Large Projects into Sub-tranche Grouping – Key considerations

Smaller and manageable chunk of related applications form a sub-tranche.

Sub-tranches provide the flexibility to roll out applications to AWS in smaller groups.

Better manageability and easier to rollback if the production cutover runs into issues.

Minimize changes to applications that are yet to move to AWS

Technology based sub-tranching allows for optimal utilization of skilled resources

Tranche Groups

Tranche 1 -

Infrastructure applications

Integration Foundational Elements

Tranche 2

Core Front-office applications

Tranche 3

Core Back-office applications

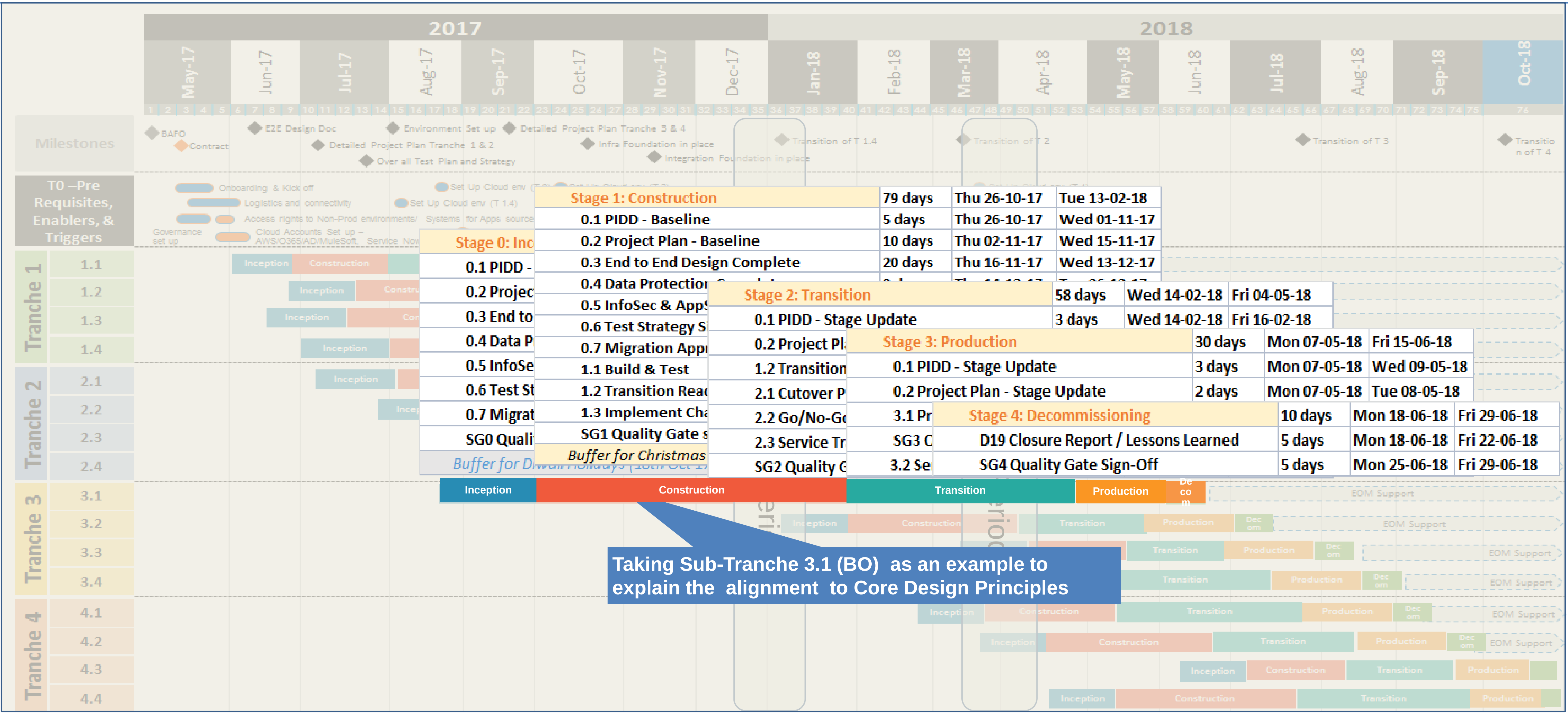
Tranche 4

Remaining applications (e.g. in active development, to be retired)

Key Considerations

- Foundational infrastructure and integration elements will be setup before any applications are moved to AWS.
- Logical grouping of applications based on dependencies and criticality
- Healthy mix of simple and complex applications. Simple applications to keep the business interest and Complex applications to prove that any show stoppers are addressed early in the life cycle

High Level Plan - Overall



Stage 0: Inc
0.1 PIDD -
0.2 Projec
0.3 End to
0.4 Data P
0.5 InfoSe
0.6 Test St
0.7 Migrat
SG0 Quali
Buffer for D

Stage 1: Construction	79 days	Thu 26-10-17	Tue 13-02-18
0.1 PIDD - Baseline	5 days	Thu 26-10-17	Wed 01-11-17
0.2 Project Plan - Baseline	10 days	Thu 02-11-17	Wed 15-11-17
0.3 End to End Design Complete	20 days	Thu 16-11-17	Wed 13-12-17
0.4 Data Protection			
0.5 InfoSec & AppS			
0.6 Test Strategy S			
0.7 Migration Appr			
1.1 Build & Test			
1.2 Transition Read			
1.3 Implement Cha			
SG1 Quality Gate s			
Buffer for Christmas			

Stage 2: Transition	58 days	Wed 14-02-18	Fri 04-05-18
0.1 PIDD - Stage Update	3 days	Wed 14-02-18	Fri 16-02-18
0.2 Project Pl			
1.2 Transition			
2.1 Cutover P			
2.2 Go/No-G			
2.3 Service Tr			
SG2 Quality G			

