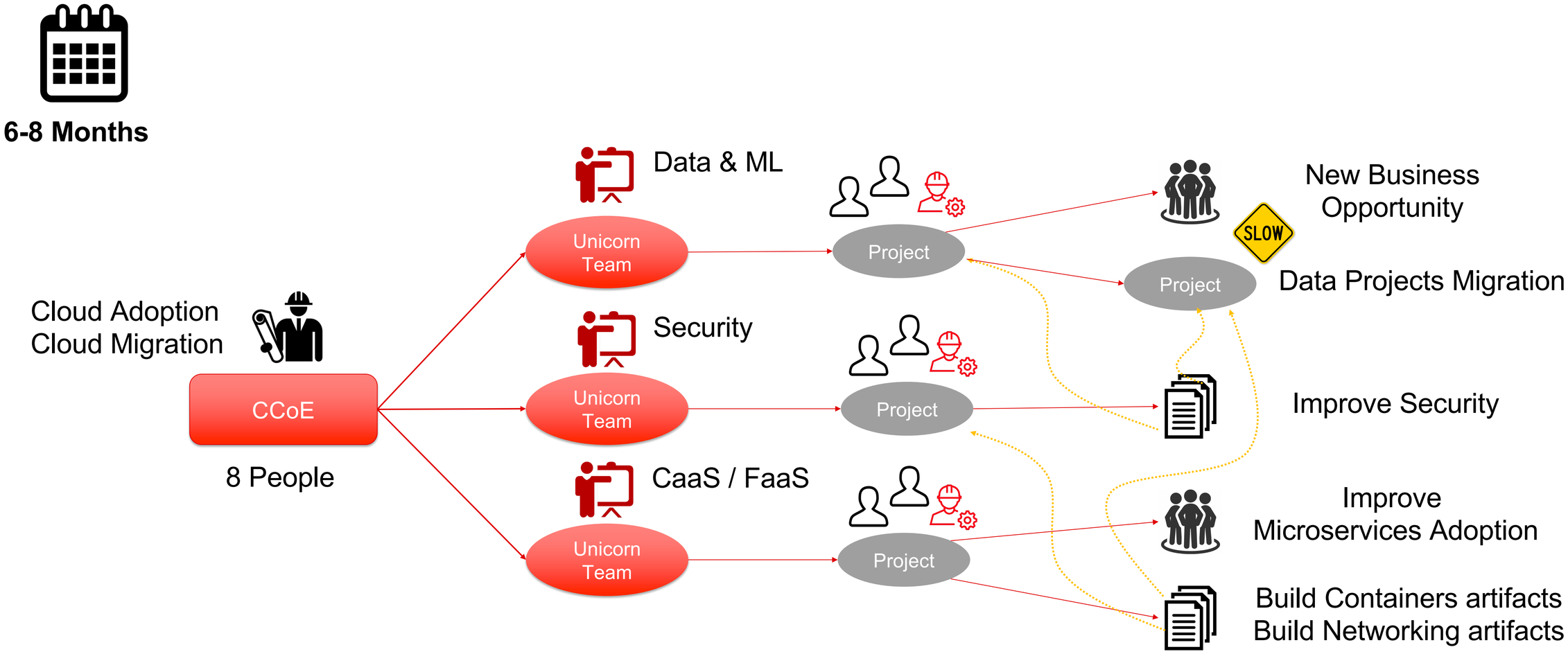
claranet

CLOUD DAY 2020
29 OTTOBRE 2020
ONLINE CONFERENCE

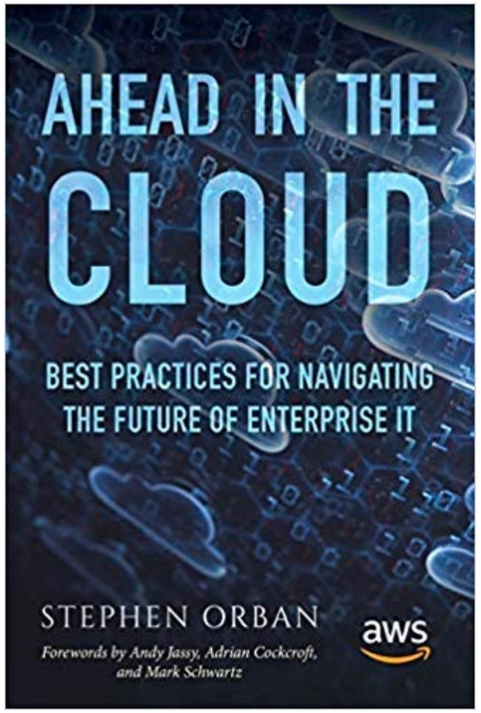
Appendix - CCoE – Use Case



Appendix - CCoE – Use Case



Reference



Gartner.

Evolve Your Infrastructure and Operations Organization to Remain Relevant in the Cloud Era

Published: 19 June 2017 **ID:** G00327279

Analyst(s): Craig Lowery

An effective move to public cloud requires profound changes in the structure, missions and roles of and within IT organizations. Infrastructure and operations leaders must implement these changes to ensure the ongoing success of their cloud strategies and the relevance of their organizations.

Key Challenges

- Cloud adoption will succeed in the long term, but only if IT organizations make fundamental changes in their organizational mission and team member roles.

An Overview of the AWS Cloud Adoption Framework

AWS Whitepaper

February 2017

amazon web services

claranet

CLOUD DAY 2020
29 OTTOBRE 2020
ONLINE CONFERENCE