# Technical Architecture Survival Resources

* Product Line Dashboard and VASI system entries <https://app.powerbigov.us/groups/me/apps/5eb0697d-8cc5-4ff1-a01f-fe692977d6c4/reports/f3e44332-26b8-49be-a444-c75b7f3581f0/ReportSection6fba42507bc077948bcc>
* Technical Reference Model (TRM): <http://trm.oit.va.gov/>
* [DevSecOps Enterprise Architecture Repository (OneStop)](https://dvagov.sharepoint.com/sites/OITEPMOVAEA/devops/SitePages/Home.aspx)
* SaaS/PaaS Catalog (VA Cloud Software Catalog)
* [FedRAMP-approved products used in VA](https://marketplace.fedramp.gov/#/agency/department-of-veterans-affairs?sort=productName)
* Relevant Technical Architecture Dashboards:
  + [Security Dashboard](https://app.powerbigov.us/groups/me/apps/5303d5ca-e063-4a4c-bc46-43392328111d/dashboards/6e64419d-90f3-4a64-b278-2a77ea71584d?ctid=e95f1b23-abaf-45ee-821d-b7ab251ab3bf)
  + [Hosting Method Details Dashboard](https://app.powerbigov.us/groups/me/apps/5303d5ca-e063-4a4c-bc46-43392328111d/reports/d66e49b4-914d-4d14-937a-bf29148bd430/ReportSectionbc59fb9b790f16f28f2e?ctid=e95f1b23-abaf-45ee-821d-b7ab251ab3bf)
  + [Technology Dashboards for each product line (current state)](https://app.powerbigov.us/groups/me/apps/5303d5ca-e063-4a4c-bc46-43392328111d/dashboards/ebd6e453-57f9-4666-8e32-2644afe410f8?ctid=e95f1b23-abaf-45ee-821d-b7ab251ab3bf)
  + [Testing Automation Dashboard](https://dvagov.sharepoint.com/sites/OITACOEPortal/ReportingAndAnalytics/SitePages/Testing-Automation-Dashboard.aspx)
* [PAL: DevSecOps Product Management](https://vaww.oed.wss.va.gov/process/Public/API/DisplayFrameworkLt.html?ID=DPM&header=yes)
* API: <https://developer.va.gov/explore> and Status Page: <https://valighthouse.statuspage.io/>
* [ServiceNow – Incident Reports per Product Line](https://yourit.va.gov/$pa_dashboard.do?sysparm_dashboard=9e65282bdb55b34412bc70808c961971&sysparm_tab=35b5e86fdb55b34412bc70808c9619c6&sysparm_cancelable=true&sysparm_editable=false&sysparm_active_panel=false)
* [Approved Secure Configuration Baselines (ITOPS Solution Delivery, Security Engineering)](https://vaww.vashare.oit.va.gov/sites/itops/svcs/sma/BCM/Approved_Baselines/Forms/AllItems.aspx#InplviewHashedefea9d-0c5b-4dfb-8ea5-8618887a60d2=SortField%3DModified-SortDir%3DDesc)
  + The development and approval process for all baselines and implementation standards is now tracked through a ServiceNow request. To request a new or updated baseline or standard, please submit a [SNOW request](https://yourit.va.gov/va?id=sc_cat_item&sys_id=4894aef0dbedc0949b1534cc7c961902).
* Security Engineering references (including ESECC):
  + [Security Engineering Research Analysis Documents](https://vaww.portal2.va.gov/sites/infosecurity/ess/Enterprise%20Security%20Emerging%20Technology%20Review/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fess%2FEnterprise%20Security%20Emerging%20Technology%20Review%2FInitial%20Product%20Review&FolderCTID=0x012000DABFDCB4DD05E84C913E4EB490443108&View=%7B8FBF4B1B%2D473A%2D4AD8%2D8E72%2D4296BEE3FCFD%7D#InplviewHash8fbf4b1b-473a-4ad8-8e72-4296bee3fcfd=FolderCTID%3D0x012000DABFDCB4DD05E84C913E4EB490443108-RootFolder%3D%252Fsites%252Finfosecurity%252Fess%252FEnterprise%2520Security%2520Emerging%2520Technology%2520Review%252FInitial%2520Product%2520Review-SortField%3DModified-SortDir%3DDesc)
  + [Enterprise Security External Change Control Documents](https://vaww.portal2.va.gov/sites/infosecurity/ess/Enterprise%20Security%20Change%20Control%20Board/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fess%2FEnterprise%20Security%20Change%20Control%20Board%2FESECC%20Documents&FolderCTID=0x0120001DB00E0F426C3D429E742B38FC955BDE&View=%7BC2FD1072%2D3E35%2D445C%2DAA1A%2D309444D15588%7D)