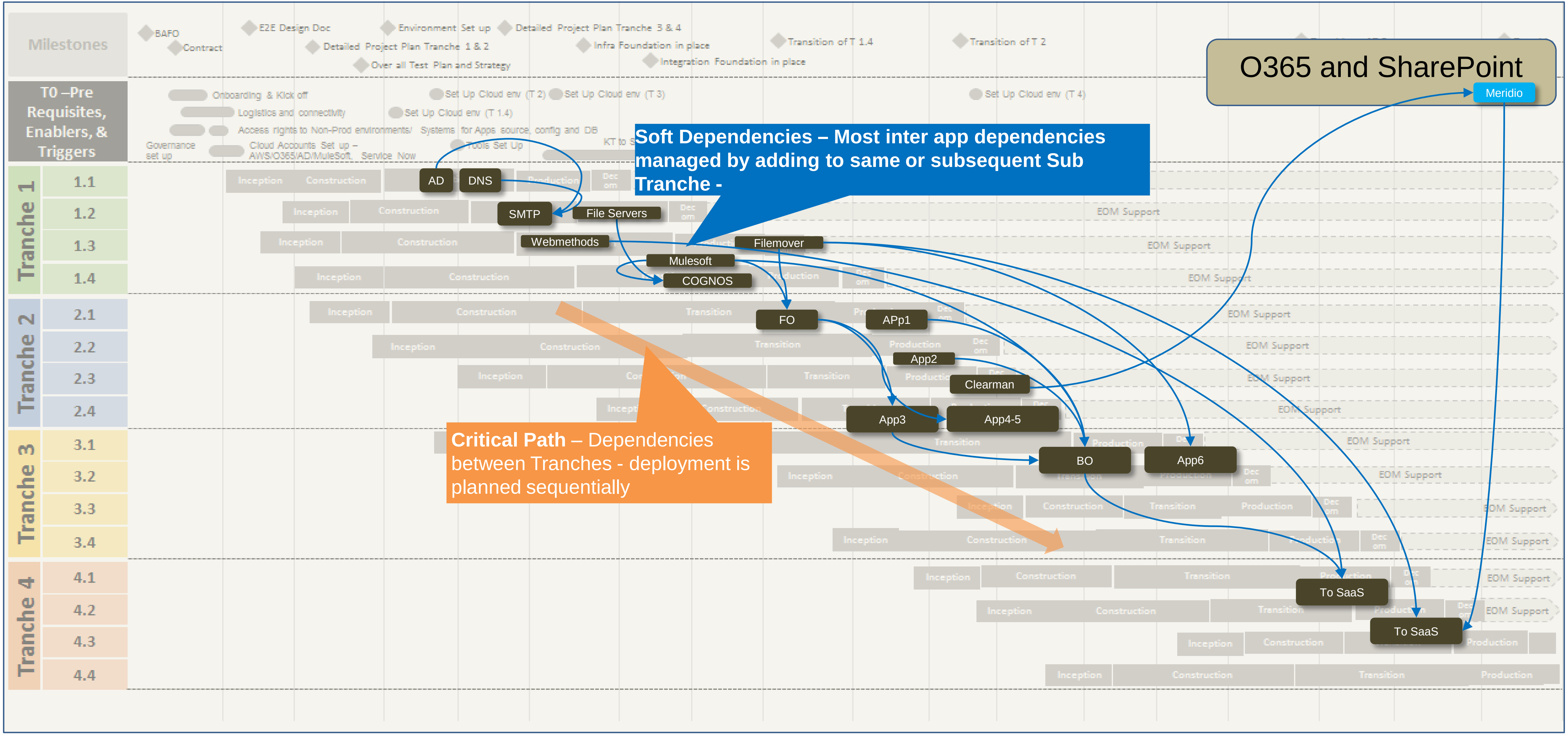
Stage 3: Production	30 days	Mon 07-05-18	Fri 15-06-18
0.1 PIDD - Stage Update	3 days	Mon 07-05-18	Wed 09-05-18
0.2 Project Plan - Stage Update	2 days	Mon 07-05-18	Tue 08-05-18
3.1 Pr			
SG3 Q			
3.2 Se			

Stage 4: Decommissioning	10 days	Mon 18-06-18	Fri 29-06-18
D19 Closure Report / Lessons Learned	5 days	Mon 18-06-18	Fri 22-06-18
SG4 Quality Gate Sign-Off	5 days	Mon 25-06-18	Fri 29-06-18

Inception	Construction	Transition	Production	Decom

Taking Sub-Tranche 3.1 (BO) as an example to explain the alignment to Core Design Principles

