Enabling Finance-Grade DevOps Automated Governance & Audit

Jamie Plower & Aoife Fitzmaurice

September 2021

Fidelity INVESTMENTS

Disclaimer

This presentation is a case study of the Fidelity Investments experience.

This is not an endorsement or recommendation of any vendor product or service.

About US

Jamie Plower

Integration Services Squad Lead

Aoife Fitzmaurice

Pipeline Platforms Squad Lead

Fidelity INVESTMENTS

1946

Fidelity Management & Research Company Founded

1965

Fidelity Purchases First Computer

1995

Fidelity Becomes an Internet Pioneer with First Mutual Fund to Create a Home Page

2016

Fidelity's First Product Application Deployed to the Cloud

2019

Fidelity Launches Multi-Cloud Hybrid Strategy

2020

1,900 + Applications on Public Cloud

Fidelity INVESTMENTS

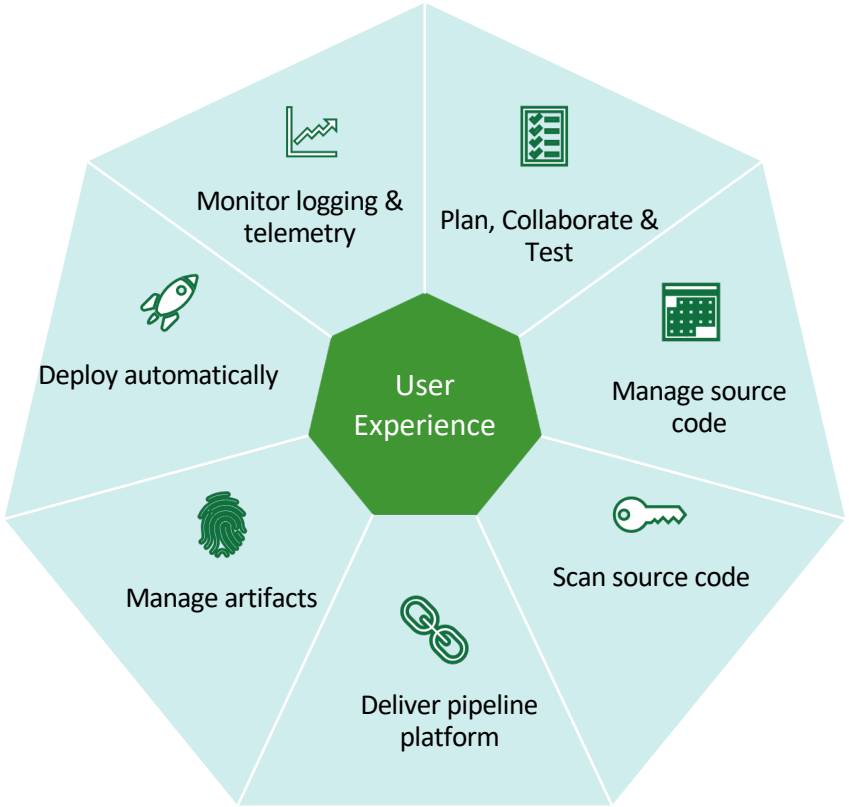
Enabling ALM for the Enterprise

Goals

- Enterprise Focused Services
- Capability Based Offerings
- Focused on User Experience
- Self-Service: Get Developers Going Fast!
- Manage @Large Enterprise Scale with focus on Security, Resiliency, Simplicity

Challenges

- Multiple Different Businesses
- Different Needs and Wants
- Focus on **Enabling** Business Value across All

