Keys to Successfully Implementing FinOps for Cloud

ITFMA Conference - St. Paul, MN

May 8, 2025

AGENDA

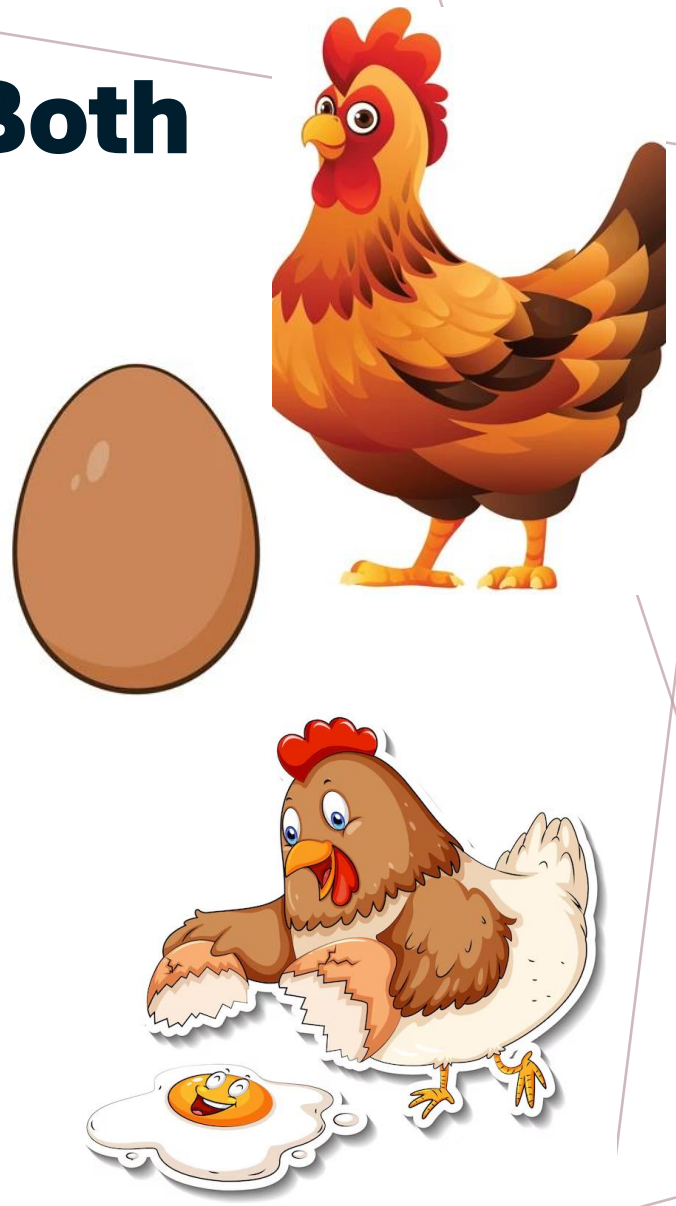
- Introduction
- ITFM vs FinOps
- Our Project
- Data and Tools
- Roles & Responsibilities
- We Did IT! Now What?
- Final tips & takeaways

ITFM & FinOps: Neither, Either or Both

Organization requirements, strategic priorities, levels of cloud adoption and financial management maturity all factor into this decision.

- Invest in ITFM to drive financial transparency, cost management and to help demonstrate value delivered by all IT spend.
- If cloud adoption is high or rapidly growing, FinOps brings the discipline to measure and manage the “all you can eat” buffet of cloud services.
- Integrate FinOps practices into the broader ITFM discipline to gain a holistic view of both cloud and non-cloud IT spend, and improve overall IT financial transparency and control.

ITFM and FinOps share the core principles of cost transparency and Optimization in pursuit of business value. We were already mature in ITFM so adding in FinOps was just another step along that journey at GuideWell.



Our Project

Our Timeline

February 2024

- Cloud Strategy & Governance
- Process Design & Tools Assessment
- Data Tagging
- Controls & Alerts
- Showback & Chargeback
- Design Reporting & Analytics
- Continuous Improvement

April 2025

Our Team

Our FinOps Structure

IT Finance

ITFM

Provides financial expertise and works closely to reconcile cloud provider invoices with cloud billing data to accurately forecast, budget and chargeback cloud costs.

- Financial expertise
- Budgeting and Forecasting
- Cost Allocation Analysis
- Financial Reporting

** NEW **

Bridge business, engineering, and finance teams to establish FinOps culture and enable evidence-based decisions to maximize the business value of cloud.

- Analytics
- Cost Management & Optimization
- FinOps Practice Continuous Improvement
- Problem Solving
- Change Management
- Cross-Team Collaboration

Operations (Engineering)

Infrastructure Services

Responsible for designing, managing and optimizing cloud infrastructure to achieve cost-effectiveness, performance, and reliability while ensuring the security and compliance of cloud environments.

- **Cloud Governance**
- Cloud Infrastructure Management
- Application & Service Deployment
- Resource Optimization
- Monitoring and Alerting
- Security and Compliance
- Automation and Tooling
- Architecting Sustainably for Cloud

FinOps Framework

finops.org/framework

FinOps is an operational framework and cultural practice which **maximizes the business value of cloud and technology**, enables timely data-driven decision making, and creates financial accountability through collaboration between engineering, finance, and business teams.

Principles

- Teams need to collaborate
- Business value drives technology decisions
- Everyone takes ownership for their technology usage
- FinOps data should be accessible, timely, and accurate
- FinOps should be enabled centrally
- Take advantage of the variable cost model of the cloud

FinOps Foundation

Business Strategy ↔ FinOps ↔ Technology Strategy

Scopes give context for Practitioners to apply the FinOps Framework.

Public Cloud | SaaS | Data Center | Licensing | AI | Custom

Core Personas are always engaged in a FinOps practice.

- Engineering
- FinOps Practitioner
- Finance
- Leadership
- Procurement
- Product

Allied Personas support a FinOps practice.

- ITFM
- ITAM
- ITSM
- Security
- Sustainability

Domains are the outcomes of a FinOps practice & **Capabilities** describe how to achieve them.

Understand Usage & Cost

- Data Ingestion
- Allocation
- Reporting & Analytics
- Anomaly Management

Quantify Business Value

- Planning & Estimating
- Forecasting
- Budgeting
- Benchmarking
- Unit Economics

Optimize Usage & Cost

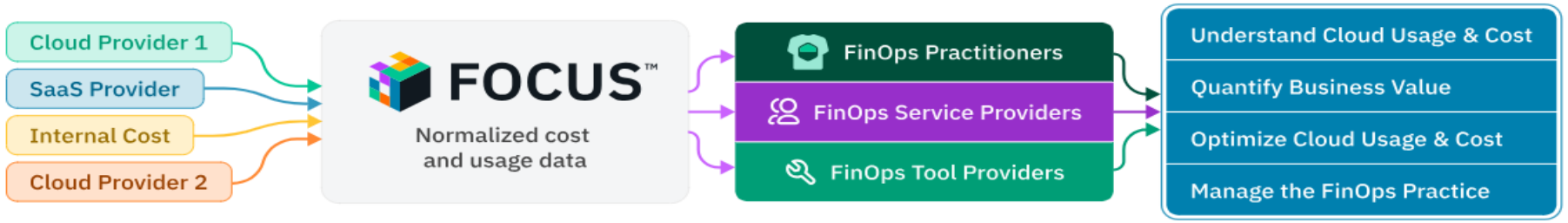
- Architecting for Cloud
- Rate Optimization
- Cloud Sustainability
- Workload Optimization
- Licensing & SaaS

Manage the FinOps Practice

- FinOps Practice Operations
- Policy & Governance
- FinOps Assessment
- FinOps Tools & Services
- FinOps Education & Enablement
- Invoicing & Chargeback
- Onboarding Workloads
- Intersecting Disciplines

FOCUS on the Data

- Tagging the data contained in the Cloud provider's invoice is KEY to automating the analytics, cost management and accurate showback / chargeback to users for their consumption.
- This is was "labor of love" engaging Engineering and ITFM. Security and Application Support teams also factored in to ensure alignment.
- We followed the international FOCUS framework to better enable future expansion of services, promote automation and enable future benchmarking endeavors.



See the Appendix for our Detailed Data Tagging Design

FOCUS Framework Illustration

Business Units & Applications

Business Unit 1 | Business Unit 2 | Business Unit 3 | Business Applications 1 | Business Applications 2 | Business Applications 3

Services

Delivery Services

Strategy & Planning

Technology Business Management
- Budgets

Innovation & Ideation

Enterprise Architecture

Program & Project Management

Business Solution Consulting

IT Vendor Management

Development

Design & Development
- CodeCommit
- CodeDeploy
- CodePipeline
- CodeBuild
- OpsWorks
- Application Insights
- HockeyApp
- Team Services
- Visual Studio
- Firebase
- Firebase Auth
- Firebase Database
- Firebase Hosting
- Source Respository

Testing
- Device Farm

System Integration

Support

Application Support
- Developer Support
- Business Support
- Enterprise Support
- XL SLES

Service Desk
- Connect

IT Training

Central Print

Operations

IT Service Management
- Config
- Service Catalog
- AWS Organizations

Monitoring
- CloudWatch
- Cognito
- CloudTrail
- Cognito Sync
- X-Ray
- Operational Insights
- Application Insights
- Monitor
- Log Analytics
- OMS Insight and Analytics
- Google Service Control
- Stackdriver
- Stackdriver Logging

Deployment & Administration
- EC2 Container Registry (ECR)
- Automation
- Container Builder
- Weaveworks

Capacity Management

Security & Compliance

Security
- Inspector
- Directory Service
- Key Management Service (KMS)
- Web Application Firewall (WAF)
- CloudHSM
- Shield
- Key Vault
- Active Authentication
- Active Directory Domain Services
- Multi-Factor Authentication
- Security Center
- Cloud Key Management Service (KMS)

Business Continuity & Disaster Recovery
- Recovery Services
- Site Recovery

Governance, Risk & Compliance

Platform Services

Data

Database
- Athena
- Cloud Directory
- DynamoDB
- Relational Database Service (RDS)
- SimpleDB
- Elastic MapReduce (EMR)
- HDInsight
- SQL Database
- DocumentDB
- StorSimple
- BigQuery
- BigQuery-Data Transfer Service
- Cloud Bigtable
- Cloud Spanner
- Cloud SQL

Distributed Cache
- ElastiCache
- Redis Cache
- Cache

Data Warehouse
- Redshift
- Synapse Analytics

Data Management
- Database Migration Service
- Data Pipeline
- Snowball
- Ingestion Service
- Data Pipeline
- API Management
- Data Factory
- Data Lake Analytics
- Data Lake Store
- Import/Export
- Time Series Insights
- Cloud Dataflow
- Genomics
- Komprise
- Transcode API

Data Analytics & Visualizations
- QuickSight
- Power BI
- Data Studio

Machine Learning
- Machine Learning (ML)
- Machine Learning
- ML API Services
- Cloud Dialogflow API
- Cloud ML Engine

Content Management

Applications

Application Hosting
- GameLift
- Lightsail
- Greengrass
- App Service
- Cloud Services
- Logic Apps
- Mobile Services
- Service Fabric
- Xamarin Test Cloud
- App Engine-App Services
- App Engine-Compute
- App Engine-Network
- App Engine-Storage

Search
- Top Sites
- CloudSearch
- OpenSearch Service
- Bing Autosuggest APIs
- Bing Search APIs
- Search
- App Engine-Search

Artificial Intelligence
- Cloud Natural Language API
- Cloud Video Intelligence API
- Cloud Vision API
- Prediction
- Translate
- Vertex AI

Message Bus & Integration
- API Gateway
- Simple Email Service (SES)
- Simple Notification Service (SNS)
- Simple Workflow Service (SWS)
- IoT
- Simple Queue Service (SQS)
- Pinpoint
- API Management
- IoT Hub
- BizTalk Services
- Event Hubs
- Mobile Engagement
- Hybrid Connections
- Service Bus
- Cloud IoT Core
- Cloud Pub/Sub
- SendGrid
- Zync

Streaming
- Elastic Transcoder
- Kinesis
- Stream Analytics
- Media Services
- Cloud Dataflow

Infrastructure Services

Network

Internet Connectivity
- DataTransfer
- Networking
- GCE-Network

Virtual Private Network
- Virtual Private Cloud (VPC)
- Direct Connect
- ExpressRoute
- Virtual Network
- VPN Gateway
- GCE-Network VPNTunnel

Domain Services
- Route53
- DNS
- Cloud DNS
- GCE-Network-IPAddress

Load Balancing
- Application Load Balancer
- Gateway Load Balancer
- Network Load Balancer
- Azure Load Balancer
- Google Cloud Load Balancer

Data Network

Voice Network

Compute

Virtual Compute & Containers
- EC2 Instance
- Elastic Container Service (ECS)
- Elastic Kubernetes Service (EKS)
- Azure Virtual Machine
- Azure Kubernetes Service (AKS)
- GCE Virtual Machine
- Google Kubernetes Engine (GKE)

Serverless Compute
- Lambda
- Functions
- Cloud Functions

Physical Compute

Mainframe

Storage

Networked Storage
- Elastic Block Storage (EBS)
- Storage Gateway
- Managed Disks
- Persistent Disk

File & Object Storage
- Simple Storage Service (S3)
- Blob Storage
- Cloud Storage

Backup & Archive
- Glacier
- Backup
- Nearline
- Coldline

Distributed Storage (CDN)
- CloudFront
- CDN
- Cloud CDN
- GCE-Network-CDNCacheFill

Legend

- Service Type
- Service Category
- Service Name
- AWS Service
- Azure Service
- Google Cloud Service
- Service with no AWS, Azure, or Google Cloud Service equivalent.

IT Towers

Data Center | Compute | Storage | Network | Output | End User | Application | Delivery | Security & Compliance | IT Management

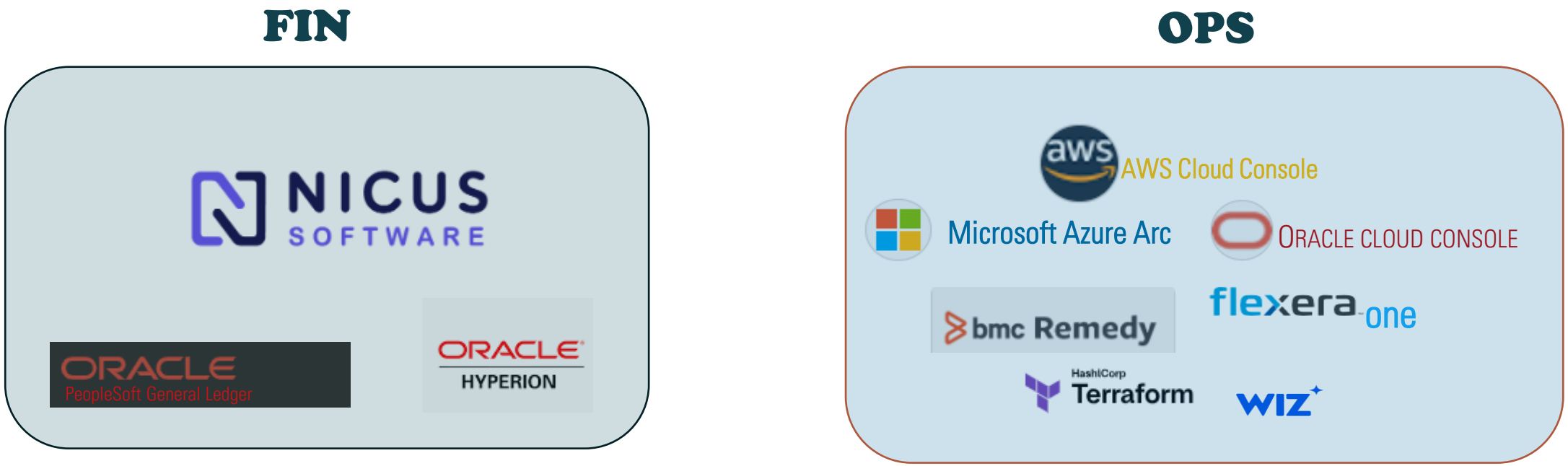
Cost Pools

Internal Labor | External Labor | Outside Services | Hardware | Software | Facilities & Power | Telecom | Other | Internal Services

Cloud Provider Billing Detail & Your Related Costs

Our FinOps Toolbox

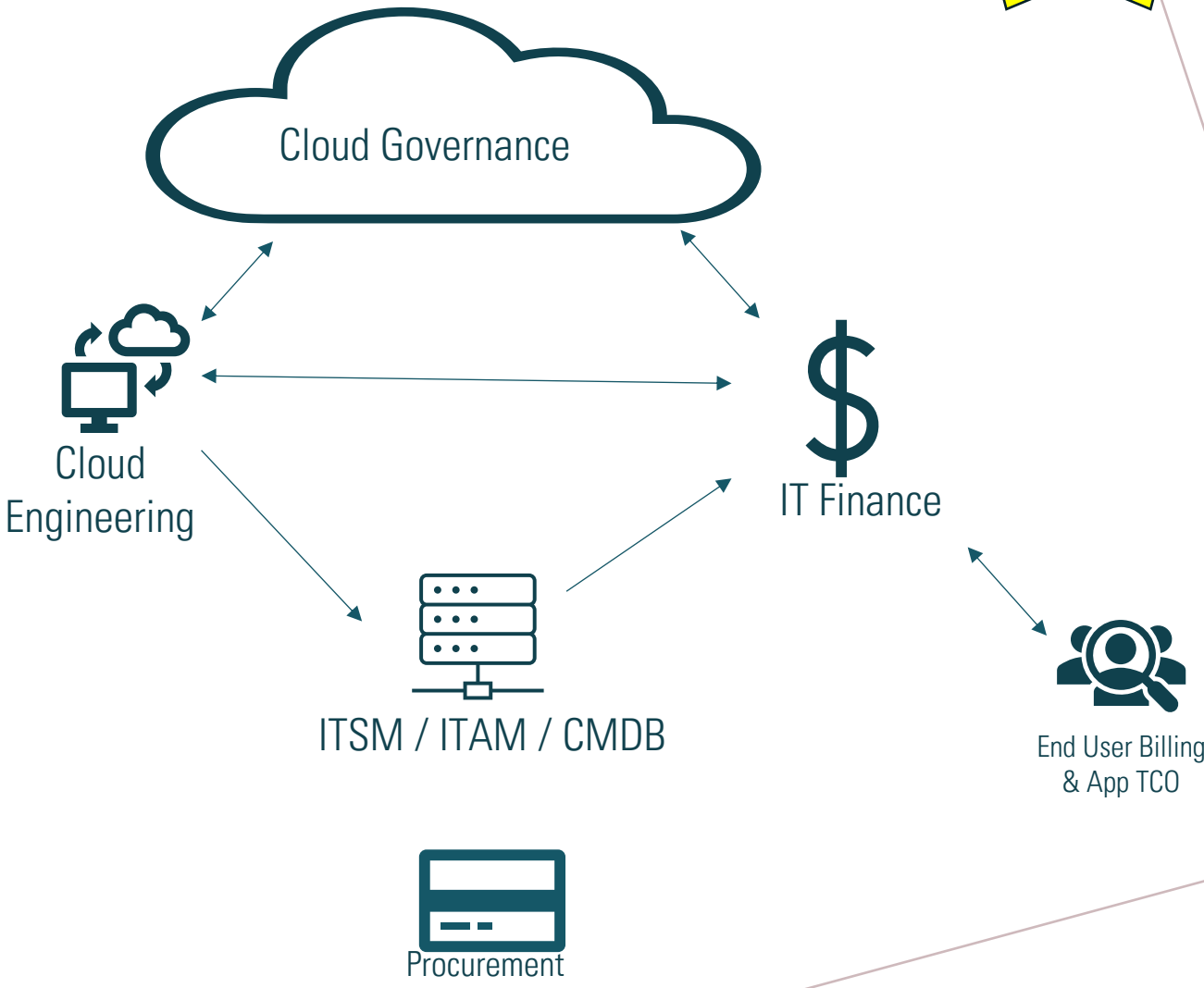
- To fully automate the FinOps process, we leverage an array of tools across Infrastructure Operations and IT Finance.



Roles & Responsibilities

- At GuideWell, we rely on stringent Cloud Governance as to WHAT workloads & data are best suited for the cloud, WHICH services they are likely to consume, and WHO will be billed for the charges (and HOW).
- Cloud Engineering will provision the new services in alignment with new CIs created in the CMDB. At the time of instantiation, the required metadata will be collected and stored for use in IT Finance for "billing" purposes.
- Each week, our data upload arrives from the external cloud providers. Any NEW services will be flagged for review and tagging. Once tagged, the data will be consumed by IT Finance for accounting and billing purposes.

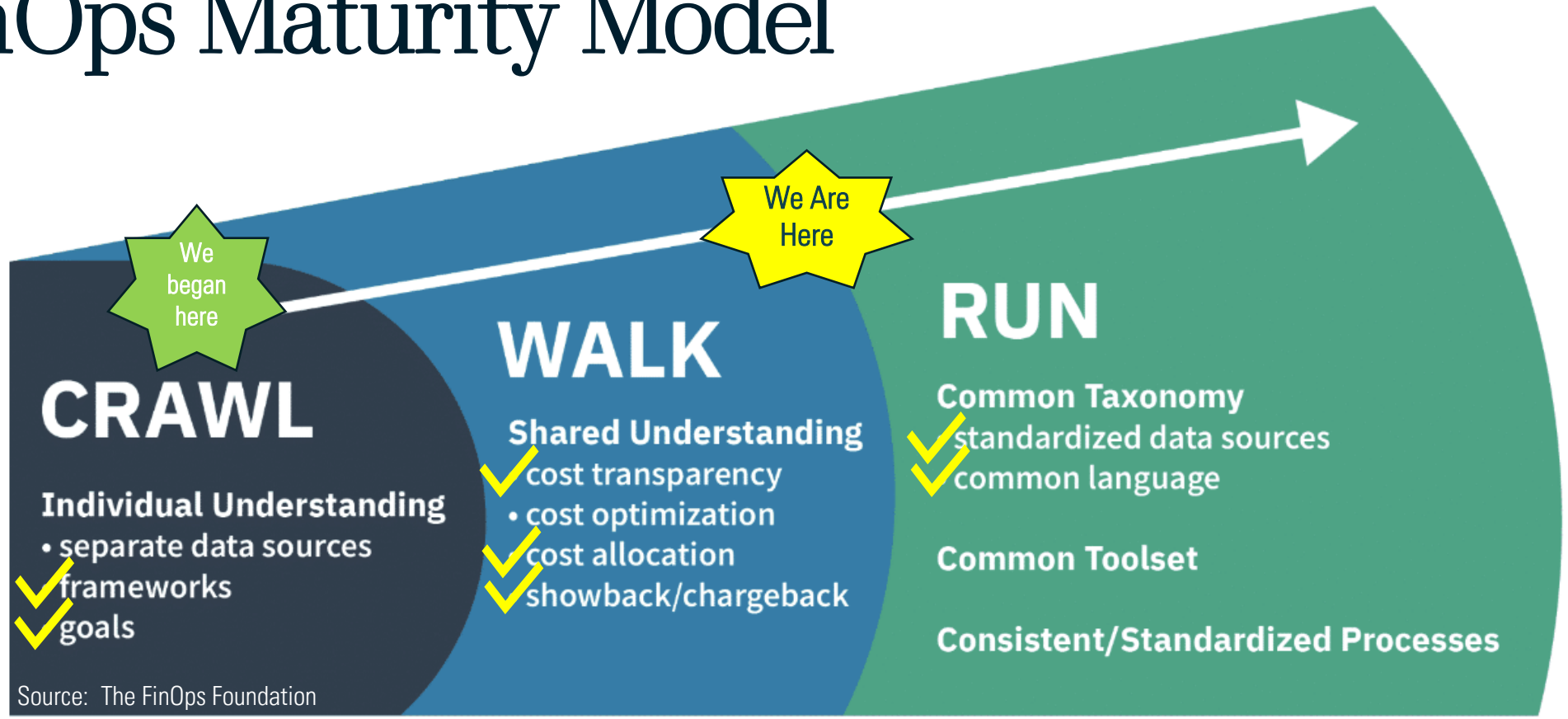
Well-defined Processes are KEY!



WE DID IT!

NOW WHAT?

FinOps Maturity Model



Focus now is on RUN, Optimize and Enhance Reporting and Analytics to support more informed Decision Making & Accountability with business partners. Next is learning how to forecast usage and build budgets for cloud expenses.

Lessons Learned

FinOps is a TEAM SPORT

- Engaging Key Stakeholders in every phase is critical to avoid rework.

Don't Reinvent the Wheel

- Leverage standard frameworks wherever possible.
- Fully leverage native management consoles before adding costs & complexities incumbent in adding tools.

Great Time to Reimagine Adjacent Processes / Tools

- Aligned with this capability, we reassessed the efficacy of other processes and systems such as ITAM, ISAM, ITSM, etc.

Man cannot live by DATA alone

- It is easy to focus on data mapping – and this is critical, but don't forget that FinOps involves numerous PROCESSES in Infrastructure Engineering, Vendor Management, Procurement and IT Finance.

Don't Be Afraid to Ask for Help

- We leveraged a partner to implement FinOps and as a Manager Service Provider to run the FinOps process, develop analytics templates, design stakeholder reporting and to teach us ways to optimize this process moving forward. We will rely on and learn from our partner for the first 6 mos. of RUN operations and then take the reigns.

Q & A

THANK YOU

Ginger Allen

904-563-3378 (please txt first)

ginger.allen@bcbsfl.com

APPENDIX

Resource Tagging Detailed Design

Version 1.3 (Work in Progress)
Created Date: 5/20/2024 | Modified Date: 6/25/2024

Purpose

Tagging allows administrators to assign metadata to resources and services, such as names, descriptions, labels, and categories. This metadata can be used to filter, search, and group resources and services, making it easier to manage and automate cloud infrastructure tasks.

Scope

The tagging strategy has been designed to be universally applicable on resources that reside on platforms that GuideWell uses. This includes, but is not limited to:

- Amazon Web Services (AWS)
- Microsoft Azure
- VMWare
- Nutanix
- OpenShift
- Oracle

Tags outlined here may be appended or enhanced as the process is implemented and as new requirements become identified.

Constraints

- Retroactively applying tagging standards to existing resources may be resource intensive.
- Platforms have a max length for tag key and value, and the number of tags.
    - AWS: Tag keys can have a maximum character length of 128 characters, and tag values can have a maximum length of 256 characters.
    - Azure: The tag name has a limit of 512 characters and the tag value has a limit of 256 characters. For storage accounts, the tag name has a limit of 128 characters and the tag value has a limit of 256 characters. Each resource, resource group, and subscription can have a maximum of 50 tag name-value pairs.
    - VMWare: You can use up to 256 characters for the name of the tag.
    - Kubernetes / OpenShift: must be 63 characters or less (can be empty), unless empty, must begin and end with an alphanumeric character ([a-z0-9A-Z]), could contain dashes (-), underscores (_), dots (.), and alphanumeric between.

Tags Design

As a baseline standard, the listed tags are universally applicable to any resource. Additional tags can be applied to a given resource as needed, but this document should be revised to include them if they would be needed universally.

Tag Key	Description	Details	Required	Example Value(s)	Required by
company	The GuideWell company that the resource is being deployed to support.	Comes from the request ticket.	Y	Florida Blue GuideWell GuideWell Source First Coast Service Options, Inc. Novitas Solutions, Inc.	ITIS
application	Name of application, service, or workload the resource is associated with.	Comes from the request ticket, aka Technical Service (Application) the user selects on the request form.	N	CIP – Consumer Information Platform	FinOps
environment	Deployment environment of this application, workload, or service.	Comes from the environment selected on the request ticket	Y	prd stg tst unt sbx	FinOps
costCenter	User's cost center	If being deployed for use by a singular business user/business use case, the cost center of that user.	N	0652	FinOps
projectCode	Related I$ or O$ project that is supporting the resource funding.	Comes from the MSEPM project code selection on request form.	N		FinOps
requestId	Ticket or identifier for initial resource provisioning.	ITSM Ticket (CRQ, WO, REQ, etc)	Y	CRQ12345	ITIS
createdBy	Individual UserID or Service Account that created the resource.	If resource is created manually, this would be the fulfiller's RACF ID. If the resource is created via automation, this would be the service account name.	Y	ob3	ITIS
createdDate	The date the resource was provisioned.	UTC Date/Time is preferable if the platform allows.	Y	2023-11-10T23:04:32	ITIS
modifiedDate	The date a resource was modified last.	UTC Date/Time is preferable if the platform allows.	N	2023-11-10T23:04:32	ITIS

Resource Tagging Detailed Design

Version 1.3 (Work in Progress)
Created Date: 5/20/2024 | Modified Date: 6/25/2024

Purpose

Tagging allows administrators to assign metadata to resources and services, such as names, descriptions, labels, and categories. This metadata can be used to filter, search, and group resources and services, making it easier to manage and automate cloud infrastructure tasks.

Scope

The tagging strategy has been designed to be universally applicable on resources that reside on platforms that GuideWell uses. This includes, but is not limited to:

- Amazon Web Services (AWS)
- Microsoft Azure
- VMWare
- Nutanix
- OpenShift
- Oracle

Tags outlined here may be appended or enhanced as the process is implemented and as new requirements become identified.

Constraints

- Retroactively applying tagging standards to existing resources may be resource intensive.
- Platforms have a max length for tag key and value, and the number of tags.
  - AWS: Tag keys can have a maximum character length of 128 characters, and tag values can have a maximum length of 256 characters.
  - Azure: The tag name has a limit of 512 characters and the tag value has a limit of 256 characters. For storage accounts, the tag name has a limit of 128 characters and the tag value has a limit of 256 characters. Each resource, resource group, and subscription can have a maximum of 50 tag name-value pairs.
  - VMWare: You can use up to 256 characters for the name of the tag.
  - Kubernetes / OpenShift: must be 63 characters or less (can be empty), unless empty, must begin and end with an alphanumeric character ([a-z0-9A-Z]), could contain dashes (-), underscores (_), dots (.), and alphanumeric between.

Other Tags for Future Consideration

The below listed tags below will be considered in the future if use cases develop to merit them being part of the universal standard.

- **requestedBy** – individual who requested the resource to be created. This information can also be found in the ticket which is already listed as a tag.
- **businessCriticality** – This might align to the Application Tier, but there is still work to be done on defining tiers of applications that might be better realized in the NextGen ITSM.
- **businessUnit** - Maybe redundant to costCenter, ownedBy and application but this could be useful for grouping if the need arises.
- **backup** – Optiv recommended. This way Backup team knows what needs to be backed up when.
- **availability** – Optiv recommended. For resources that don't need to be available 24x7, automation can shut the resources down certain times of day.

Tags Design

As a baseline standard, the listed tags are universally applicable to any resource. Additional tags can be applied to a given resource as needed, but this document should be revised to include them if they would be needed universally.

Tag Key	Description	Details	Required	Example Value(s)	Required by
company	The GuideWell company that the resource is being deployed to support.	Comes from the request ticket.	Y	Florida Blue GuideWell GuideWell Source First Coast Service Options, Inc. Novitas Solutions, Inc.	ITIS
application	Name of application, service, or workload the resource is associated with.	Comes from the request ticket, aka Technical Service (Application) the user selects on the request form.	N	CIP – Consumer Information Platform	FinOps
environment	Deployment environment of this application, workload, or service.	Comes from the environment selected on the request ticket	Y	prd stg tst unt sbx	FinOps
costCenter	User's cost center	If being deployed for use by a singular business user/business use case, the cost center of that user.	N	0652	FinOps
projectCode	Related IS or OS project that is supporting the resource funding.	Comes from the MSEPM project code selection on request form.	N		FinOps
requestId	Ticket or identifier for initial resource provisioning.	ITSM Ticket (CRQ, WO, REQ, etc)	Y	CRQ12345	ITIS
createdBy	Individual UserID or Service Account that created the resource.	If resource is created manually, this would be the fulfiller's RACF ID. If the resource is created via automation, this would be the service account name.	Y	ob3	ITIS
createdDate	The date the resource was provisioned.	UTC Date/Time is preferable if the platform allows.	Y	2023-11-10T23:04:32	ITIS
modifiedDate	The date a resource was modified last.	UTC Date/Time is preferable if the platform allows.	N	2023-11-10T23:04:32	ITIS
		This should be assigned through automation.			
ownedBy	Team or Dept that owns and utilizes the resource.	This should correlate to the ITSM Support Group name that would be listed as the owner in the CMDB.	Y	Infrastructure Automation	ITIS
supportedBy	Operational team that manages and supports the resource from an infrastructure perspective.	This should correlate to the ITSM Support Group name that would be listed as the owner in the CMDB.	N	Network	ITIS
compliance	Type of data transmitted or audit scope for the resource	Need to determine how this info is captured from the intake process or how it can be inferred.	N	SOC2, HiTrust, CM8, ARS	InfoSec and Compliance
confidentiality	An identifier for the specific data confidentiality level a resource supports	Need to determine how this info is captured from the intake process or how it can be inferred.	N	PHI, BlueCard, FEP	InfoSec and Compliance