Intra tranche and sub-tranche dependencies

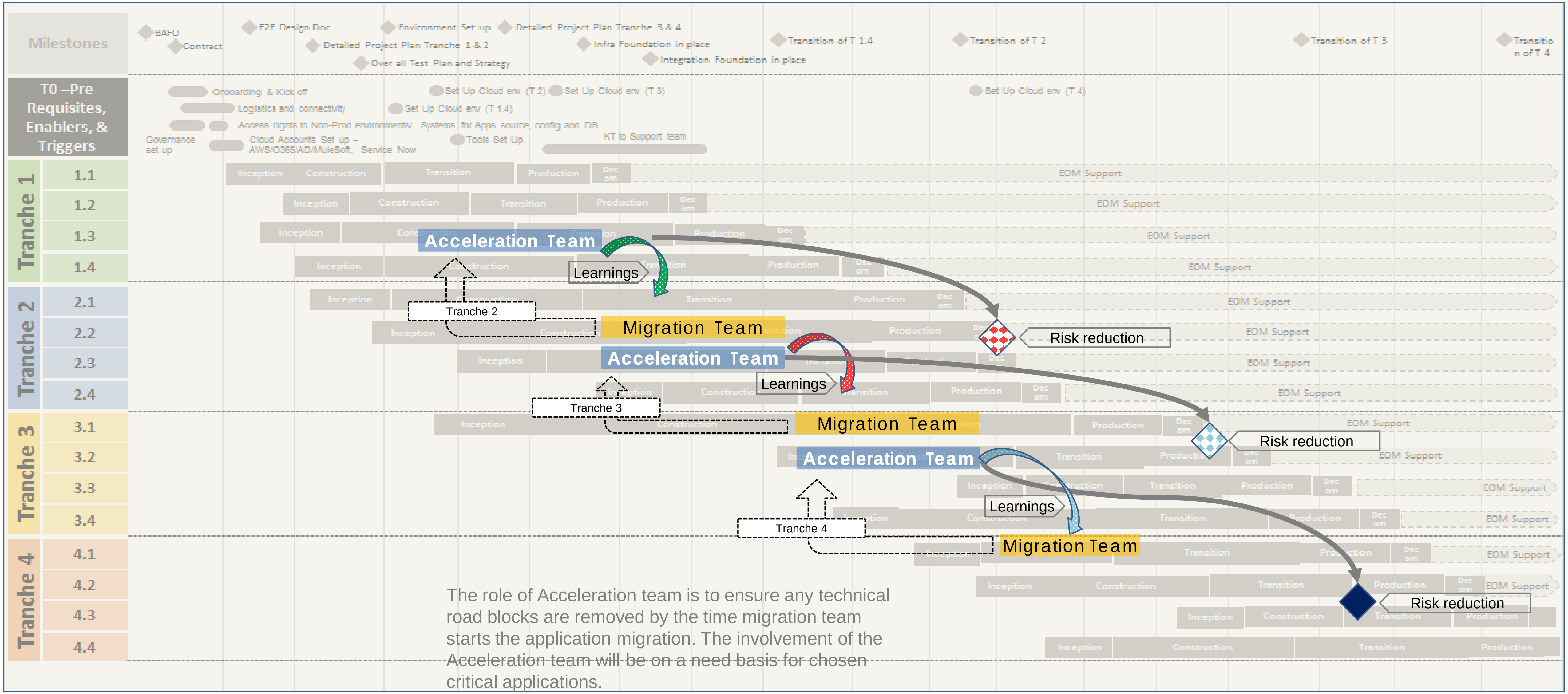


O365 and SharePoint

Soft Dependencies – Most inter app dependencies managed by adding to same or subsequent Sub Tranche -

Critical Path – Dependencies between Tranches - deployment is planned sequentially

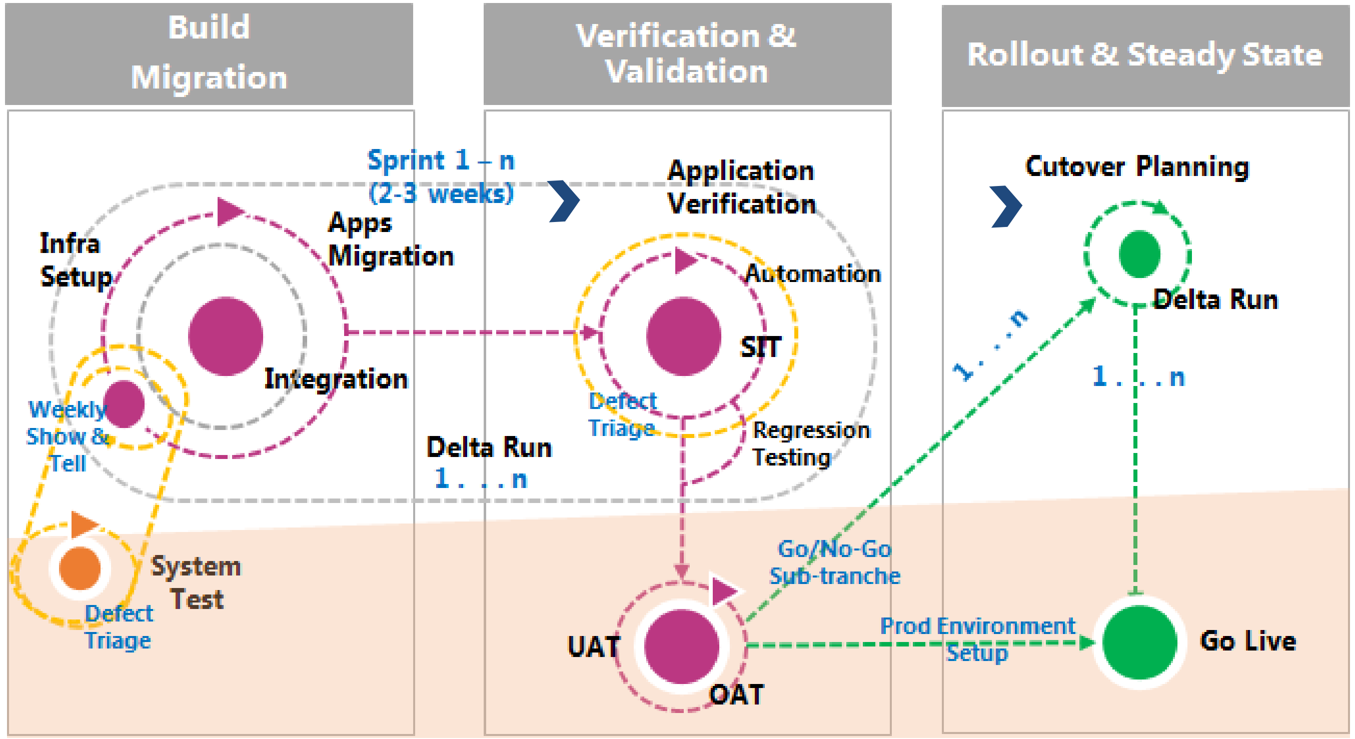
Acceleration Team to de-risk Migration challenges



The role of Acceleration team is to ensure any technical road blocks are removed by the time migration team starts the application migration. The involvement of the Acceleration team will be on a need basis for chosen critical applications.