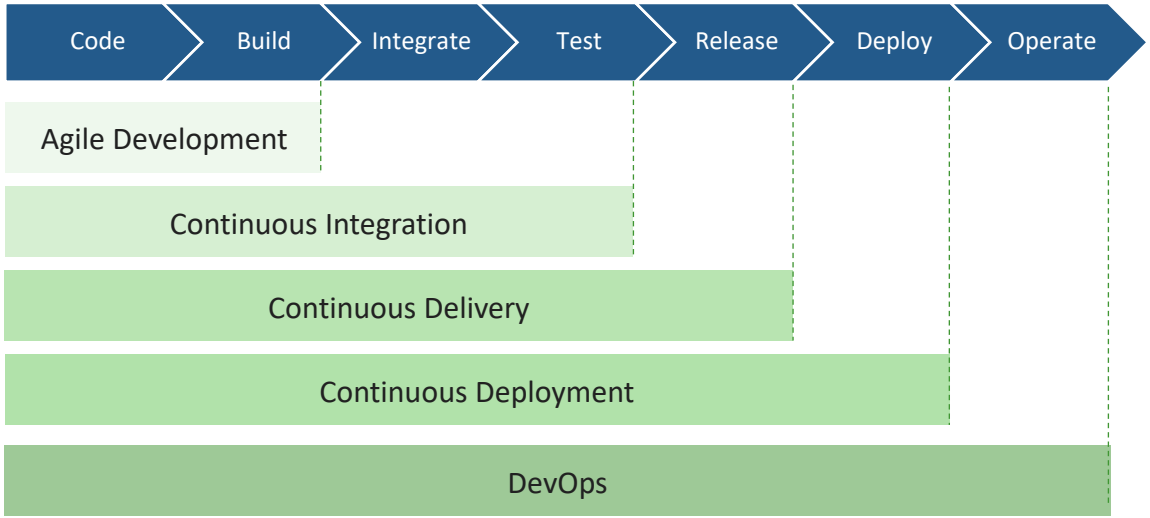


Fidelity INVESTMENTS

Principles for Enabling a Secure Pipeline Platform

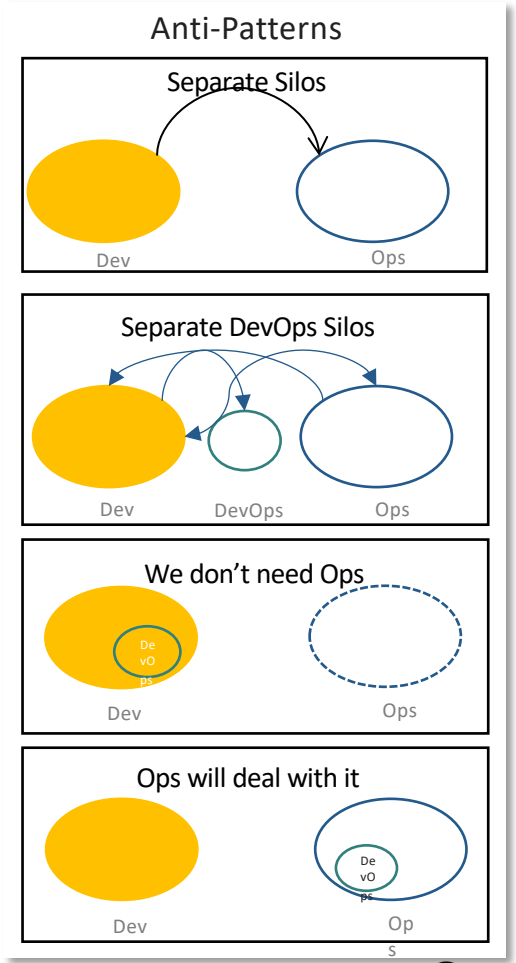
Traditional vs. DevOps Teams

DevOps is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than organizations using traditional software development and infrastructure management processes. This speed enables organizations to better serve their customers and compete more effectively in the market.
– Amazon Web Services



Team use cases to be enabled:

- Strict adherence to 'Separation of Duty' by maintaining a firewall between Dev and Ops roles in a team – ***Continuous Delivery Teams***
- Separation of Duty is achieved through service accounts, build & test then promote – ***Continuous Deployment Teams, DevOps Teams***



Using Key Principles as Guardrails with ALM

- Leverage Open Source
- Buy vs. build
- Minimal customizations
- Self-service capabilities
- Everything as a Service with API's
- Everything as code
- Full automation
- 12-Factor design methodology
- Pace over perfection
- De-coupled architectures
- Use our own capabilities and follow our own best practices
- Mentoring and training

Enabling Value through Self Service Model – A Win Win

Value to Users

Ability to self-onboard with:

- All of the access a developer needs to get going
- Both UI and CLI/API Based experiences
- Access to the full ALM stack

Benefits to Dev Teams

- Stop being ticket punchers
- Concentrate on high value work
- Measure our success
- Standardize the access for audit

