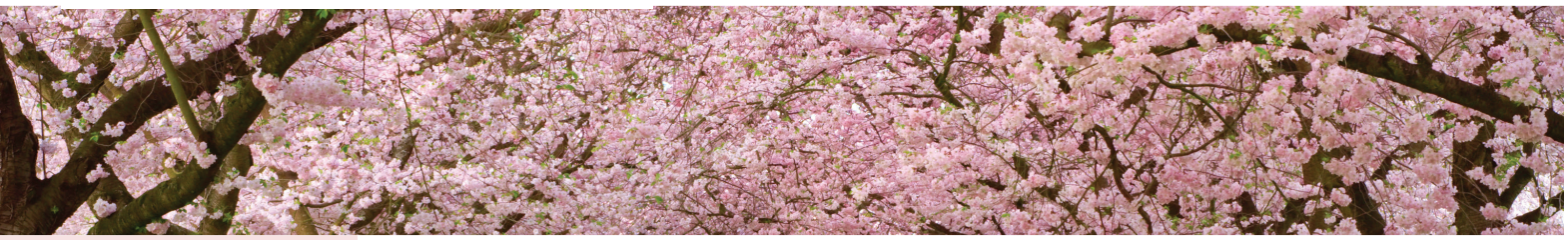
ActioNews

SPRING 2020
THE NEWSLETTER OF ACTIONET



Turning VISION into ACTION®

CHAIRMAN'S NOTE

Dear Friends,

22 years ago, my mentor told me "Ashley, there are only 2 rules in our line of business. Rule number 1 – The customer is always Right. Rule number 2 – If the customer is wrong, read Rule number 1." For our first Good Morning, ActioNet, we would like to feature ActioNet Customer Experience (ACX). We are committed to our Customers' and Each Other's Success.

At ActioNet, we Embrace Diversity and Learn from Each Other. Gratitude brings Happiness. Thanks for continuing to make ActioNet one of the Top Workplaces!

Ashley W. Chen
Chairman & CEO

IN THIS ISSUE

ActioNet Customer Experience (ACX)

By Crystal Compton, Service Delivery

What is Customer Experience (CX)?

In simplest terms, it's how your customers perceive and emotionally feel about their overall experience with your business before, during and after their transaction with you. Per OMB mandate, Circular A-11, Section 280, the government defines it as "a combination of factors that result from touchpoints between an individual, business, or organization. These factors include ease/simplicity, efficiency/speed, and equity/transparency of the process, effectiveness/quality of the service itself, and the helpfulness of service delivery employees." The purpose of CX is to increase customer satisfaction and loyalty via enhanced service delivery.

"Transformation starts with ourselves and ActioNet has defined, built and adopted a CX culture that yields results."

OMB Mandate

The private and government sectors are quickly adopting this framework. OMB mandate (Circular A-11) requires that High Impact Service Providers (HISPs) develop, implement, measure and report out on their Customer Experience Program. HISP are agencies that have a high volume of customer facing transactions. For example: DOS-Passport Services, DHS-Airport Security Checkpoints, and DOT-Taxpayer Services, to name a few. This guidance is expected to establish a CX-mindful culture, provide structure and consistency, identify accountability and governance, ensure high-impact agencies are maturing through government-wide comparative assessments.

continued on page 4

ActioNews, the newsletter of ActioNet, Inc. is published to provide examples and applications of cutting edge IT topics and practices.

ActioNews is published quarterly (March, June, September and December) as a service to its staff, customers, and potential customers.

ActioNews Staff

Lead Designer
Lynda D. Pitman

Contributing Authors
Crystal Compton
Kate Russell

"Establish the Software Factory concept and processes up front - then have technology iteratively enable it."

Software Factory: A Systems View of DevSecOps

By Kate Russell, Program Manager

As a follow on to our Fall 2019 ActioNews article DevSecOps Unleashed, in this article we explore the concept of a DevSecOps "Software Factory". A Software Factory approach is defined as a structured collection of related software assets that aids in producing computer software applications or software components according to specific, externally defined end-user requirements through an assembly process.

Often DevSecOps implementation focuses on advanced capabilities without solidifying fundamentals or modifying well-established governance and/or processes. This tends to result in a significantly inefficient and/or ineffective DevSecOps implementation. Some of the typical impacts of this type of DevSecOps implementation include a CI/CD pipeline that cannot be automated effectively and a loss of quality control…this inevitably leads to an increase in the pace at which chaos occurs. Some things to consider are balancing controls vs flexibility (i.e. Governance). Effective automation requires established process to automate…and finally, that the Crawl, Walk, Run implementation model vs the "Big Bang" approach is recommended to ensure an effective implementation of DevSecOps, and more importantly, a predictable and reliable Software Factory.