Overall Programme View – Project Execution

Migration (Iterations at each Sub-Tranche Level)



Stage 1: Construction

- 0.1 PIDD - Baseline
- 0.2 Project Plan - Baseline
- 0.3 End to End Design Complete
- 0.4 Data Protection Complete
- 0.5 InfoSec & AppSec Checklist Complete
- 0.6 Test Strategy Signed Off
- 0.7 Migration Approach Complete
- SG1 Quality Gate sign-off

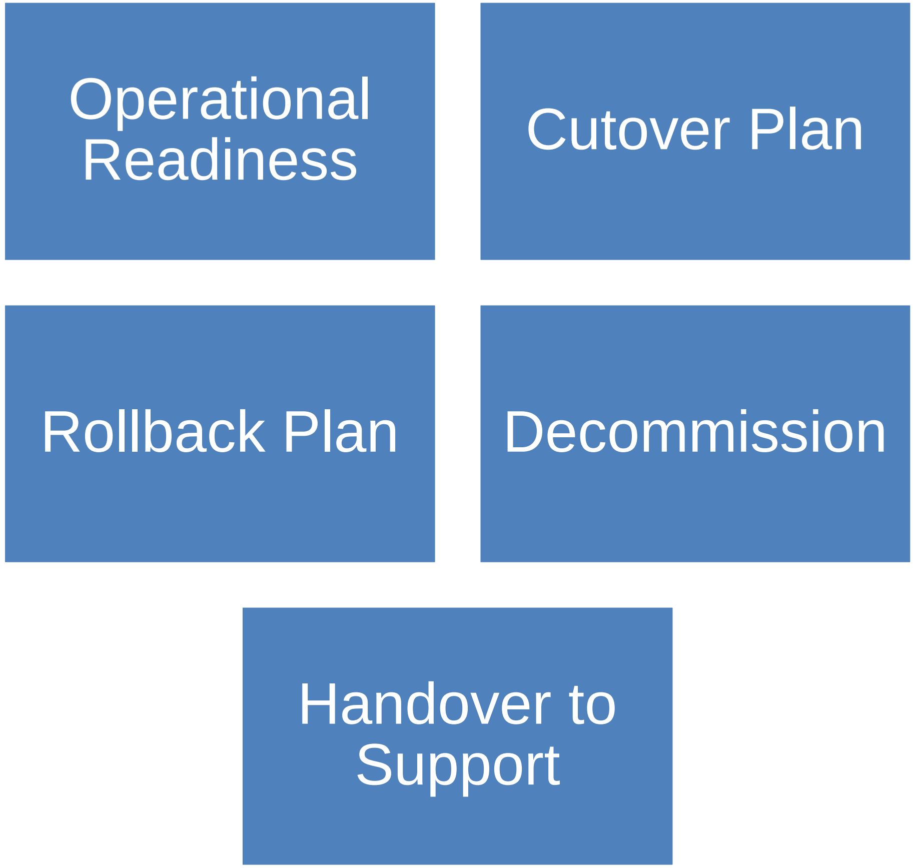
Stage 2: Transition

- 0.1 PIDD - Stage Update
- 0.2 Project Plan - Stage Update
- 1.2 Transition Readiness
- 2.1 Cutover Plan
- 2.2 Go/No-Go Criteria
- 2.3 Service Transition
- SG2 Quality Gate Sign Off

Stage 3: Production

- 0.1 PIDD - Stage Update
- 0.2 Project Plan - Stage Update
- 3.1 Project Closure
- 3.2 Service Transition Complete
- SG3 Quality Gate Sign-Off