Fidelity INVESTMENTS

Measuring with DevOps Research and Assessment (DORA) & BU Metrics

Metrics

- Metrics That Matter
- Beyond Traditional Platform (RYG) or Uptime at the enterprise
- View from our BU team and what value they experience
- Technology → Business Value

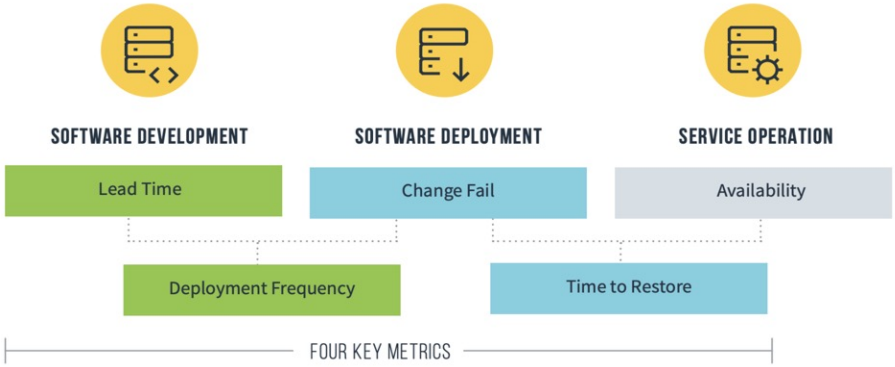
Assess It

Frequency
How often is code deployed or released to users?

Cycle Time
How long does it take to restore services?

Quality
Does released code result in service impairment?

