

Agile & DevOps vs. Controls & Compliance: Inherently Opposed or Unrealized Opportunity?

Jason Brucker - Protiviti
Director, Technology Strategy &
Operations

Core Competencies – C12

SPEAKER INTRODUCTION

A stylized graphic of the San Francisco skyline is positioned behind the "CyberSizelT" text. It includes silhouettes of the Golden Gate Bridge, the Transamerica Pyramid, and other city buildings against a light, hazy background.

CyberSizelT

Today's Agenda:



Core Concepts

Challenges &
Control Gaps

Implementing
Controls

Case Study

Polling Ground Rules



1 Questions will be answered via smartphone by scanning a provided QR code or by entering provided URL into your browser

2 Answer honestly based on your own knowledge and experience

3 Feel free to ask questions and discuss results during table break-outs

Audience Profile!



Vote on live.voxvote.com
or download app.  

PIN: 50317

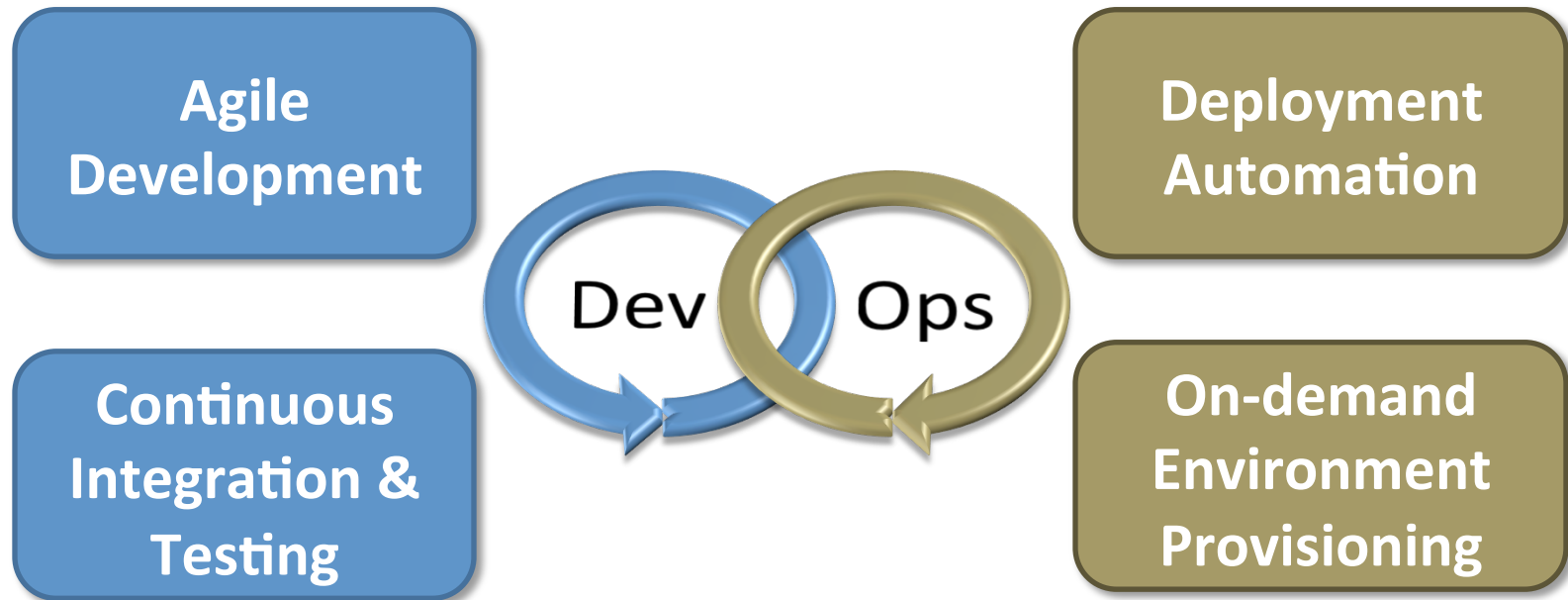
A Few Common Myths...

- Agile and DevOps processes cannot be controlled and are not “compliant”
- Agile and DevOps can only work in small companies
- Companies who do not embrace Agile and DevOps cannot be innovative
- Development and operations teams must always be separate for proper SoD and compliance
- Agile is the best fit and can be applied to any project
- Agile helps teams move faster by avoiding all documentation

DevOps Concepts: *Common Definition*

DevOps focuses on improving the ***communication and coordination*** between the Development and Operations functions. DevOps techniques and tools ***enhance collaboration*** across these traditional silos to enable ***greater velocity and quality***.