Overall Programme View – Post Application Treatment



Operational Readiness

Cutover Plan

Rollback Plan

Decommission

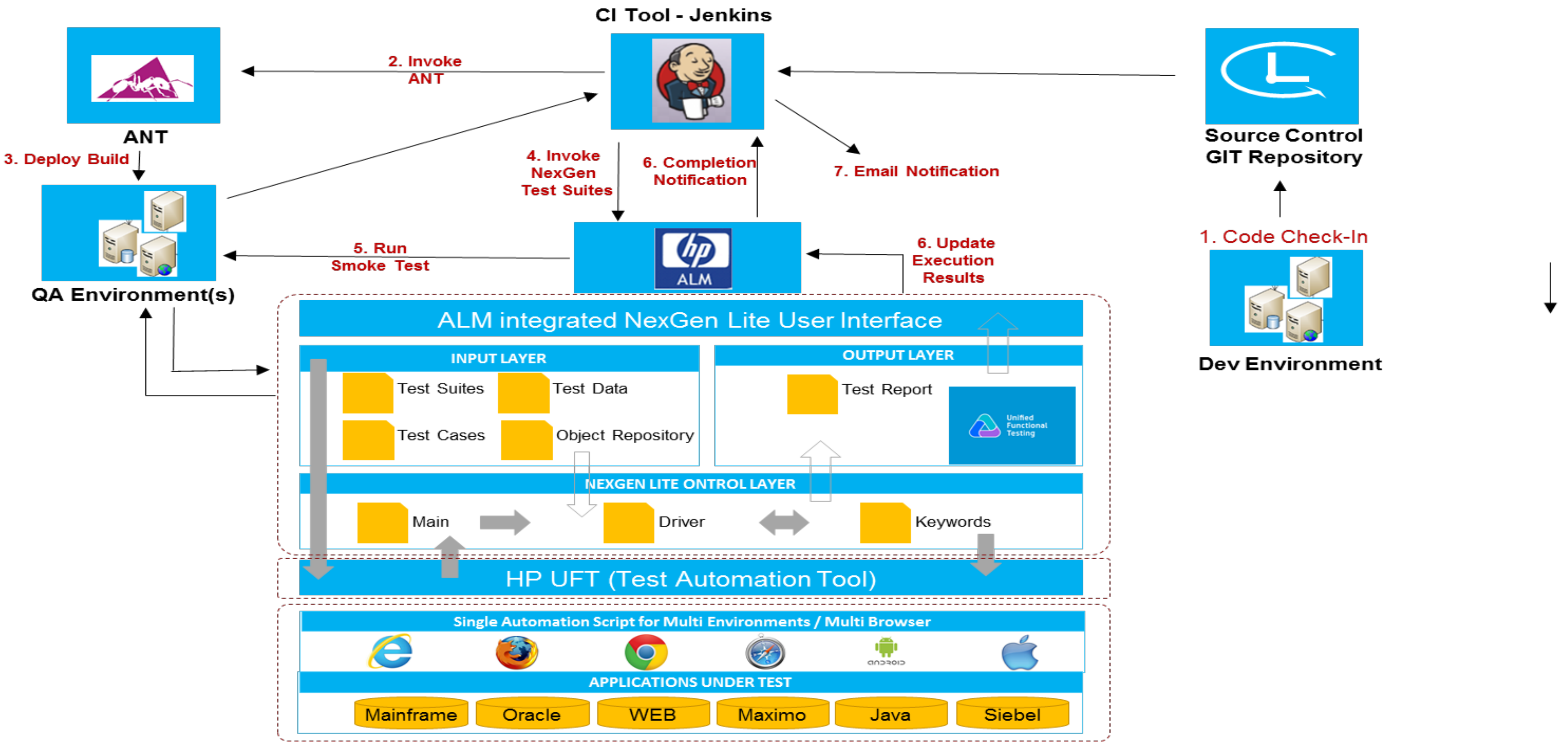
Handover to Support

Test Automation Accelerators

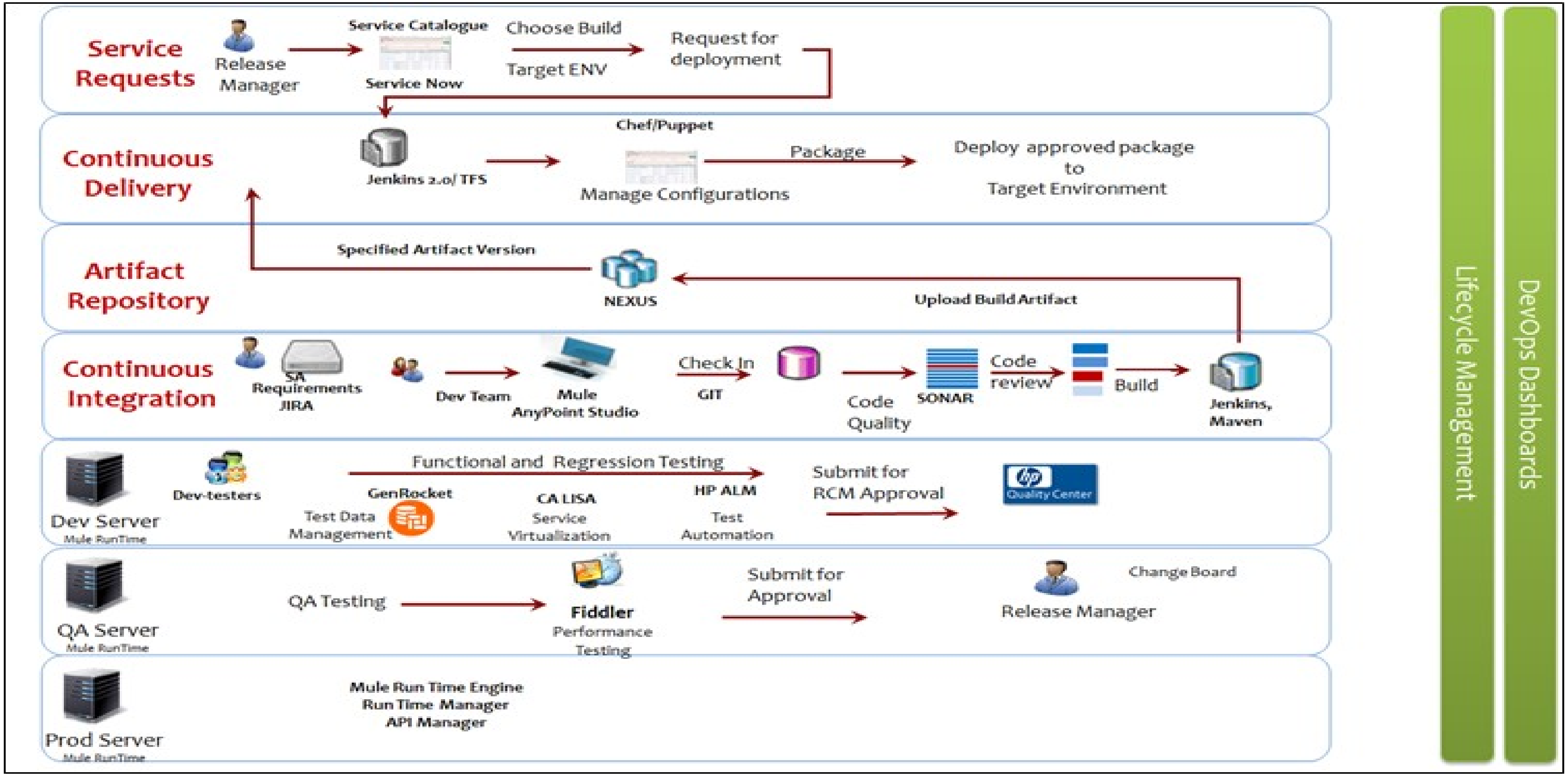
NexGen Test Automation Framework → Accelerate Migration