To achieve this, consider the following solutions and techniques…establish or modify any governance, policies, and processes to be DevSecOps friendly prior to implementation. Establish the Software Factory concept and processes up front - then have technology iteratively enable it (Continuous Evolution). Finally, follow an evolutionary maturity model to lay the 'building blocks' of capabilities in a deliberate manner.

Breaking down the approach into the following categories will further help to define your Software Factory implementation:

Portfolio and Release Management

Risks: Lack of effective portfolio and release management governance, controls, and planning may lead to a factory model which produces a lot of work but delivers little value.

Solutions and Techniques:

- Smaller Enterprise Planning Sessions
- A disciplined approach of time and resources to strategic planning which is enabled and supported by engineering teams.
- Continuous Planning at the Enterprise, Portfolio and Product Level
- Weekly Enterprise Collaboration for strategic adjustments to the roadmap
- Feedback from Release Management for Continuous Improvements

Change and Configuration Management

Risks: Lackluster CCM often results in little to no control of enterprise changes and their likely negative impacts. Conversely, CCM controls can also be too restrictive, ineffective, and inappropriately applied which results in significant throttling of DevSecOps capabilities.

Solutions and Techniques:

- Institute a Guardrail approach: Clearly delineate between major and minor changes, automate approval conditions, and tightly integrate environment and software baseline change automation throughout the enterprise environments and CI/CD pipeline.
- Ensure extensive integration and automation of CMDB to provide continuous insight
- Effective Knowledge Management which integrates a comprehensive knowledge base of documentation, artifacts, and inventories for products, middleware, and environment for effective and timely Change Impact Analyses
- Scratch builds integrated into CI/CD Pipeline and version control all artifacts (including 3rd party) to build product

Deployment Management

Risks: If there is a lack of or ineffective integration of Quality, CCM, and Security throughout the CI/CD and Factory disciplines, then Deployments tend to produce a myriad of issues during and after deployments. Without matured implementation of these functions with extensive automation as part of the enterprise CI/CD, the result is a significant bottleneck for the delivery of value and releases.

Solutions and Techniques:

- Automated Deployments is typically the

best target to achieve first, then consider Continuous Deployments

- CCM: Keep pre-prod environment mirrored to production, institute Guardrail controls in Dev/Test environments
- QA: Effective implementation of an end-to-end Automated Testing Framework is essential
- Environment Orchestration is essential across the enterprise; take advantage of Infrastructure-as-Code technology

Cybersecurity and Accreditation

Risks: In order for the full benefits of DevSecOps to be realized, Cybersecurity and Accreditation activities should be factored into the factory concept in a way that transforms security into a feature vs. a challenge.

Solutions and Techniques:

- Effective Cyber Compliance in a DevSecOps Software Factory environment requires extensively automated and integrated CCM controls with reliable and accurate information.
- Cybersecurity and Accreditation activities integrated as part of normal feature planning and development or… Security as a feature mindset.

Environment Orchestration

Risks: Overly restrictive environments constrain the ability of the technology to enable efficient development, testing, and deployment. Without a consistent reference architecture, cohesive technology management, and disciplined integration of other software factory functions, then the environment will tend to produce negative outcomes more quickly.

Solutions and Techniques:

- Appropriately allocate Static vs. Dynamic Environments
- Fix only in automation
- Extensively leverage Infrastructure-as-code to provision environments
- Control all configurations, deployment of versioned artifacts only

Development and Testing Framework

Solutions and Techniques:

- Automated Unit Testing Frameworks for developer compile verification
- Continuous Integration Builds with reports
- Automated Smoke Tests to verify Environment Build and Tech Stack
- Automated Critical Functional Test
- Automated Regression Testing
- Security, Performance, Deployment

Enabling Technologies

Risks: Inability to leverage the appropriate technologies to provide the most effective DevSecOps pipeline and Software Factory environment results in an overly complex environment and thus adds additional costs and administrative overhead requirements along with Technology Interoperability.

Solutions and Techniques:

- Plan your processes and identify tools appropriately
- Ensure people, processes, and tools stay in sync
- Ensure your teams are properly trained or have skill sets that match your toolsets
- Don't use only best of breed for selection criteria, but best integration for requirements
- Key on automation

Group Integration and Collaboration

Risks: Knowledge and awareness are key. Ensure all three functions (DEV+SEC+OPS) are aware of key activities of other groups.

Challenge: Having appropriate collaboration on all aspects of the DevSecOps pipeline, impacting effectiveness and predictability. In other words, how to foster collaboration vs. forcing it?

Solutions and Techniques:

- Targeted Enterprise engagement but enable team-level opportunities for collaboration
- Ensure all teams have appropriate representation in SCRUMS, Planning sessions, and other appropriate boards –
- Embed representatives into meetings of other teams (DevSecOps vs. DevOps+Sec)
- Ensure all teams are represented during deployments
- Engineer processes in an integrated approach with representation from all groups

Organizational Alignment

Challenge: Aligning the organization in such a way as to drive Software Factory success rather than individual group success.

Solutions and Techniques:

- Foster collaboration and communication – keep everyone on the same page
- Define a meaningful purpose and clear goals; ensure everyone understands the "why"
- Define and capture metrics that define success

continued on page 4

" Overly restrictive environments constrain the ability of the technology to enable effiecient development, testing, and deployment"

ActioNews

- Founded in 1998, 1000+ ActioNeters in 40+ States
  - Overall Customer Retention Rate > 98%
  - Annualized Professional Staff Retention Rate > 92%
- CMMI®-DEV Level 4 Externally Assessed
- CMMI®-SVC Level 4 Externally Assessed
- HDI Certified Support Center
- ISO 20000 (ITSM), ISO 27001 (Information Security) and ISO 9001 (Quality) Registered
- GWAC and IDIQ Contract Vehicles!
  - **GSA Alliant 2**
  - **GSA IT Schedule 70**
  - **NIH CIO-SP3 SB OTSB**
  - **NIH CIO-SP3 8a OTSB**
  - **GSA PSS**
  - **DISA Encore III**
  - **Air Force NETCENTS-2**
  - **ARMY ITES-3S**
  - **HHS SPARC**
  - **NAVY Seaport-NxG**
  - **NRC GLINDA**
  - **US Courts JMAS IV**
- "92 out of 100" Rating from Open Ratings
- "Exceeds Customer Expectations" from D&B
- "5A1" the Highest Financial Rating from D&B
- Certified Earned Value Management (EVM) System
- DoD Top Secret Facility Clearance with Secret Safeguarding Capability

ActioNet, Inc.
2600 Park Tower Drive
Suite 1000
Vienna, VA 22180
PHONE 703-204-0090
FAX 703-204-4782
info@actionet.com
www.actionet.com

ActioNet

ActioNet Customer Experience continued from page 1

Developing the CX Charter

Create a clear customer experience CX vision

Build the Governance for decision making and cross functional committees

Activate the Roadmap, execute initial CX steps

Develop CX measurements and capture customer feedback via feedback loops, act and communicate

Develop CX Change management and core principals; communicate and empower change agents and front line management

ActioNet Customer Experience (ACX)

ActioNet has also introduced CX to our customers to improve service delivery. For example, we recently introduced and implemented a Customer Experience initiative, working closely with our federal counterpart to implement a plan, targeted areas to focus on, baselined; and ultimately tracked and reported out on progress. This resulted in increased Survey return rates, increased customer satisfaction, improved processes, reduced ticket backlogs, improved employee morale and faster resolution times for service restoration.

To implement CX, there are several templates and tools you can use such as Journey Mappings, Personas, Storytelling Canvas and more. These tools help you to look at where you are, where you want to go, personas of your customers and evaluate touchpoints the customer has with your business. All of these help you truly understand your customer's perspective in order to make improvements. Implementing CX is not a one time process. It is iterative and becomes a culture within your organization.

How does this relate to you? Your agency may be required to implement CX, and therefore you may be answering data calls or improving processes to support their initiatives; or you may consider adding value to your programs by implementing CX.

To learn more about Customer Experience, you can receive training and ultimately a certification. Recently, several ActioNeters took the Forrester training and certification. Some members of this team are actively involved in developing in enhancing our ActioNet Customer Experience (ACX) program to improve the Employee experience, and ultimately drive improved service delivery to our Federal clients and internal customers. Transformation starts with ourselves and ActioNet has defined, built and adopted a CX culture that yields results.

GOOD MORNING ActioNet

Software Factory: A Systems View of DevSecOps continued from page 3

- Implement clear roles and responsibilities, integrate functions together where applicable
- Establish separate DevOps team for the framework and build the pipeline capabilities, but let the dev teams develop their own automated functions for CI/CD pursuant to their product needs

ActioNet knows DevSecOps. By implementing DevSecOps via a Software Factory, or Systems view approach; we take into consideration the implementation of DevSecOps from the governance, processes, and policies perspective to ensure successful implementation of DevSecOps for our customers.