DevOps Concepts: *Key Capabilities & Benefits*

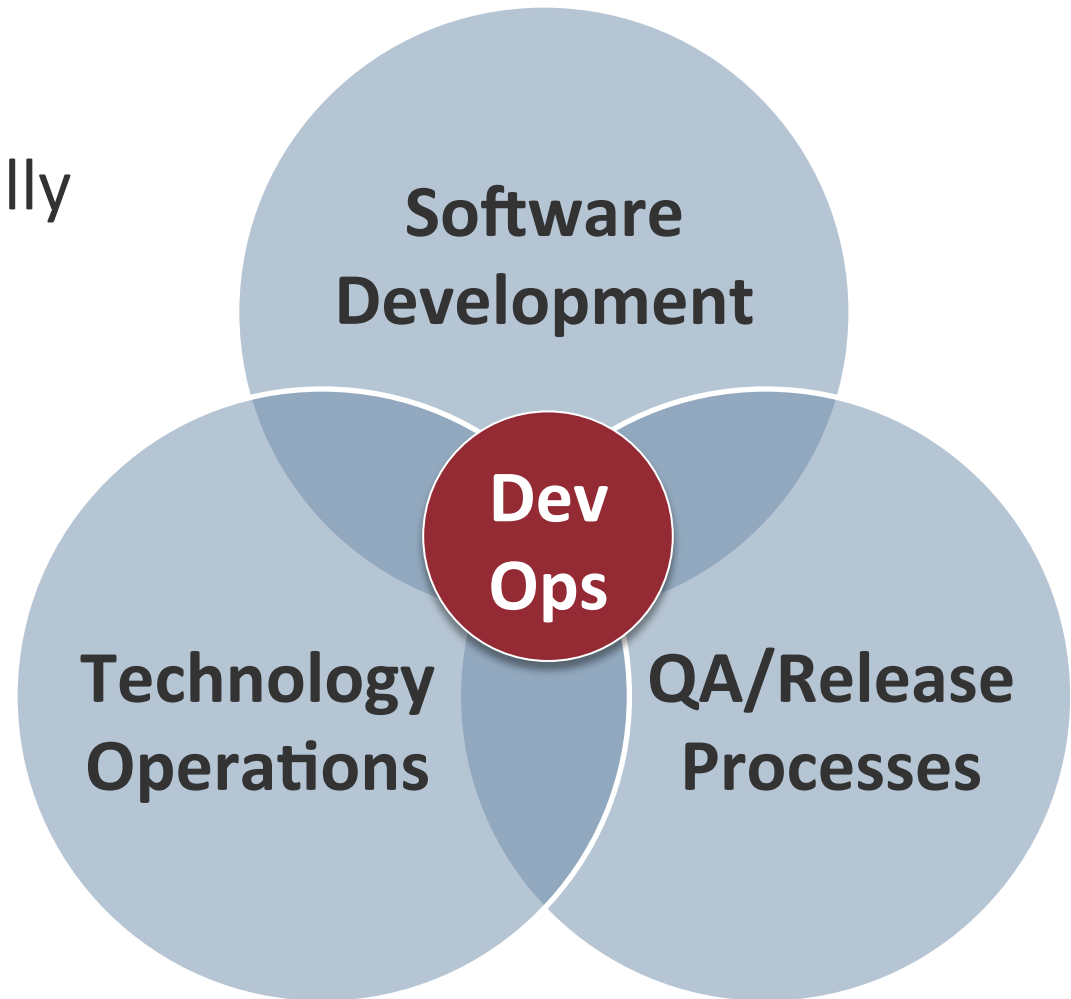


Combining Development and Operations yields:

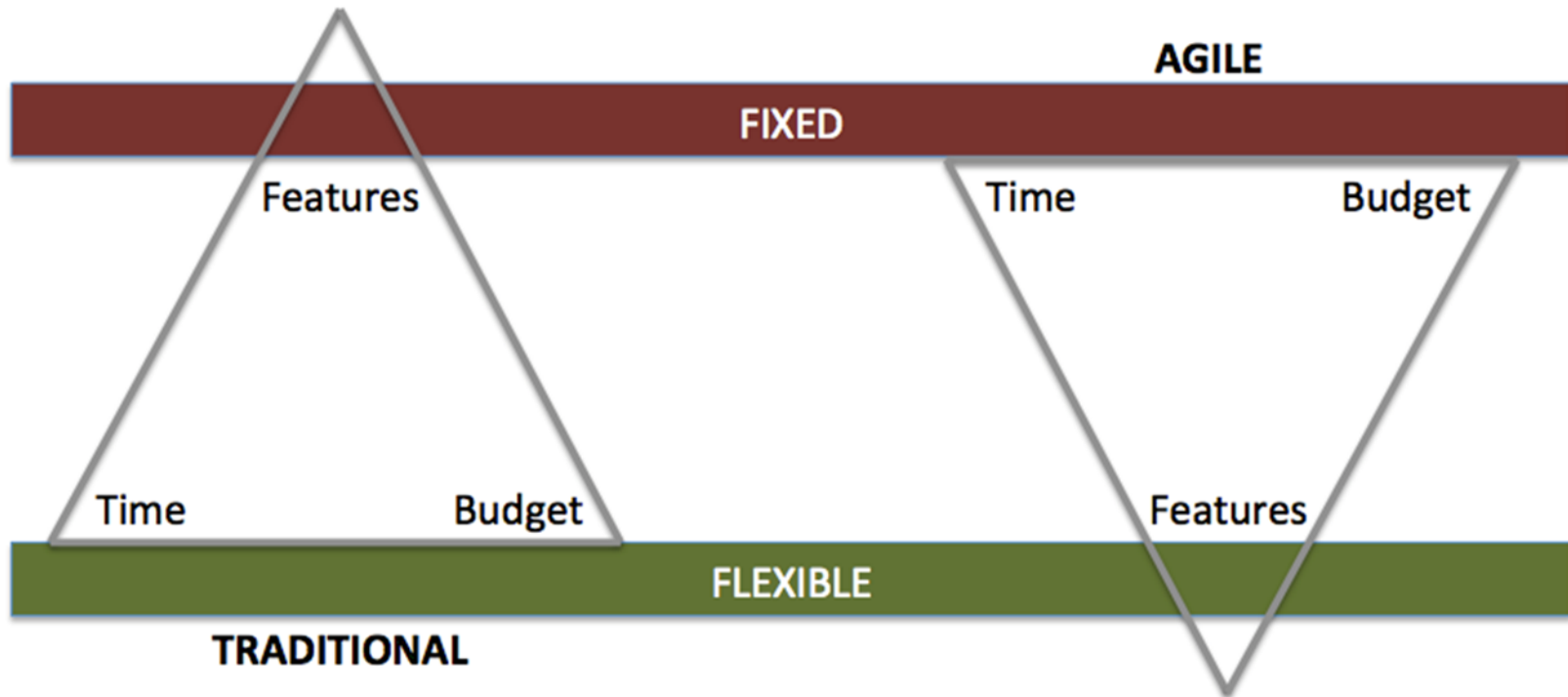
- ✓ *Faster software delivery*
- ✓ *Reduced defects*
- ✓ *Increased business alignment*