One Click Automation → Accelerate Migration / Lower Costs

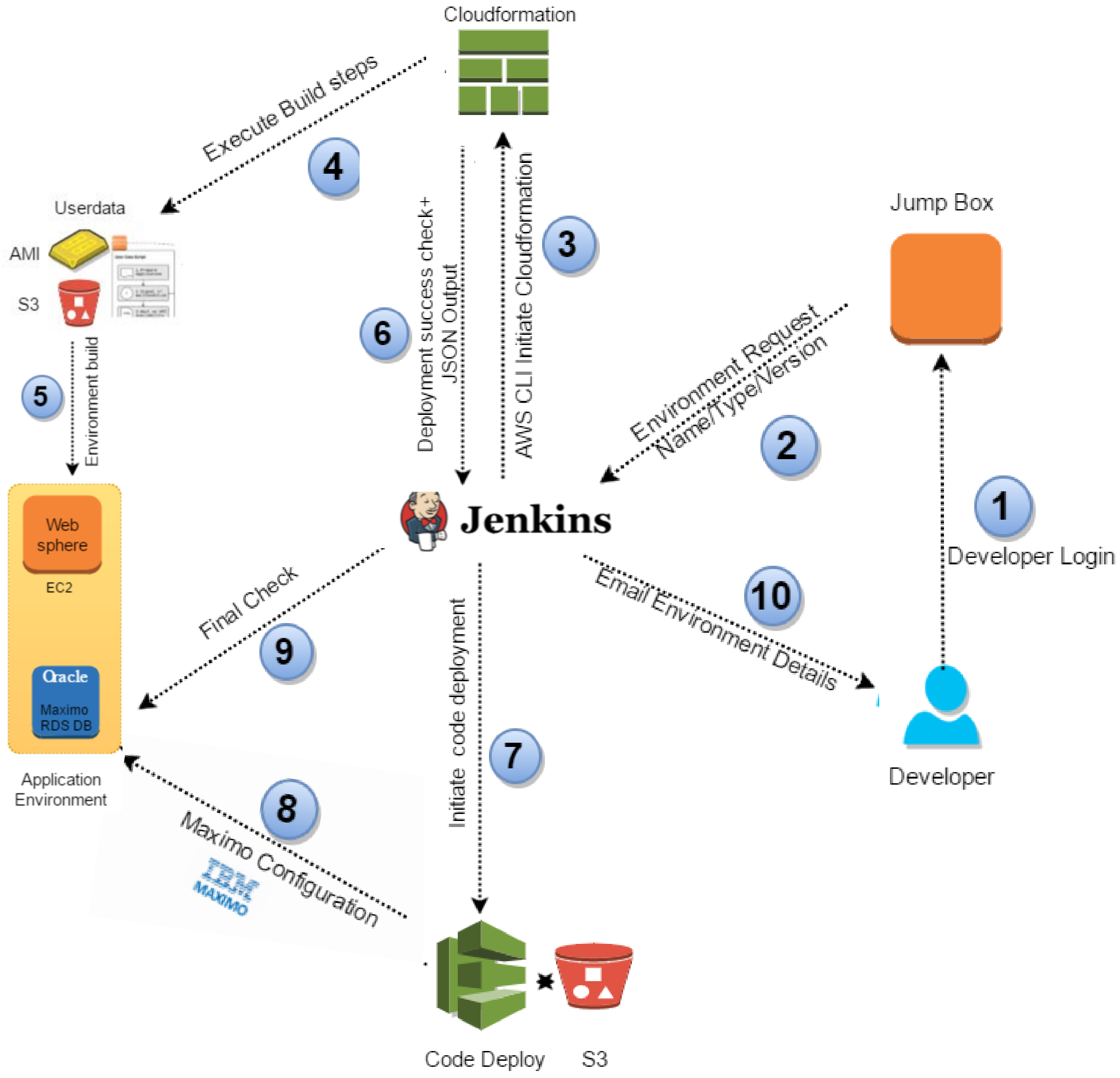
Single Script – Multi Browser / Platform → Accelerate Migration / Lower Costs