  + [Initial Product Reviews (IPR)](https://vaww.portal2.va.gov/sites/infosecurity/ess/Enterprise%20Security%20Emerging%20Technology%20Review/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fess%2FEnterprise%20Security%20Emerging%20Technology%20Review%2FInitial%20Product%20Review&FolderCTID=0x012000DABFDCB4DD05E84C913E4EB490443108&View=%7B8FBF4B1B%2D473A%2D4AD8%2D8E72%2D4296BEE3FCFD%7D#InplviewHash8fbf4b1b-473a-4ad8-8e72-4296bee3fcfd=FolderCTID%3D0x012000DABFDCB4DD05E84C913E4EB490443108-RootFolder%3D%252Fsites%252Finfosecurity%252Fess%252FEnterprise%2520Security%2520Emerging%2520Technology%2520Review%252FInitial%2520Product%2520Review-SortField%3DModified-SortDir%3DDesc)
  + [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks/) - Typically, the order of VA preference of available checklists is DISA STIG, CIS benchmark, third-party NIST checklist, then DISA SRG.
* Human Centered Design (HCD): [Product management handbook](https://department-of-veterans-affairs.github.io/va-product-management-handbook/).
* ITOPS: [Technical Architecture Standards](https://vaww.vashare.oit.va.gov/sites/ioservices/ARC/Lists/Architecture%20Standards%20List/AllItems.aspx#InplviewHashcd45cf3b-655b-42b2-8e07-792445bb8f1b=SortField%3DDocument_x0020_Date-SortDir%3DDesc)
* DOTS: Coordinate with PL tech leads and architects on toolsets, DevTest environment settings/standards, pathways to production, lessons learned/best practices, tool recommendations (either SaaS or new COTS/TRM assessment)
* ATOs: If not already submitted please enter a new item on this portal:  [**eMASS Pre-Registration (click new item on the portal)**](https://vaww.portal2.va.gov/sites/infosecurity/ca/ISRM/Operations/Lists/eMASS%20PreRegistration/AllItems.aspx?InitialTabId=Ribbon.List&VisibilityContext=WSSTabPersistence) that will get it started for ATO process of your new VAEC system (in addition to obtaining a VASI ID)
  + Application registration in the [Common Application Enumeration](https://wiki.mobilehealth.va.gov/display/OISSWA/Common+Application+Enumeration)
  + [VA CSOC vulnerability scanning information (per A&A process)](https://vaww.vashare.oit.va.gov/sites/ois/KnowledgeService/TAAP/Pages/VA-SCAN-Schedule.aspx)
  + [Web Registry](https://vaww.va.gov/webregistry/)
  + [SNOW WAN Request](https://yourit.va.gov/va?id=sc_cat_item&sys_id=6df1dfebdbd413007ed130ca7c96195d)
* Veteran-facing Service Platform (VfSP) – coordinate with Digital Service and PSF
  + Onboarding Guide: <https://department-of-veterans-affairs.github.io/va-digital-service-handbook/delivery/onboard-team>
  + VfSP includes the technologies and processes that support Vets.gov (VASI 2314), and handbook for creating digital services using VfSP is at:
    - <https://department-of-veterans-affairs.github.io/va-digital-service-handbook/delivery/index.html>
    - <https://github.com/department-of-veterans-affairs/va.gov-vfs-teams/blob/master/DeveloperDocs/development-workflow.md>
  + VA.gov – IT problem resolution before going live: <https://vaww.oit.va.gov/how-effective-it-problem-solving-helped-save-the-va-gov-launch/>
* ACOE Release Readiness:
  + [Release Readiness Checklist](https://dvagov.sharepoint.com/:w:/r/sites/OITACOEPortal/QualityAssurance/_layouts/15/Doc.aspx?sourcedoc=%7B22E5C1BA-16A9-41B5-B67F-122925BAB8D8%7D&file=RRC%20-%20Editible%20Version.docx&action=default&mobileredirect=true)
  + [POLARIS](https://polaris.va.gov/sites/URC/Pages/Home.aspx) – Review of relevant releases for projects that relate to the products
* [Enterprise Design Patterns](https://vaww.ea.oit.va.gov/enterprise-design-patterns/) help establish the VA enterprise’s IT principles about the use of enterprise shared services, and authoritative technical standards (including executable templates for CI/CD pipelines and reusable software components provided as hardened containers running in pre-certified dev/test and production environments)
* Digital standards (applicable across all product lines): <https://department-of-veterans-affairs.github.io/va-digital-service-handbook/digital-standards>
* Veterans Experience Office – 3E’S of CX:

<https://www.nextgov.com/it-modernization/2019/05/va-codify-customer-experience-part-core-values/157115/>

* + **Ease:** VA will make access to VA care, benefits, and memorial services smooth and easy.
  + **Effectiveness:** VA will deliver care, benefits and memorial services to the customer’s satisfaction.
  + **Emotion:** VA will deliver care, benefits, and memorial services in a manner that makes customers feel honored and valued in their interactions with VA. VA will use customer experience data and insights in strategy development and decision-making to ensure that the voice of veterans, servicemembers, their families, caregivers, and survivors inform how VA delivers care, benefits, and memorial services.
* VAEC: <https://dvagov.sharepoint.com/sites/OITEPMOECSO/SitePages/VA-Enterprise-Cloud-VAEC.aspx> (Includes VAEC Service Catalog and Azure/AWS Welcome Packets)
  + VAEC Cybersecurity: <https://dvagov.sharepoint.com/sites/OITEPMOECSO/SitePages/Cybersecurity-in-the-VAEC.aspx>
  + Security Lessons Learned from ECSO (applies to all portfolios):
    - Start thinking about the ATO process at the start of your project’s development, not the end
    - Understand the shared responsibility model and what controls you need to focus on in your SSP
    - Use the templates and guidance provided by ECSO
    - ECSO has published a [customer responsibility matrix](https://vaww.portal.va.gov/sites/ECS/Shared%20Documents/Cloud%20101/VAEC_CRM_APPROVED_6FEB2019.xlsx)  to help projects understand who is responsible for what control
    - VAEC can assist teams in collecting evidence of compliance using different tools such as BigFix logs and Nessus scans

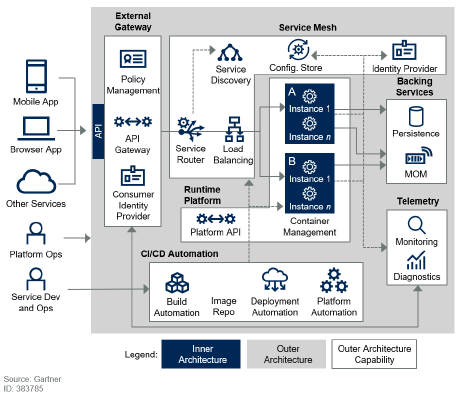
Leveraging modern app development technologies like Docker:

* <https://success.docker.com/article/modernizing-traditional-dot-net-applications>
* <https://blog.docker.com/2018/03/video-series-modernizing-java-apps-developers-part-1/>

Design, Engineering, and Architecture (DEA) Considerations:

* A VA solution that is highly efficient for use, designed to scale out, and measured for the (current) capacity and (future) scalability, which can be monitored and enforced. This includes measurements of capacity (infrastructure, network, and storage) and network performance. Industry metrics and benchmarks for Quality of Service (QoS) levels of capacity and scalability efficiencies apply to VA System Owners building the VA systems and/or VA-approved Cloud Hosting Providers hosting the VA systems, initiating with the planning phase and continuing through the operational phase of the VA systems.
* Use of approved DevSecOps toolchains via TRM and DOTS, and ACOE Technology Support Squad: <https://dvagov.sharepoint.com/sites/OITACOEPortal/TechnicalSolutions/TSS>

Gartner: The agile web application architecture includes an intelligent client in the browser that is backed by APIs supported by lightweight services running on a flexible platform