DevOps Concepts: *Key Challenges*

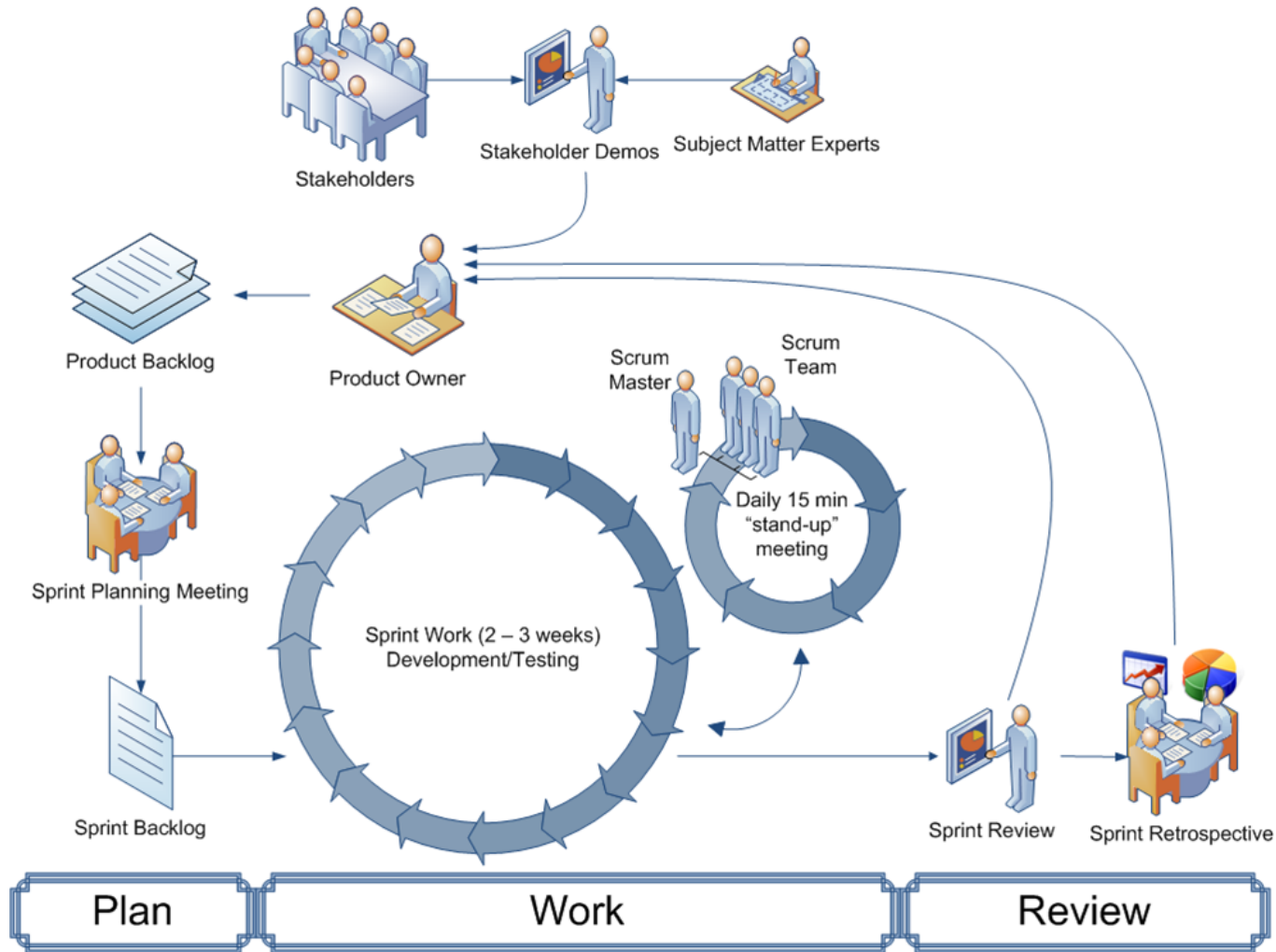
- Bringing together & controlling traditionally **dissimilar processes**
- Improving **communication** between cross-functional teams
- Really getting the value out of **automation tools**



Agile Concepts: *Shift in Perspective*

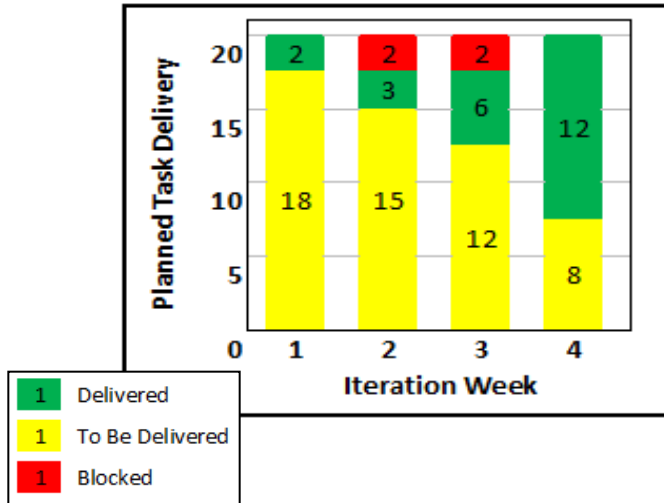


Agile Concepts: *Typical Lifecycle*

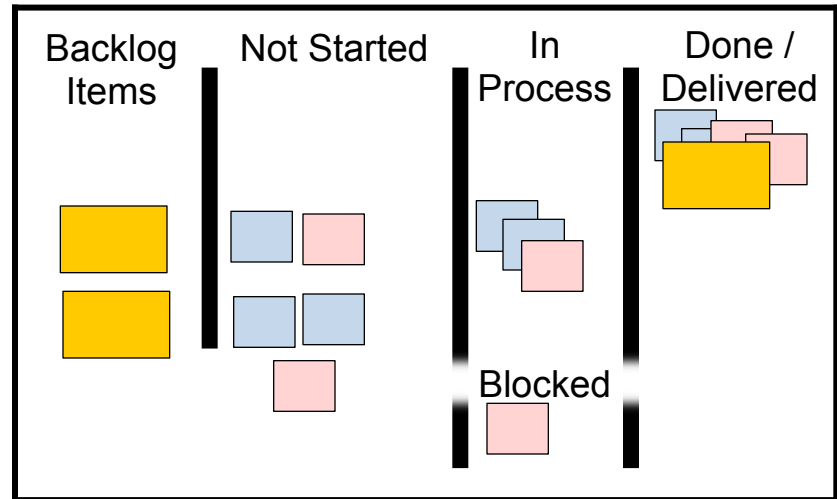


Agile Concepts: *Common “Tools”*

Burndown Chart



Project Task Board



Daily Standup

Ground Rules:



1. Limited to 15 minutes.
2. Action-oriented.
3. Not for detailed project status.

3 Questions:

1. What did you do yesterday?
2. What will you do today?
3. What is blocking you?

Polling Question: *Who is Agile?*



Vote on live.voxvote.com
or download app.  

PIN: 50317

Challenges: *The “Macro” View*

“Non-traditional” technology management processes can conflict with corporate governance requirements:

- Sarbanes-Oxley Act (SOX) compliance
- SOC reporting (under SSAE No. 16)
- PCAOB audit firm reviews
- Updated COSO framework
- Other compliance requirements: PCI, HIPAA, etc.

Organizations need to balance control and compliance requirements with the need for speed and innovation

Challenges: *Agile Project Delivery*

Failure to fully evaluate project value and/or return on investment.

Inability to detect and control scope creep / business case alignment.

Inadequate business engagement and signoff.

Failure to maintain and estimate backlogs.

Inadequately training the business on newly delivered features.



Using Agile as an excuse to not complete required project documentation.

Lack of project measures: scope, schedule, etc.

Misalignment with “traditional” IT controls.

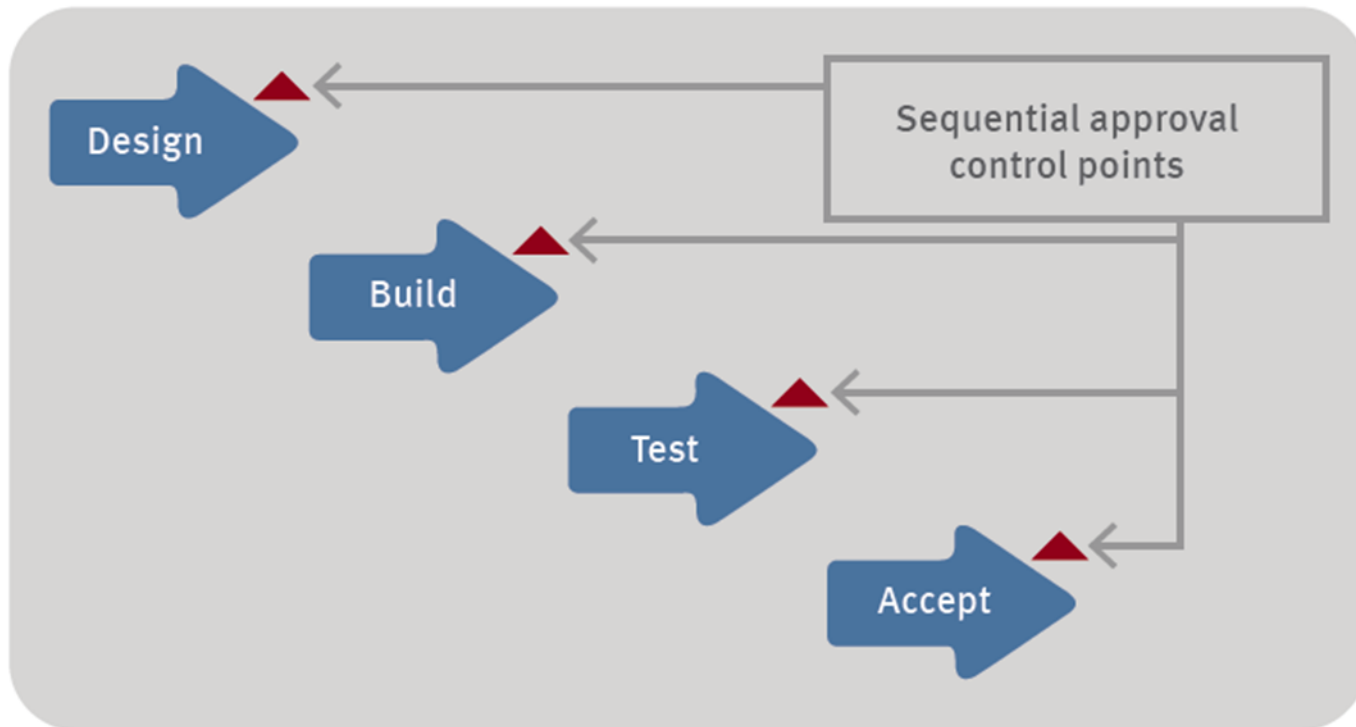
Polling Question: *Challenges*



Vote on live.voxvote.com
or download app.  

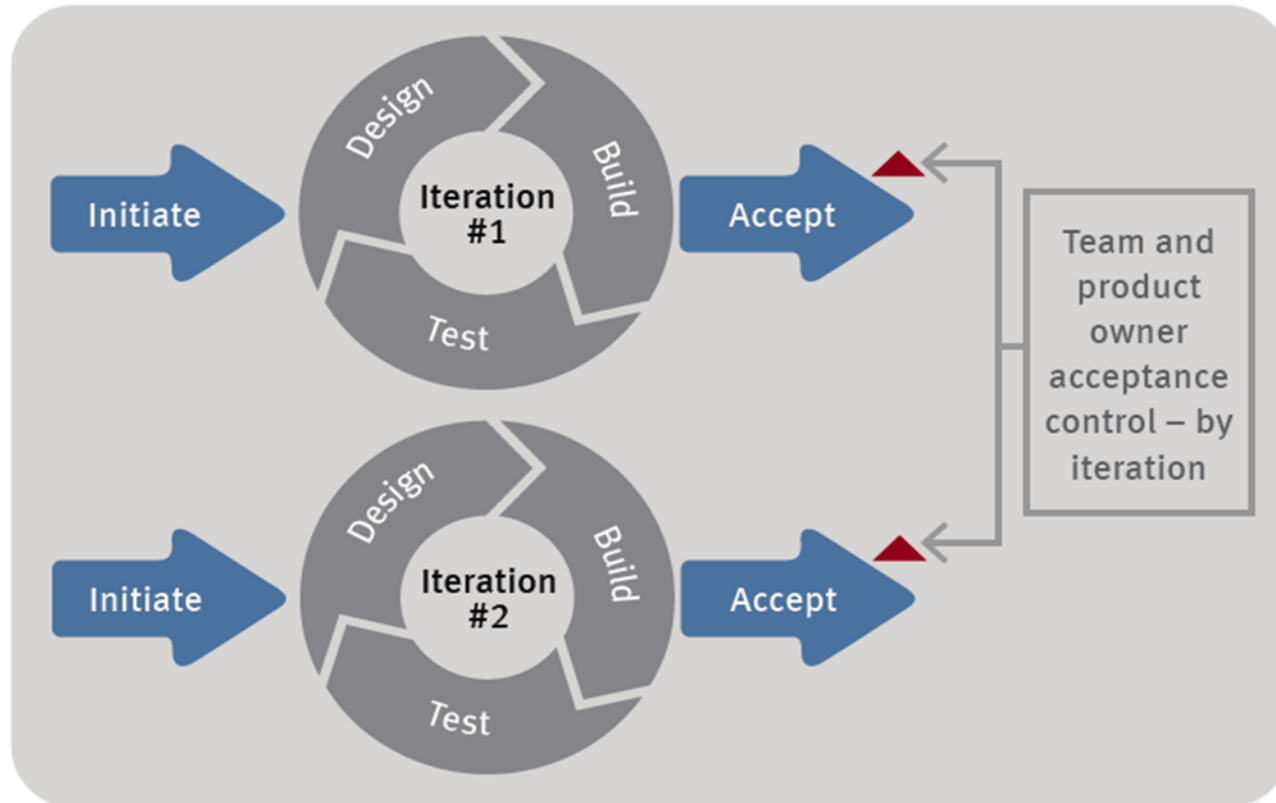
PIN: 50317

SDLC Controls: *Tradition is Driving the Way*



*Widespread familiarity with traditional or waterfall approaches makes it the basis for controlling SDLC at most organizations – **this perspective needs to shift!***

SDLC Controls: *Shifting the Perspective for Agile*



*Agile SDLC controls need to be “per iteration” – **multiple control objectives may be addressed at one time!***



SDLC Controls: *Key Takeaways*

Audit and control approaches need to be properly aligned with the SDLC methodology. Misaligned approaches can create unnecessary “overhead”, and often fail to mitigate key risks.

Regardless of SDLC methodology, controls still need to address all the traditional SDLC risks for design, build, testing, and acceptance. However, for Agile SDLC, audit and control approaches need to take an integrated view to assessing risks on per-iteration basis.

Polling Question: *Implementing Controls*

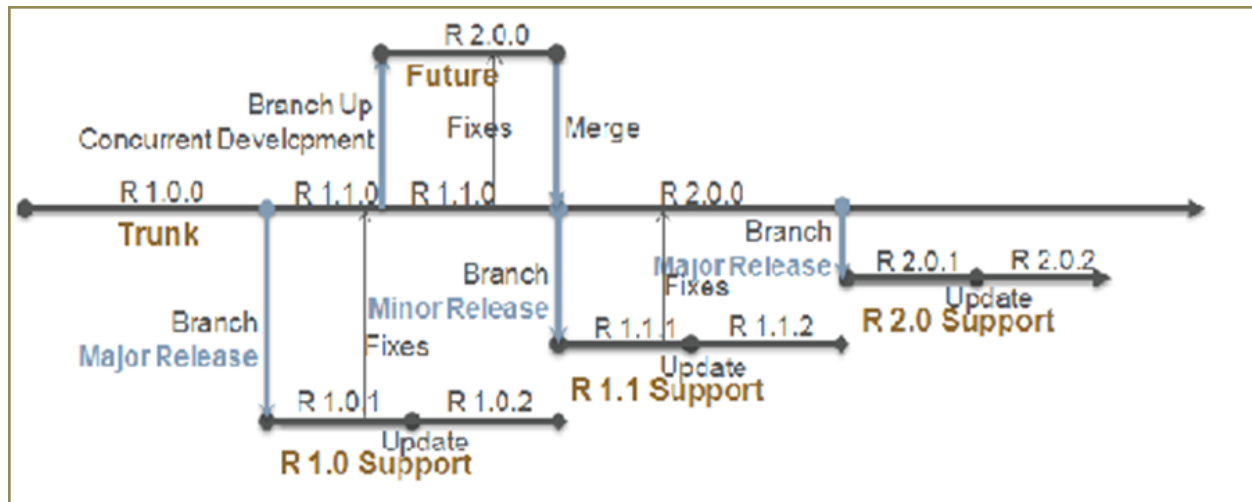


Vote on live.voxvote.com
or download app.  

PIN: 50317

Testing: *Continuous Releases = Complexity*

Continuous integration and release approaches result in much more frequent change: **weekly, daily, even hourly!**



Challenge: *How can testers, and more specifically user testers keep up with this pace of change?*

Testing: *Agile & DevOps Benefits*

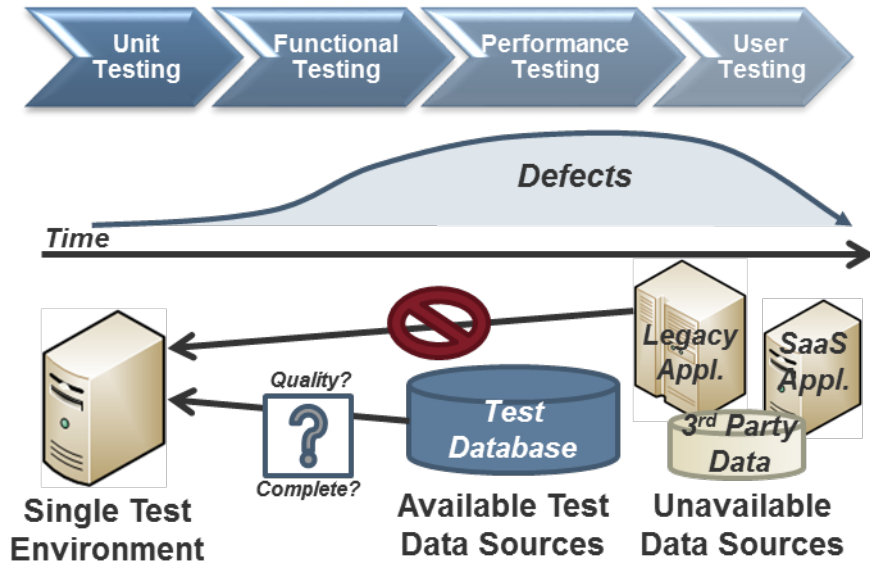
Agile and DevOps processes can actually help make testing more effective:

- Earlier testing – integrated with development efforts
- Testing automation (scripting & documentation)
- Continuous testing
- Service virtualization

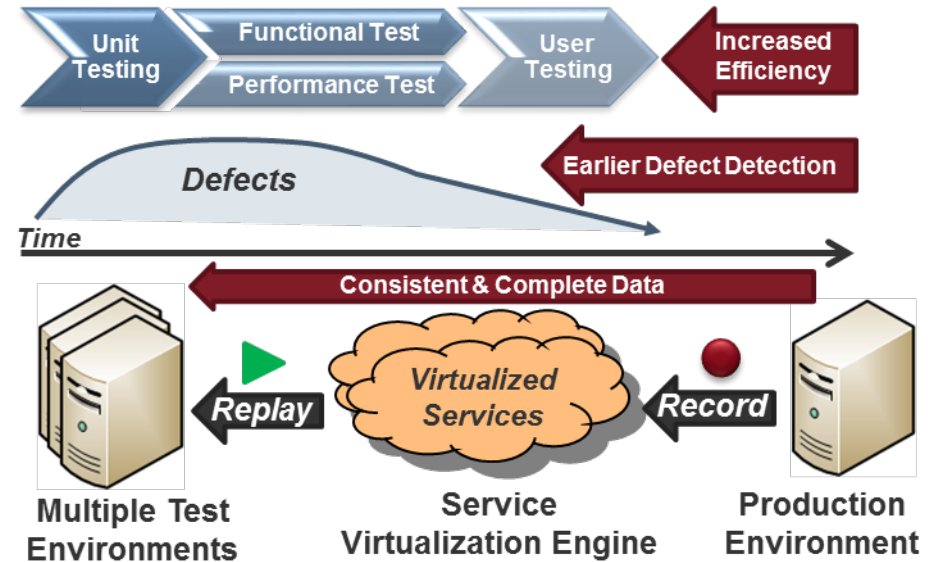
Testing tools and processes must effectively align to the key risks and requirements.

Testing: *Service Virtualization*

Traditional Testing Approach



Service Virtualization Approach



- ✓ *Faster test environment provisioning*
- ✓ *Test data matches production data*
- ✓ *Earlier defect detection & repair*
- ✓ *Reduced overall testing costs*

Access & SOD: *The Challenge of Integrated Roles*

DevOps seeks to increase the integration of the development and operations roles – ***this can effectively eliminate traditional role segregations and introduce other access control issues***

Challenges:

- *Broad administrator privilege assignment*
- *Full development lifecycle access: source code through deployment*
- *Peer review on the “honor system”*
- *Unclear monitoring responsibilities*

Access & SOD: *DevOps “Done Right”*



DevOps approaches do not have to compromise security and heighten risks – ***processes and tools can help manage risk while enabling flexibility:***

- Production environment monitoring
- Identity management automation
- Firecall IDs
- Release & deployment automation (workflow)

**Note: DevOps solutions may not be appropriate for all system environments – some frameworks still include very strict SoD requirements that need to be observed and will limit how DevOps processes can be implemented*

Polling Question: *Compliance Issues*



Vote on live.voxvote.com
or download app.  

PIN: 50317

Performance Measures: *Agile Mis-alignment*

Traditional and Agile project metrics need to be derived using different methods – ***many organizations fail to adapt their metrics when adopting Agile***

Challenges:

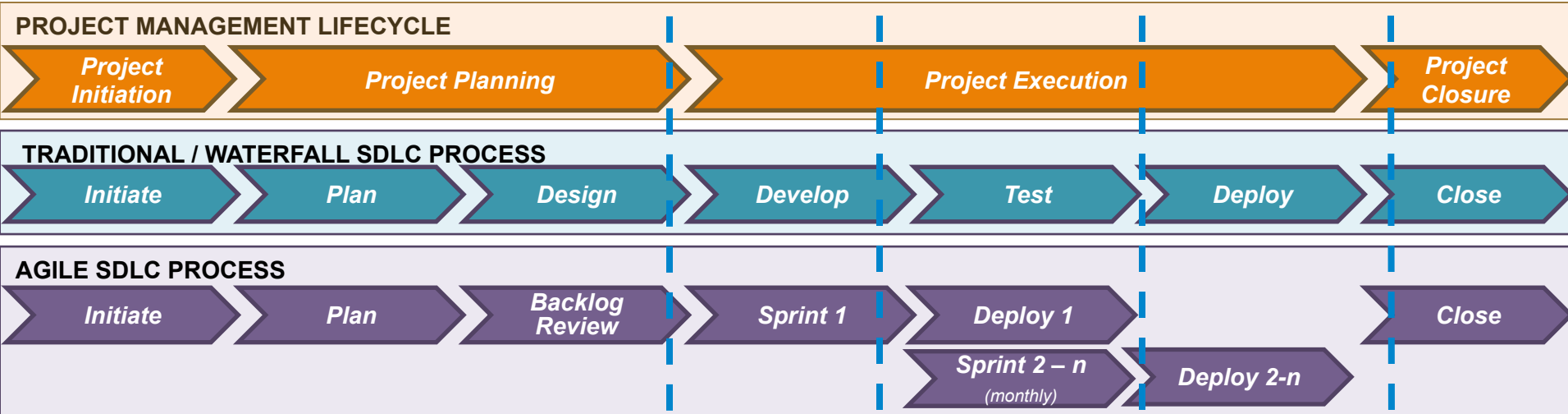
- *Evaluating project timeline / phase status*
- *Measuring % complete when scope and budget are derived / defined iteratively*
- *Translating detailed Agile project metrics to management reports*
- *Comparing Traditional and Agile project statuses*

Performance Measures: *Adapting to Agile*

Most IT project measures have been derived based on Traditional delivery methodologies which cannot be applied to Agile projects without modifications:

- Conceptually separate Project Management & SDLC
- Define the Project level metrics that are required
- Define how the Project metrics can be derived from projects delivered within each lifecycle (Agile, Traditional, and other)

Performance Measures: Agile vs. Traditional



Metric: Planned Value

Traditional: Base on key milestones & est. efforts

Agile: Base on backlog priorities (e.g., story points)

Metric: Schedule Variance

Traditional: base on key milestones & detailed plan dates

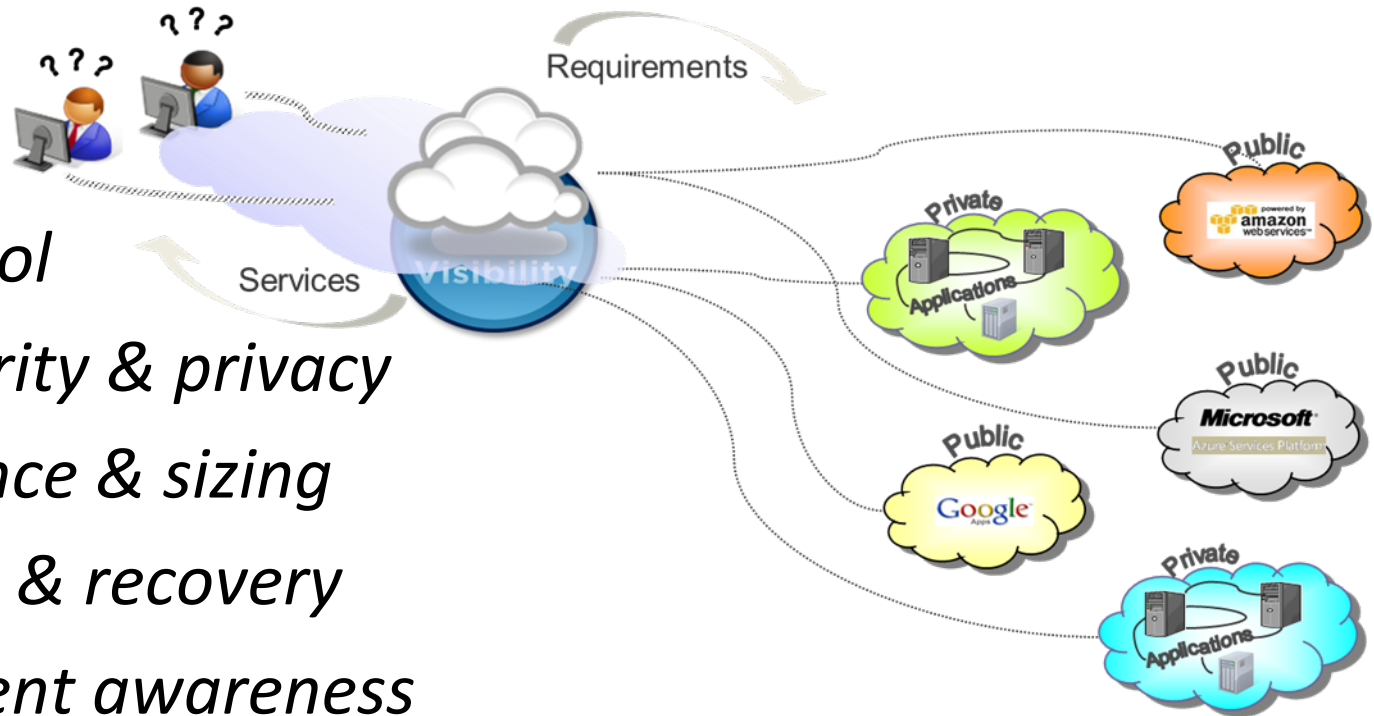
Agile: Base on delivery velocity; plan vs. actual per iteration

Cloud Provider Utilization: *Is There Visibility?*

Agile and DevOps approaches are often paired with use of cloud-based solutions to enable scale and flexibility.

Challenges:

- *Cost control*
- *Data security & privacy*
- *Performance & sizing*
- *Continuity & recovery*
- *Environment awareness*





Cloud Governance: *Balancing Speed & Control*

Effective governance is required to help optimize use of cloud environments within Agile and DevOps processes

- **Decision-making:** *should be timely and information based, and not become a barrier*
- **Requirements:** *key requirements (compliance, performance, sizing, etc.) should be known and evaluated before environments are provisioned*
- **Modeling & Monitoring:** *an “inventory” of cloud providers and existing environments should be maintained and reviewed*

Polling Question: *Pain Points*



Vote on live.voxvote.com
or download app.  

PIN: 50317

CASE STUDY

A silhouette of the San Francisco skyline is shown against a light, hazy background. The Golden Gate Bridge is the most prominent feature on the left. Other buildings and bridges are visible in the background.

CyberSizeIT

Q&A



Trust in, and value from, information systems

San Francisco Chapter

A stylized graphic of the San Francisco skyline and the Golden Gate Bridge, rendered in black and white with a yellow and orange gradient background. The Golden Gate Bridge is prominent on the left, and the city skyline is on the right.

CyberSizelT

*Powerful Insights.
Proven Delivery.®*

Confidentiality Statement and Restriction for Use

This document contains confidential material proprietary to Protiviti Inc. ("Protiviti"), a wholly-owned subsidiary of Robert Half ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public, should be used solely and exclusively to evaluate the capabilities of Protiviti to provide assistance to your Company, and should not be used in any inappropriate manner or in violation of applicable securities laws. The contents are intended for the use of your Company and may not be distributed to third parties.