Measure It

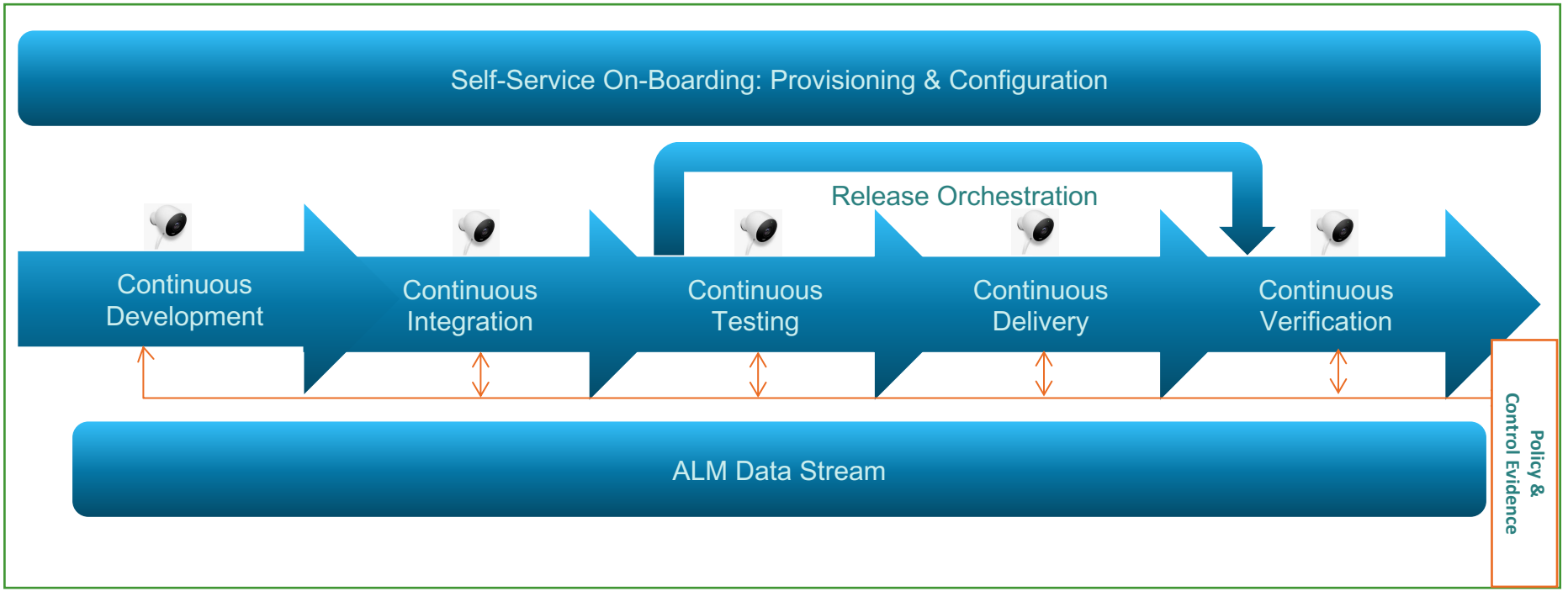


Mature It

- Elite Performers
- High Performers
- Medium Performers
- Low Performers

Fidelity INVESTMENTS

Architecture Reference Guide



Fidelity INVESTMENTS

Governance & Audit Proof Pipelines

Challenges identified migrating toward continuous compliance

- **TEAM AUTOMOMY**: As teams become more decentralized it can make adhering to governance seem more difficult
    - As we shift left in enabling devops processes need mechanism to ensure it is clear and concise for engineers to adopt improved governance and compliance in the SDLC processes as policy evolves
- **PROCESS IMPEDIMENTS**: Processes designed for a world where things change month/quarterly/annually are less useful in a world where things can change daily
    - Due to audits being carried out manually, they are time consuming and expensive and therefore occur less often. By embedding in pipelines, we enable continuous collection and feedback loop .
- **DRIVE AUTOMATION**: Many controls (including processes and procedures) are designed to manage the behaviour of people. As automation proliferates, these practices are less appropriate
    - For success to be realized real data required as change agent within teams to drive towards and orient to the correct practices and simplify audit ready processes
- **STANDARD FOR SELF DOCUMENTING**: Processes that rely on written documentation/paperwork as evidence are troublesome and rely heavily on attestations (opinions) rather than verifiable facts
    - Ensures audit based on real evidence and not accountability
- **CHANGE MANAGEMENT**: Traditional change management processes intentionally slow things down in favour of alignment
    - Provides opportunity for existing processes to be challenged & be simplified by reviewing the flow of data and ensure most optimal check and balances are required and remove unnecessary heavy process-oriented items

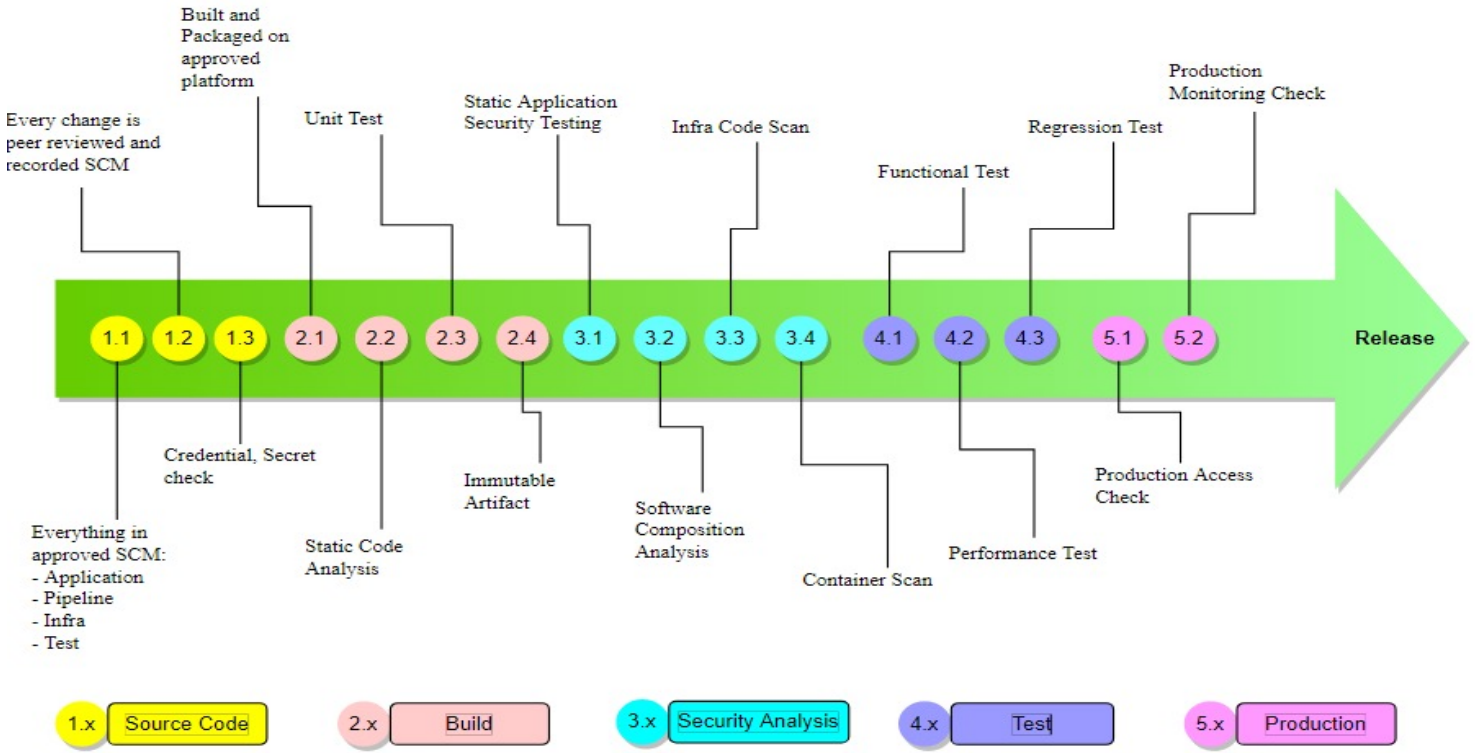
Software Delivery Platform: CI/CD & RO Platform

Layered pipeline and workflow model for flexibility, extensibility, normalizing and scaling

Regulated Workflows	• Regulation (e.g. HIPPA) based end to end immutable Release Orchestration • Regulation Certification Reporting	
Certified Workflows	• End to End immutable Release Orchestration • Evidence gathering and approval gates • Audit Approved and Certified Compliance	• Deployment Strategies • Rollback Automation • Process & Tool Integration
Certified Pipelines	• Fully tested end to end immutable pipelines • Call Backs for extensibility • Audit Approved & Certified Compliance	• Change Management • Governance Gates
Pipeline Template Catalog	• Technology & Architecture Patterns • Pipeline Capability and Tooling Integrations • Consistent and Standardized Best Practices	• Pipeline as Code • Parameterized Configuration
Fidelity & BU Pipeline Libraries	• Common Pipeline Functions • Technology Functions • Integrated Functions	• Tool Integrations • CSP Integrations
Fidelity Buildpacks	• Technology Based Buildpacks • ECC Platform Base Buildpack • Proper SDLC & Version Control	• Technology CDK's • Vendor CDK's • Fidelity & ECC CDK's
Software Delivery Platform	• Platform Guardrails • Identity and Access Management • Data Streaming	• Preferred Tool Chain

Fidelity INVESTMENTS

Codify Process, Security & Compliance best practices in the pipeline



Note: The above controls are just a sample set

Fidelity INVESTMENTS

Align Catalog to workload patterns

1 Content Management

Hosted end to end environment for content management, curation, publication, delivery and search.

1) Content Management Service (PaaS)
2) Hosted CDN and Edge Caching

2 Cloud Data Archive

Storage of historical or infrequently accessed object based data (documents, media files, other digital content, etc.) supporting a WORM pattern.

3 Web Application

Web application with an HTML5, CSS3 and JavaScript based front end accessing web services. Internet ingress requires Web DMZ and internet egress requires egress proxy or back haul via FMN.

1) Customer facing with CMS and CDN
2) Employee facing with SSO integration

4 Web Service (Single service or Microservices)

A basic web services application that provides business domain services on top of a system of record. It is delivered over HTTP/HTTPS or JMS and are accessed via an API gateway or directly via a service end point. Service data may be cached locally for performance. A microservice is a collection of related web services forming a logical application.

5 Batch Application

Asynchronous and synchronous jobs generally doing bulk data processing such as ETL/ELT.

6 Event Driven Application

Application or function triggered by events (data changes, messages, http requests etc.) It replies on messaging services to handle asynchronous processing of application workloads.

.

7 Data Analytics Application

An application that processes real-time (streaming) or periodic (batch) data inputs using analytic compute capabilities such as a map reduce, machine learning, pattern matching, text analytics and natural language processing.

8 Legacy Application

Monolithic, BAU or Vendor applications that are not fully 12-factor compliant. These application could run on VM, IaaS or potentially on CaaS runtime platforms.

9 Cloud Hosted Database

Database management system either:

1) Deployed as a native cloud service (DBaaS) environment, or
2) Deployed by Fidelity on cloud infrastructure (Hosted database)

10 Hosted Virtual Desktop

Virtual windows desktop environments with installed applications which access web services that are either co-located or in an on premises data center. They are internally facing, but would likely require external internet access for some of their applications.

Embedded Standards

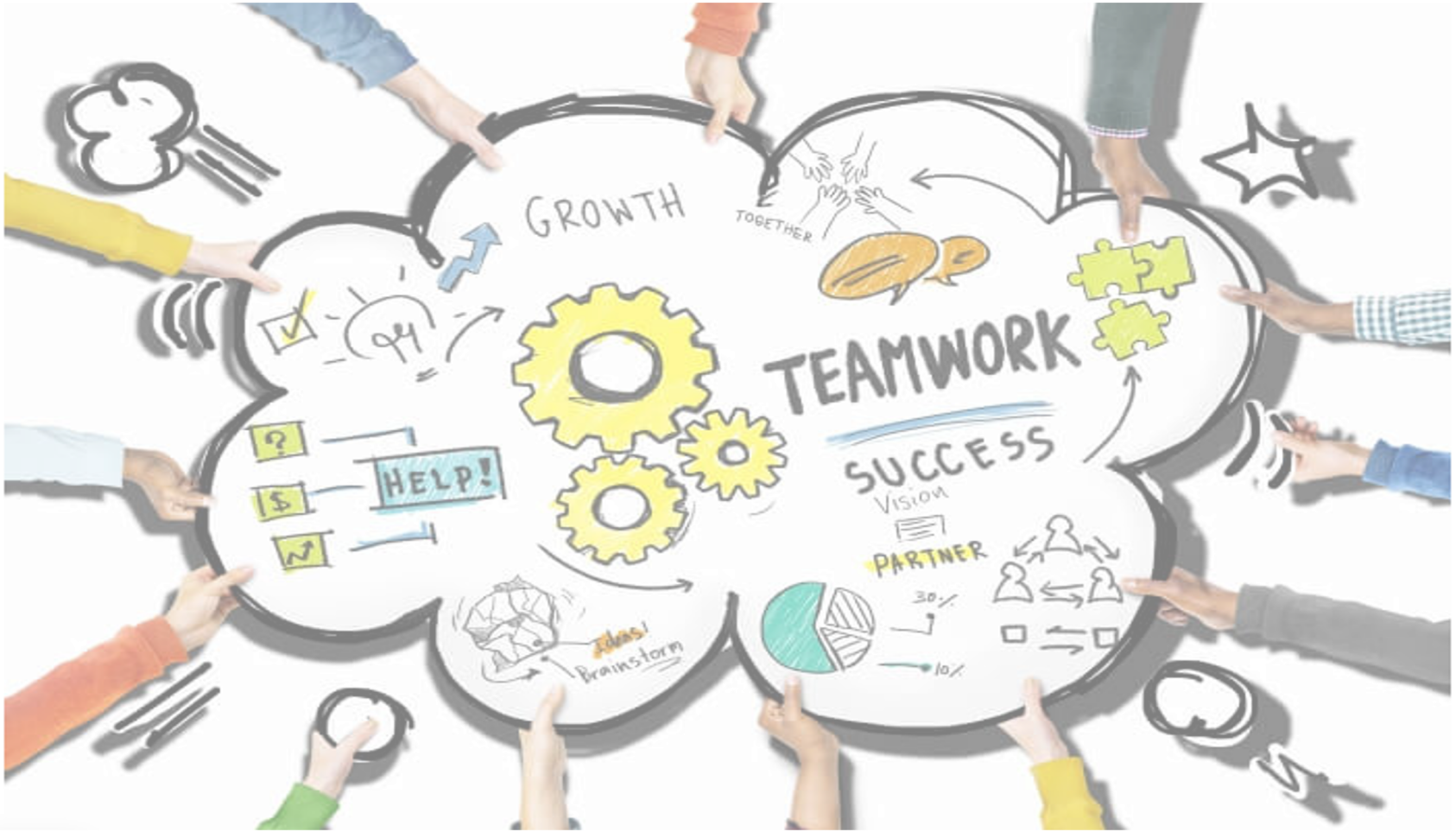
- Security
- Audit/Policy
- Governance

Cloud Platform Targets

FaaS, IaaS, CaaS, VM

Fidelity INVESTMENTS

Culture



Fidelity INVESTMENTS

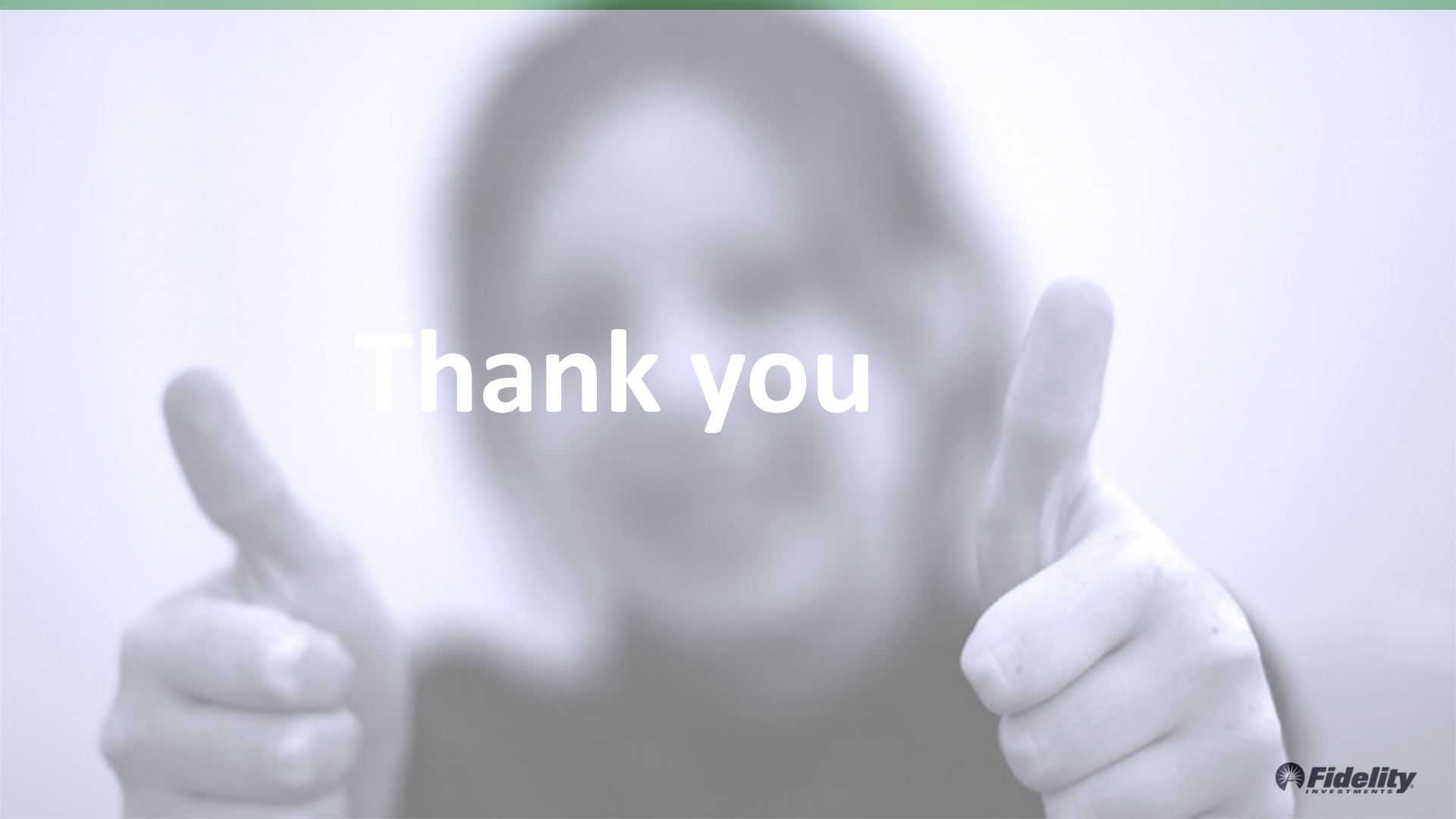
Lessons Learned & Inputs for Your Journey Forward

Technology

Team Culture

Communications

Fidelity INVESTMENTS


Thank you