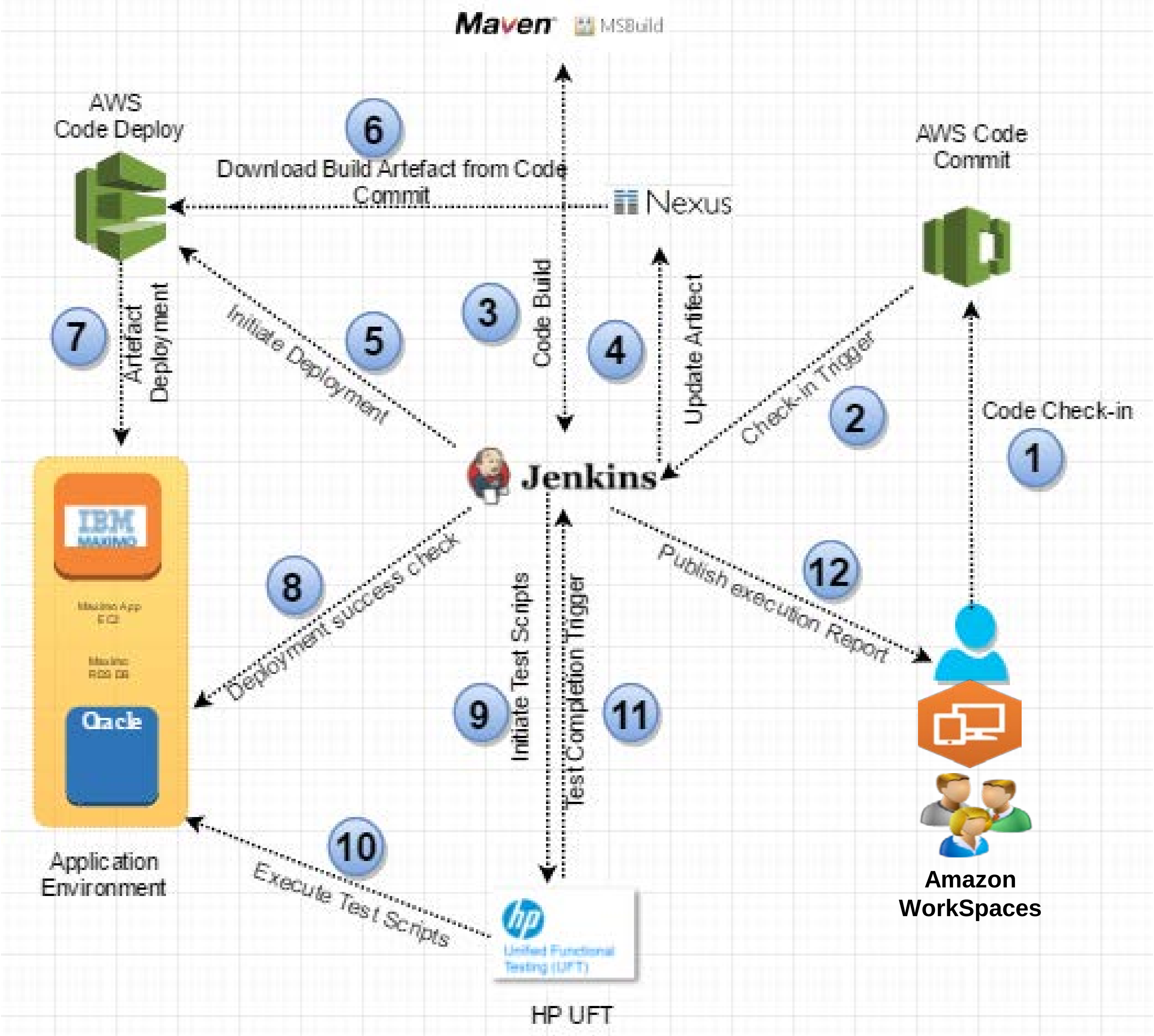
Swim lanes for CI/CD



DevSecOps Framework



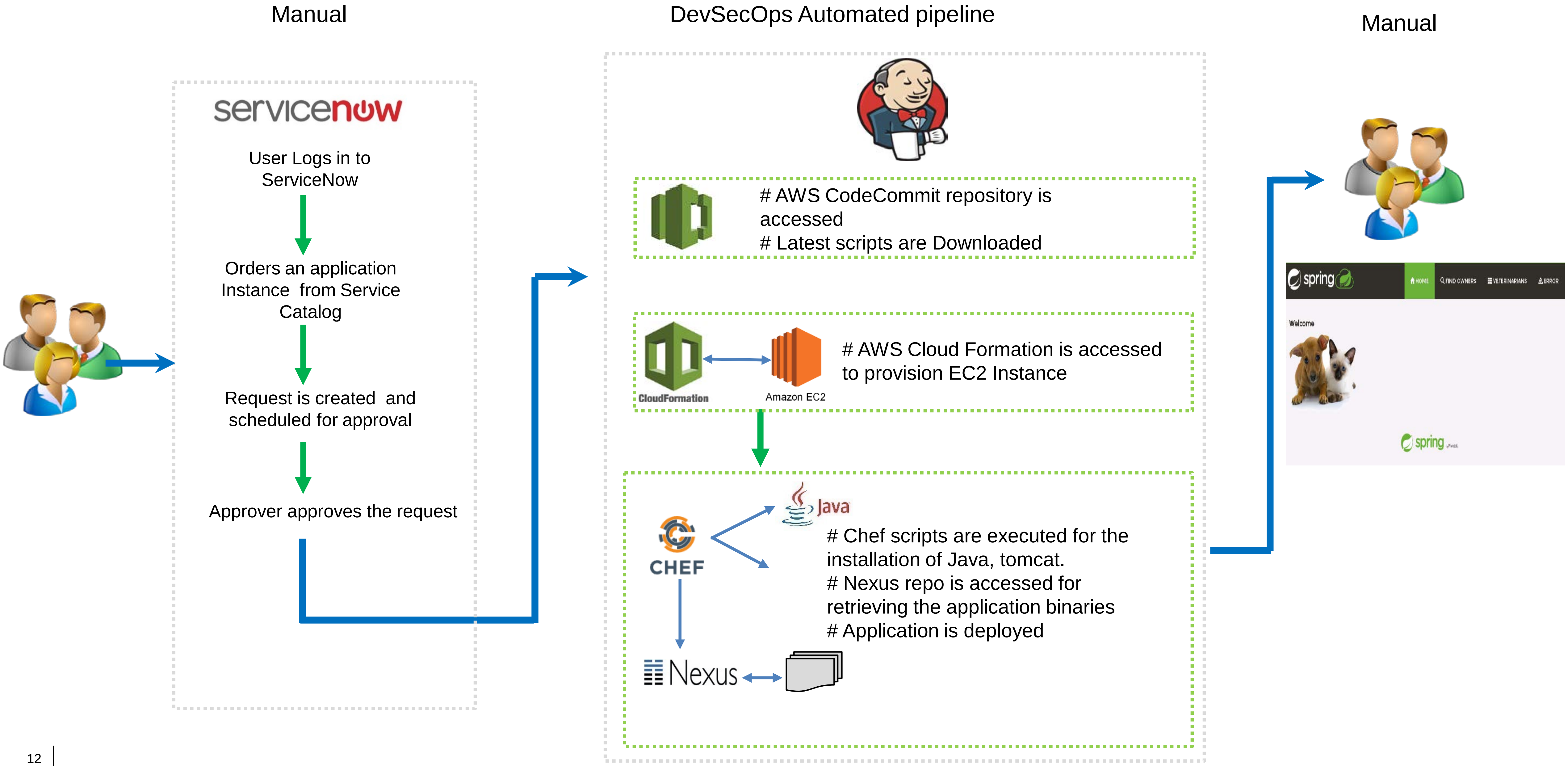
DevSecOps Stack



Key Takeaways

- DevSecOps foundational framework for all applications
- Formulated based on Pilot experience and DD findings
- Maven for Java builds and MSBuild for .NET builds
- Nexus is the artifact repository
- Jenkins is the CI orchestrator
- AWS Code Commit is the Source control system.
- Amazon Code Deploy to automate deployments

ITSM – End to End Orchestration



Manual

servicenow

User Logs in to ServiceNow

Orders an application Instance from Service Catalog

Request is created and scheduled for approval

Approver approves the request

DevSecOps Automated pipeline

# AWS CodeCommit repository is accessed
# Latest scripts are Downloaded

# AWS Cloud Formation is accessed to provision EC2 Instance

# Chef scripts are executed for the installation of Java, tomcat.
# Nexus repo is accessed for retrieving the application binaries
# Application is deployed

Manual

Tools – Testing & Integration

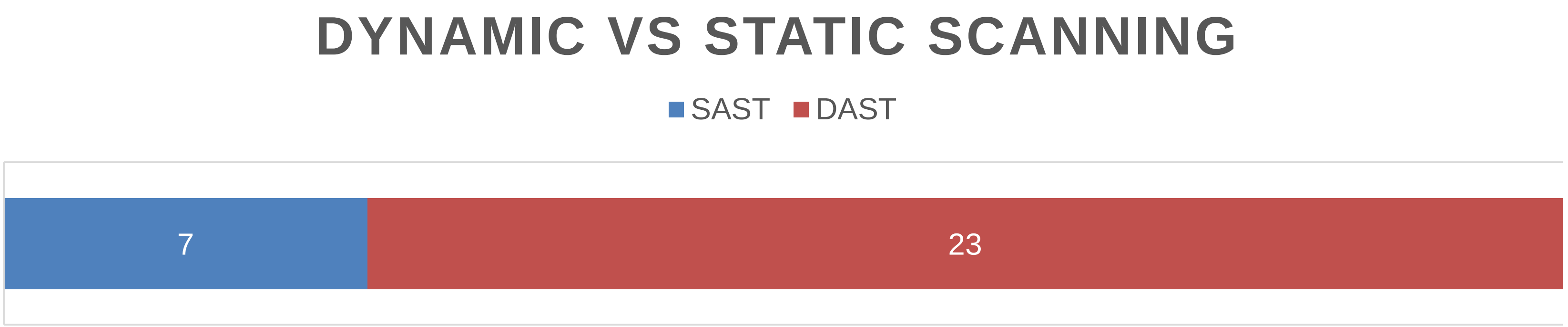
Testing			
S.No		**Tool**	
1	Test Management	HP ALM	
2	Defect Management	HP ALM	
3	Test Automation	HP UFT	
4	Performance / Load Testing	Storm Runner	
5	Security Testing	HP Fortify / IBM Appscan	
6	Automation Framework	NexGen Automation Framework	
7	Performance Test Accelerator	SmartGen	
Integration			
S.No		**Tool**	
1.	Integration testing (manual)	SoapUI/Postman	
2.	Integration Unit Testing	MUnit	
3.	Log Monitoring	Elastic Search & Kibana*	