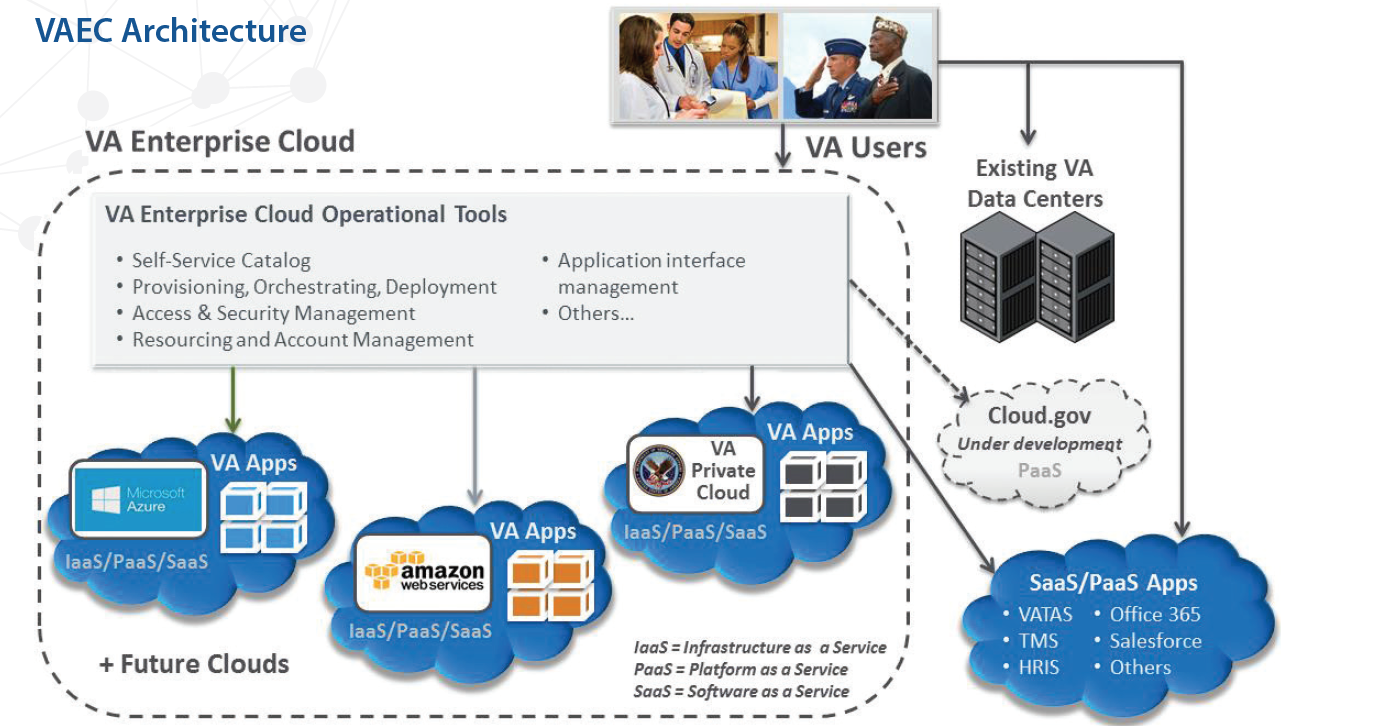
# Technical Architecture Compliance Notes

[Release Readiness Checklist](https://dvagov.sharepoint.com/:w:/r/sites/OITACOEPortal/QualityAssurance/_layouts/15/Doc.aspx?sourcedoc=%7B22E5C1BA-16A9-41B5-B67F-122925BAB8D8%7D&file=RRC%20-%20Editible%20Version.docx&action=default&mobileredirect=true)

[DEA User Stories (for reference only)](https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/SitePages/Home.aspx)

* Self-certification: The Design, Engineering and Architecture (DEA) compliance epics, sub-epics, and user stories are used for self-certification, and they include acceptance criteria to steer EA alignment throughout the agile IT project lifecycle.
* If it is a new technology/solution, not currently in use at the VA, please fill out the [eMASS Pre -Registration](https://vaww.portal2.va.gov/sites/infosecurity/ca/ISRM/Operations/_layouts/15/start.aspx#/Lists/eMASS%20PreRegistration/AllItems.aspx) form for a “new item”. This will bring the discussion to the GRC Committee for further analysis and ATO boundary resolution. For additional questions please reach out to [VAOITDevOpsIATriage@va.gov](mailto:VAOITDevOpsIATriage@va.gov).
* Are there **any approved tools** that meet my business need?
  + Use TRM-approved tools and approved SNOW configuration items
  + If other tools meet your need, but you have already deployed an unapproved tool, you must put together a transition plan
  + Refer to the VAEC service catalog and SaaS/PaaS Catalog from Project Special Forces
* Is the tool (and version number) currently listed on the TRM?
  + If the tool and/or version number are not published on TRM, submit an “Add/Update” request with the TRM
* Have I contacted my **Information System Security Officer (ISSO)**?
  + Ask your ISSO if you need a “risk assessment” or a “plan of action and milestones (POA&M)” before you start the waiver process. If you do, work with your ISSO to immediately start the eMASS process
* CRISP: ITOPS Solution Delivery creates the National Marker Solutions (passes over desktop software that has a waiver so it won’t get removed) for project teams to ensure waivered instances of unapproved technology are not remediated (removed)
* Enterprise Endpoint Management and Reporting (SCCM): <https://vaww.vashare.oit.va.gov/sites/SMS/EnterpriseReporting/SitePages/Home.aspx>
* Baselines:<https://vaww.vashare.oit.va.gov/sites/SMS/EnterpriseReporting/Baselines/SitePages/Home.aspx>
* TRM Software Removal: <https://vaww.eie.va.gov/SysDesign/CS/Lists/TRM%20Software%20Removal/AllItems.aspx>
* CSOC Notifications: <https://vaww.vashare.oit.va.gov/sites/ois/KnowledgeService/TAAP/Pages/VA-CSOC-Notification-Types.aspx>
* [ICAMP Report for TRM](http://trm.oit.va.gov/ReportICAMP.aspx) and [ICAMP site](https://spsites.cdw.va.gov/sites/FODW_PVT/newt/Home.aspx)

# VA Enterprise Cloud (VAEC) Notes



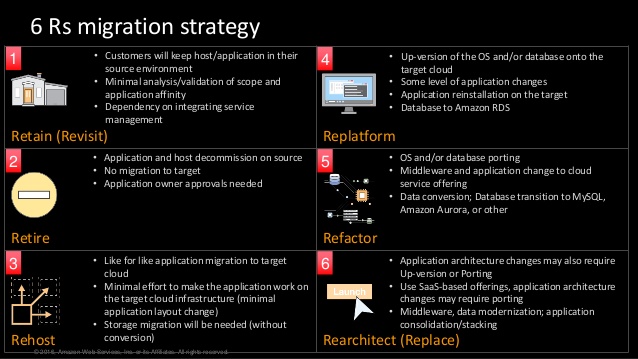
VAEC Service Catalog for both FedRAMP-approved AWS GovCloud and Azure services:

<https://dvagov.sharepoint.com/sites/OITEPMOECSO/SitePages/Cybersecurity-in-the-VAEC.aspx>

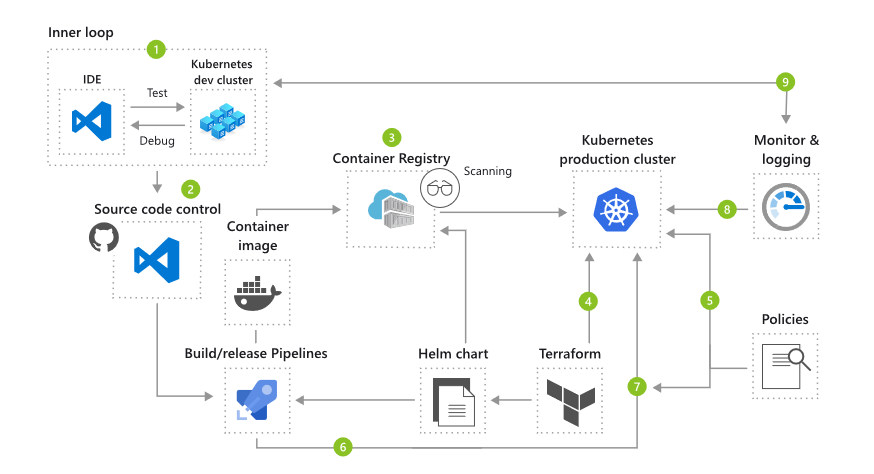
General Support Services (GSS):

Consult the VAEC site for more information on the latest GSS service offerings.

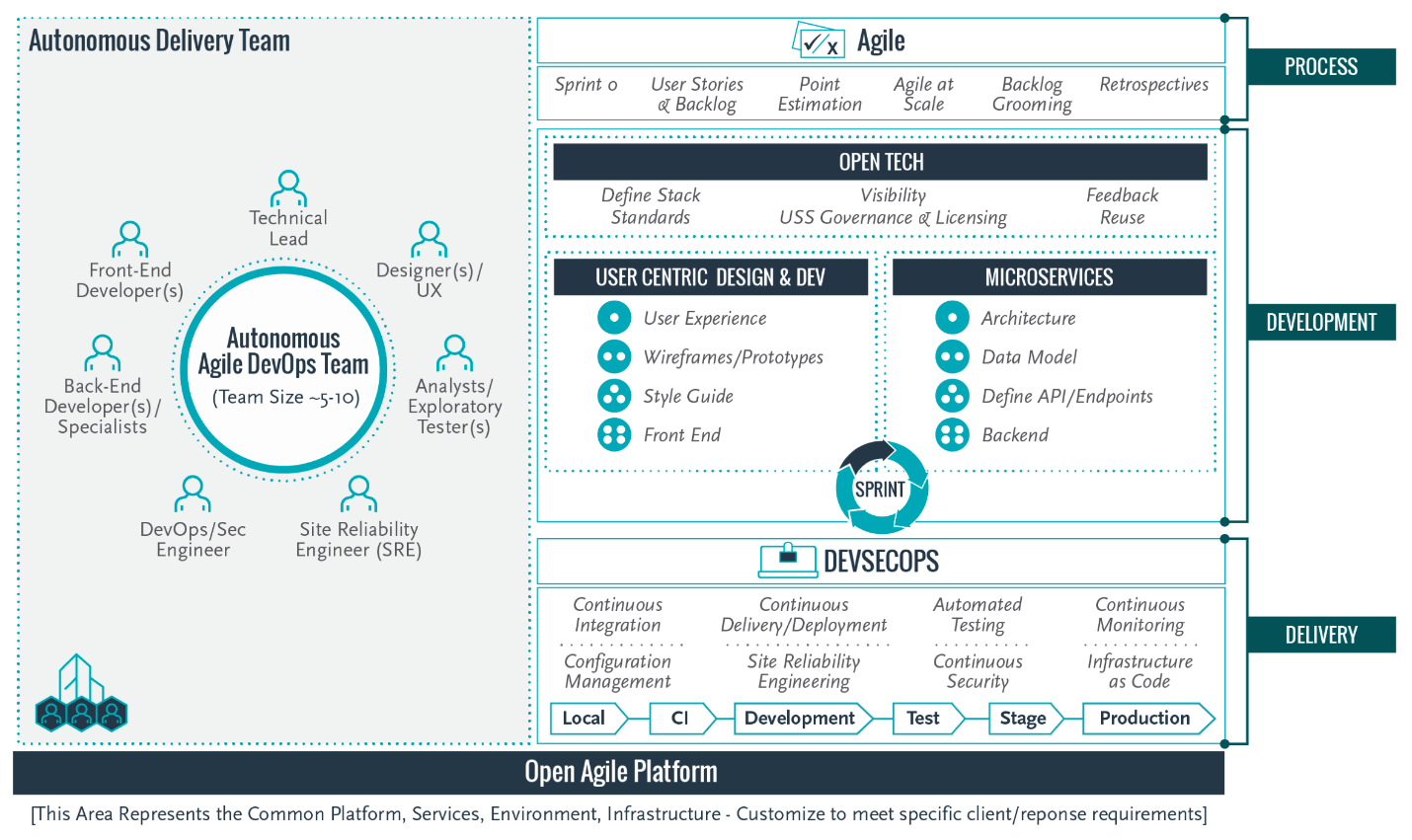
|  |  |
| --- | --- |
| **Common Services** | **Common Security and Scanning Tools** |
| * GitHub * Ansible * CA-Hub (monitoring) – APM (Data footprint) * Identity Access Management (IAM) * AD - Data Subnet * DNS Server * SMTP Relays * ADFS- SSO Services * Jump Box * File Landing Zone * Disaster recovery * Backup * VM Operating System image management | * Splunk SH * Splunk Indexer * Nessus * BigFix * McAfee |



Azure Design Pattern:



# Notes on DevSecOps Framework



[Reference Design Resources](https://vaww.vashare.oit.va.gov/sites/OneVaEa/DevOps/SitePages/Home.aspx?RootFolder=%2Fsites%2FOneVaEa%2FDevOps%2FShared%20Documents%2FDevSecOps%20References&FolderCTID=0x0120005AAC4DE7AECBD8449A40FBB09F96B75E&View=%7B3A256C5A%2D27B6%2D46F5%2D9D2B%2D2EEA7B654F5B%7D)

PAL: <https://vaww.oed.wss.va.gov/process/Public/API/DisplayOrganization.html?id=86&header=yes>

Release Process:

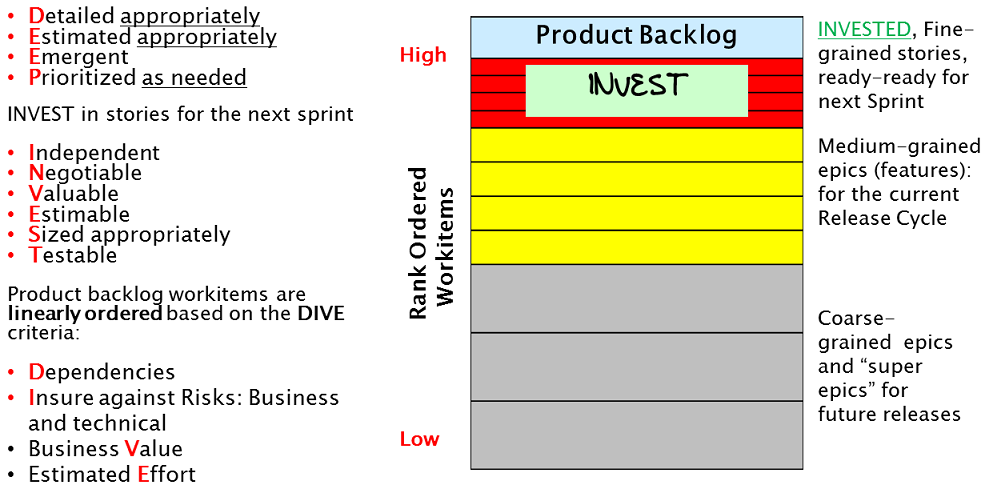
* Step 0: Understand the user need
* Step 1: Create a ticket to define and track the work
* Step 2: Develop new feature in a branch
* Step 3: Create pull request and run automated tests
* Step 4: Code Review
* Step 5: Merge code, deploy to non-production environment(s), verify functionality
* Step 6: Production approval
* Step 7: Build code and create necessary artifacts
* Step 8: Deploy to Production
* Step 9: Measure
* Step 10: Iterate

Infrastructure as Code (IaC): <https://www.ibm.com/cloud/learn/infrastructure-as-code>

In an era when it’s not uncommon for an enterprise to deploy hundreds of applications into production every day—and when infrastructure is constantly being spun up, torn down, and scaled up and down in response to developer and user demands—it’s essential for an organization to automate infrastructure in order to control costs, reduce risks, and respond with speed to new business opportunities and competitive threats. IaC makes this automation possible.

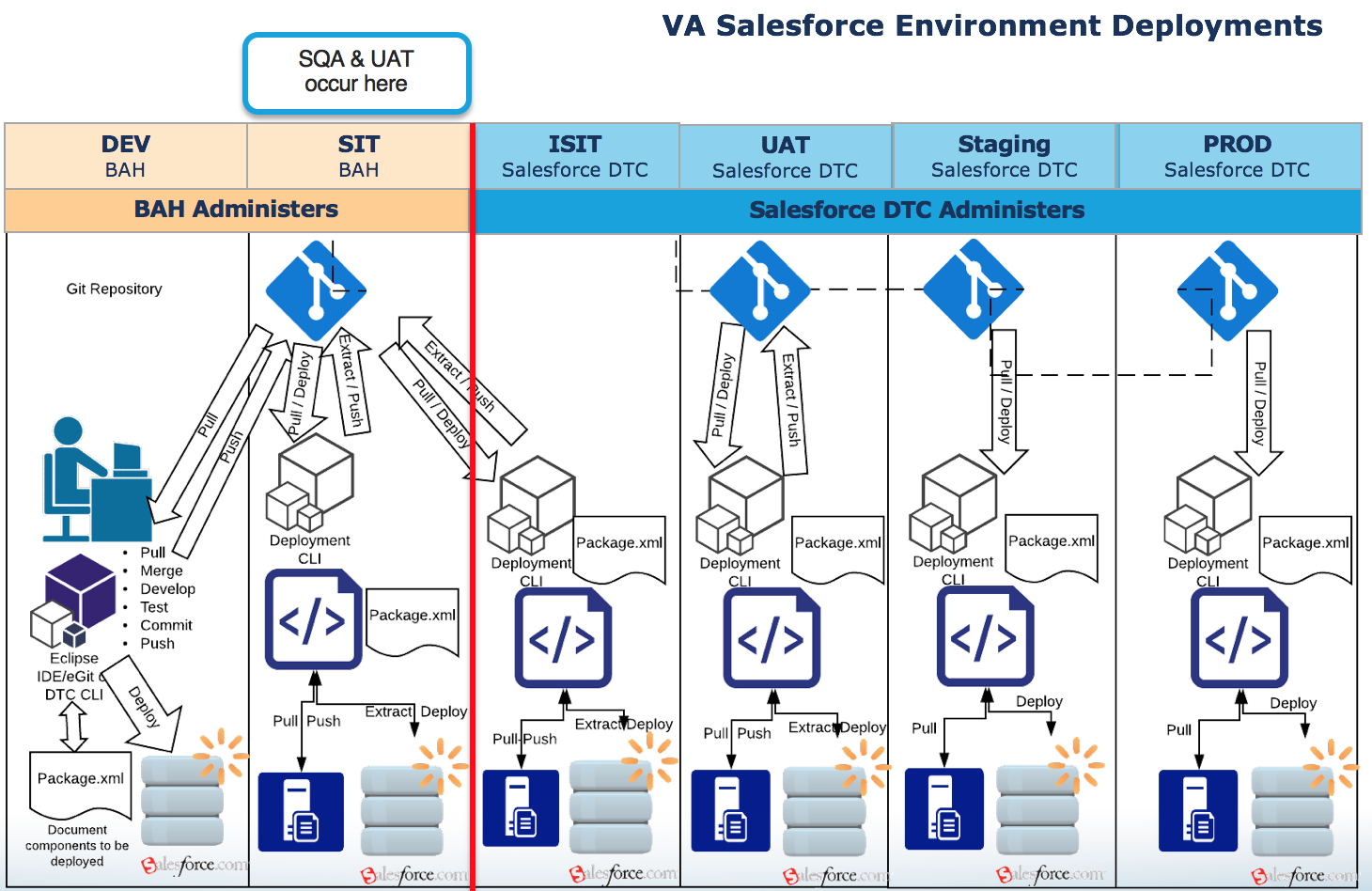
High Availability and Security Best Practices for cloud services (based on AWS but applicable for MAG too):

* Multi-data center architecture intended for high availability
* Isolation of instances between private/public subnets
* Security groups limiting access to only necessary services
* Network access control list (ACL) rules to filter traffic into subnets as an additional layer of network security
* A secured bastion host (not required with AWS Systems Manager Session Manager or Azure Bastion) instance to facilitate restricted login access for system administrator actions (using OpenSSH for Linux, PowerShell for Windows)
* Standard IAM policies with associated groups and roles, exercising least privilege
* Monitoring and logging; alerts and notifications for critical events
* Use object storage such as S3 or Blob Storage (with security features enabled) for logging, archive, and application data
* Implementation of proper load balancing and Auto Scaling capabilities
* HTTPS-enabled load balancers with hardened security policy
* Leverage approved database backup and encryption
* Leverage security tools provided by the ECSO including [AWS Systems Manager, Azure Security Center, and Netskope CASB](https://vaww.infoshare.va.gov/sites/ittrainingacademy/Lists/Calendar/Attachments/2947/4552131_SlidesNotes_20200427_v2%200.pdf)
* Ensure technical architecture is reflected in the epics and stories, and following DEEP, INVEST, and DIVE best practices for the product backlog:



# Guidance to Product Line Technical Architects

* Developer.va.gov includes the discoverable APIs available for consumption by project teams
* Cloud Software Catalog and VAEC Service Catalog provide approved cloud services
* Work with [DevOpsTeam@va.gov](mailto:DevOpsTeam@va.gov) to identify the approved DevSecOps Tool Suite that is customized for the project teams using approved hardened containers and platform services
* Ensure through the DevSecOps Product Line Management Process that approved development, testing, and staging environments are standardized across Product Lines
* VAEC reference architectures and models that support the platforms that are being established for use by the Product Lines in each Portfolio (includes environments and toolset)
* Approved hardware and software inventory, as maintained in eMASS for an ATO and cataloged through SNOW (each configuration item should have an SLA)
* Leverage the approved enterprise IT shared services, platforms and standard tools (tech roadmap for the approved toolchains, as documented in TRM), including any links to implementation details such as pre-approved templates for use in the testing and production environments to which products will be deployed and managed
* MBMS example showing different environments used:



Create an inventory of assets that will comprise the system/application. These should include all hardware, software, and other resources such as data files and network devices that are critical to the continued operation of the system/application. This inventory should include descriptions of the hardware, unique asset or host names (if possible), and the platform/ operating system/version number (if applicable) for each asset. This section should exactly mirror the System Security Plan (SSP).

|  |  |  |
| --- | --- | --- |
| System Resource/Component | Platform/OS/Version (As Applicable) | Description |
| Web Server 1 | Optiplex GX280 | Website Host |

TRM Compliance Review Example:

| Table 5: Software Inventory | | | |
| --- | --- | --- | --- |
| **Vendor** | **Product** | **Version** | **Waiver?** |
| Red Hat OpenShift | Container Platform | 3.7 | No |
| Red Hat | Ansible Tower |  | No |
| Red Hat | