Cloud Center of Excellence

Processes, Standards and Policies

Version 2.0

Last Update: 01/08/2020

For Internal Use Only

Contents

Cloud Center of Excellence (CCoE) Overview 3
Stakeholders of DevCare CCoE 3
Duties of Cloud CoE 3
Cloud Adoption Framework 4
Characteristics of DevCare Cloud CoE 4
Cloud COE activities 5
Adoption 5
Governance 6
Knowledge 6
Strategy 6
DevCare Cloud Center of Excellence Skill Sets 7
DevCare Cloud Practice Approach 8
Cloud CoE – Security Principles and Guidelines 8
Future Enhancements of Cloud CoE 10

Cloud Center of Excellence (CCoE) Overview

DevCare CCoE is used to bring together a diverse, knowledgeable group of experts from across the organization to develop best practices for the rest of the organization to follow. The best practices are cloud-focused, but center of excellence could be deployed for any long-term, strategic initiative the organization wishes to pursue.

Stakeholders of DevCare CCoE

- Leadership: DevCare CTO will establish and maintain credibility as well as give it the authority it needs to function as a governing body. CTO acts as the Executive Sponsor for the CCoE. CTO will serve as a high-profile evangelist both for the cloud and the CCoE' s mission.
- Operations: DevCare VP for Business Development and Director of IT Services will function in this domain so they can offer advice on things like application dependencies and how moving to the cloud will impact workflows, processes, and procedures. The VP for Business Development will guide the team in client and market on goings and focus areas.
- Infrastructure: DevCare's Head of Infrastructure will offer the lift-and-shift expertise you will need to figure out what cloud models will work for each scenario – IaaS, PaaS, SaaS, hybrid, private, and/or public. Ideally, they will know what infrastructure is currently being used to run which applications and store data and how transitioning to the cloud will change those dependencies.
- Security: DevCare's Security Architect along with Head of Infrastructure will provide governance in this area. Given that moving to the cloud will change how cybersecurity works at every application touchpoint from user authentication to networking, updating, and patching, we need to ensure that cybersecurity is baked into the cloud migration strategy from the beginning. Cybersecurity-as-an-afterthought is no longer an option today.
- Applications: DevCare's Director of IT Services will function as a lead for this governance area. The CCoE's main constituency is your application developers. The Director of IT Services will represent the concerns and challenges of this unique group of individuals will be key to the success of your cloud migrations.

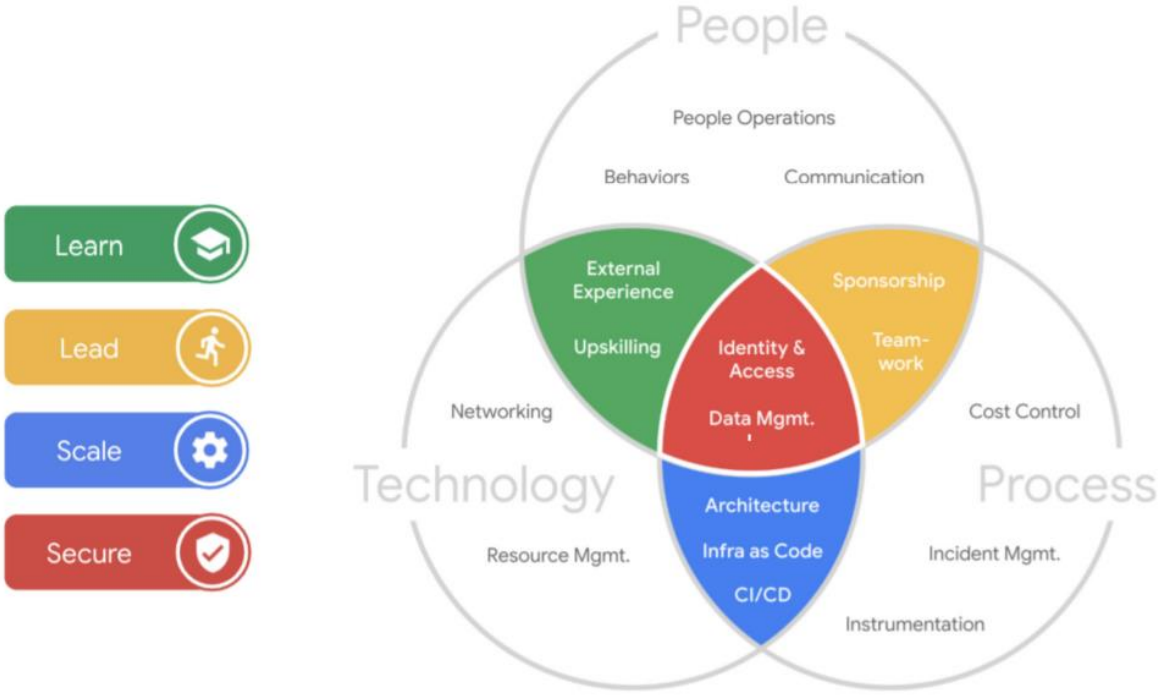
Duties of Cloud CoE

- The Cloud COE team accelerates cloud adoption by:
- Driving momentum across the organization
- Developing reusable frameworks for cloud governance
- Managing cloud knowledge and learning
- Overseeing cloud usage and plans for scale
- Aligning cloud offerings to the larger organizational strategy

A Cloud COE is not a static entity. Rather, it continually evolves to keep pace with the innovation associated with adopting the cloud. Executive leadership should design the Cloud COE as an adaptive structure that evolves as the needs of the organization do.

Cloud Adoption Framework

A successful Cloud COE is guided by the Cloud Adoption Framework, which builds a structure on the rubric of people, process, and technology that produces actionable programs within the themes of Learn, Lead, Scale, and Secure. This framework is informed by DevCare's evolution in the cloud offerings and expertise and many years of experience helping customers. The Cloud COE is the team that drives the cloud maturity of the organization forward and sets the agenda of the activities articulated in the Cloud Adoption Framework.



Characteristics of DevCare Cloud CoE

Central to the Cloud COE's role is setting the foundation for a successful cloud migration and encouraging a culture of collaboration and knowledge sharing. Cloud COE team members advise on and implement solutions, providing both thought leadership and hands-on support. In practical terms, a Cloud COE can be established based on practices, workstreams, processes, tools, or other significant structuring factors. As it is the needs, the priorities, and the capabilities of the business that drive the structure and scope of the

Cloud COE, each Cloud COE will look a little different. And the current state of cloud maturity of the team will drive its orientation and activities.

The most successful Cloud COE teams are:

- **Multidisciplinary**: Members of the team reflect the diverse perspectives of the stakeholders in the project.
- **Empowered**: The Cloud COE will have decision-making power without need for higher-level sign-off.
- **Visionary**: The Cloud COE will consider a multi-project viewpoint to understand repeatability and long-term benefits or goals for the organization.
- **Agile**: The Cloud COE will understand the necessary requirements to be able to deliver short term wins such as short development cycles and an iterative approach to building products.
- **Technical**: The Cloud COE will include experienced individuals with a history of architecting and building past solutions within the organization.
- **Engaged**: The individuals within the Cloud COE should be dedicated, able to commit full-time to the endeavor and the process.
- **Cloud-centric**: The Cloud COE will include members who will specialize in the cloud and cloud specific functions.
- **Integrated**: The individuals within the Cloud COE will be sourced from existing areas of the organization to allow for easy integration into existing teams and organizational constructs.
- **Hands-on:** Within a Cloud COE, there will be individuals who are able to do the hands-on work needed to build and test cloud solutions.

Cloud COE activities

Adoption

- Accelerate cloud adoption
- Increase cloud product/feature use
- Unlock cloud capabilities
- Implement a well-designed cloud architecture
- Advocate for cloud adoption by sharing success stories
- Develop reusable tools and artifacts
- Create and promote communication channels
- Minimize collaboration barriers across functions
- Define and monitor cross-functional collaboration activities
- Give employees access to information
- Delegate authority and empower employees to take decisions
- Encourage open communication throughout the organization

Governance

- Advise on cloud methodology
- Advise on release management
- Oversee cloud utilization and address under- and overutilization
- Improve data usage and management
- Standardize processes and methodologies
- Incorporate agile methodology in cloud releases Define cloud roadmap(s)
- Define future cloud products and features
- Align future cloud usage to the business roadmap
- Prepare for scale and optimization
- Tailor cloud architecture to business needs
- Develop management governance for the design, build, and release phases
- Build cloud architecture frameworks
- Design cloud processes
- Develop development guidelines

Knowledge

- Work with different functions to capture best practices
- Disseminate best practices across teams
- Continuously capture and propagate best practices
- Adjust processes based on best practices
- Create technical excellence within the organization
- Advise on the recruiting, training, and upskilling of cloud employees
- Serve as a centralized point of knowledge management
- Capture and encourage best practices
- Become the centralized point for questions about the cloud
- Support the development of the training approach
- Encourage continuous learning
- Develop a culture of excellence and knowledge
- Develop practices that are specific to the organization
- Develop points of view on the cloud and the organization
- Manage asset creation and publication

Strategy

- Prioritize projects and initiatives
- Deploy the cloud strategy
- Modernize infrastructure technology
- Accelerate go-to-market products
- Use the cloud to develop new use cases
- Spearhead technological innovations
- Align the cloud strategy to the larger organizational strategy
- Promote cross-functional integration
- Plan sprints, releases, and upgrades

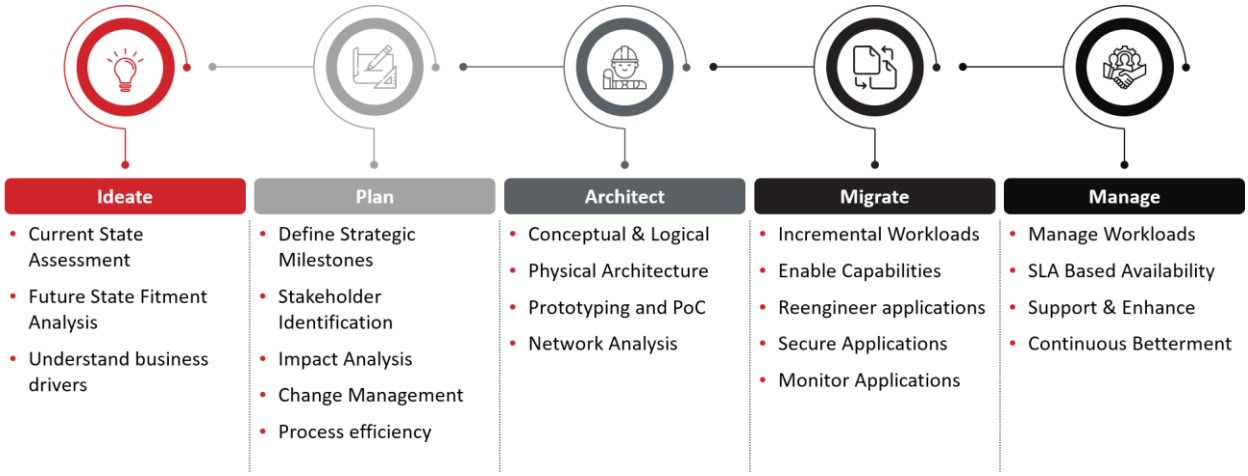
- Monitor access and identity

DevCare Cloud Center of Excellence Skill Sets

Cloud COE skill sets		
Skills	**Activities and tasks**	**Roles**
Project Management	**Strategy and adoption** • Develop repeatable assets • Create deployment checklists and scope exercises for sprints • Define scope and resources requirements for workstreams	• Cloud COE Lead • Cloud Engineering Lead • Data Scientist Lead • Developer Operations and Infrastructure Lead
Cloud Deployment	**Operations, knowledge, and governance** • Define a cloud migration checklist relevant to the organization • Establish governance frameworks • Understand cloud deployment best practices and CI/CD tooling	• Software Engineer/Cloud Architect • Network Engineer • Security Engineer • Cloud Engineer • Data Scientist • Data Analyst
Change Management and Support	**Operations and governance** • Communicate with both operations and development communities • Train and develop others • Manage change and communication activities within the organization • Influence support processes and requirements within the organization • Articulate DevOps or Site Reliability Engineering methodologies • Build the expertise in the cloud to be subject matter experts • Influence project teams to support their applications • Direct the success criteria of proof of concept workloads and use cases	• Site Reliability Engineer • Developer Operations and Infrastructure Engineer • Technical Solutions Engineer • Organization Change and Communications Specialist

DevCare Cloud Practice Approach

DevCare Cloud CoE has defined a robust approach for executing cloud migration and transformation efforts for our clients. The approach ensures all aspects of the cloud migration or transformation are executed with diligence.



While every phase is depicted as sequential, it is key to note that DevCare can establish an entry and exit at point in time with this framework.

Every phase has a set of predefined deliverables which can be customized to client needs.

Cloud CoE – Security Principles and Guidelines

Regardless of the cloud platform of choice for a client implementation, we follow strict Cloud Security guidelines and ensure all of them are met with industry mature practices.

1. Data in transit protection

User data transiting networks should be adequately protected against tampering and eavesdropping.

2. Asset protection and resilience

User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

3. Separation between users

A malicious or compromised user of the service should not be able to affect the service or data of another.

4. Governance framework

The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

5. Operational security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

6. Personnel security

Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

7. Secure development

Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.

8. Supply chain security

The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

9. Secure user management

Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorized access and alteration of your resources, applications and data.

10. Identity and authentication

All access to service interfaces should be constrained to authenticated and authorised individuals.

11. External interface protection

All external or less trusted interfaces of the service should be identified and appropriately defended.

12. Secure service administration

Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

13. Audit information for users

You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

14. Secure use of the service

The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

Future Enhancements of Cloud CoE

DevCare is working continuously and closely industry partners to expand the CCoE maturity. The next target areas for DevCare CCoE are:

1. ***Multi Cloud Architecture and Guidelines.***
2. ***Hybrid Cloud Architecture and Guidelines.***
3. ***Cloud Brokerage adoption.***