- * - These tools will be available from April 2017 onwards.
- ** - HCL will cost for IBM Appscan separately.

Tools – Migration & Infrastructure

Migration			
S.No		**Tool**	
1	Continuous Integration	Jenkins	
2	Source Control Management	AWS Code Commit	
3	Modernization Accelerator	ATMA	
4	Application Lifecycle Management	ALMSmart	
Infrastructure			
S.No		**Tool**	
1	Provisioning	Service Now	
2	Server Monitoring and Patching	AWS Managed Service	
3	Configuration Management	AWS OpsWorks	
4	Application Monitoring	Dynatrace, New Relic (TBD)	

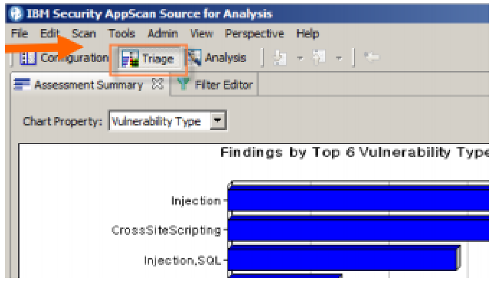
Tools – Scanning



DYNAMIC VS STATIC SCANNING

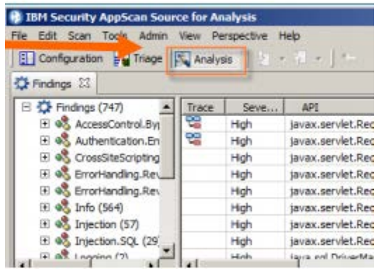
30

- Static application security testing (SAST)
  - Tests the internal structures or workings of an application
  - Referred to as white box testing



IBM Security AppScan Source for Analysis
File Edit Scan Tools Admin View Perspective Help
Configuration
Triage
Analysis
Assessment Summary
Filter Editor
Chart Property: Vulnerability Type
Findings by Top 6 Vulnerability Type
Injection
CrossSiteScripting
Injection.SQL

TRIAGE



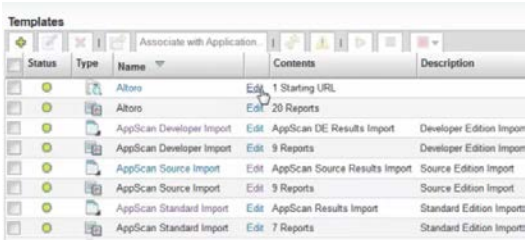
IBM Security AppScan Source for Analysis
File Edit Scan Tools Admin View Perspective Help
Configuration
Triage
Analysis
Findings

- Findings (747)
  - AccessControl.Byp
  - Authentication.En
  - CrossSiteScripting
  - ErrorHandling.Rev
  - ErrorHandling.Rev
  - Info (564)
  - Injection (57)
  - Injection.SQL (29
  - Logging (2)

Trace	Seve...	API
	High	javax.servlet.Rec
	High	javax.servlet.Rec
	High	javax.servlet.Rec
	High	javax.servlet.Rec
	High	javax.servlet.Rec
	High	javax.servlet.Rec
	High	javax.servlet.Rec
	High	javax.servlet.Rec
	High	java.sql.DriverMa

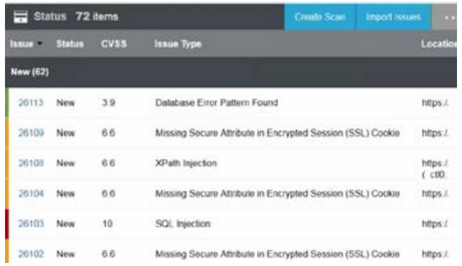
INDIVIDUAL FINDINGS

- Dynamic application security testing (DAST)
  - Tests the functionality of an application
  - Referred to as black box testing



Status	Type	Name		Contents	Description
●		Altoro	Edit	1 Starting URL	
●		Altoro	Edit	20 Reports	
●		AppScan Developer Import	Edit	AppScan DE Results Import	Developer Edition Impor
●		AppScan Developer Import	Edit	9 Reports	Developer Edition Impor
●		AppScan Source Import	Edit	AppScan Source Results Import	Source Edition Import
●		AppScan Source Import	Edit	9 Reports	Source Edition Import
●		AppScan Standard Import	Edit	AppScan Results Import	Standard Edition Imports
●		AppScan Standard Import	Edit	7 Reports	Standard Edition Imports

BLACKBOX TEMPLATING



Issue	Status	CVSS	Issue Type	Locatio
New (62)				
26113	New	3.9	Database Error Pattern Found	https:/
26109	New	6.6	Missing Secure Attribute in Encrypted Session (SSL) Cookie	https:/
26108	New	6.6	XPath Injection	https:/ (ctl0
26104	New	6.6	Missing Secure Attribute in Encrypted Session (SSL) Cookie	https:/
26103	New	10	SQL Injection	https:/
26102	New	6.6	Missing Secure Attribute in Encrypted Session (SSL) Cookie	https:/

CVE/OWASP

* Only Apps where major development effort is required are scoped for Static Scans (7 out of 30)

AppScan Components

SAST vs DAST List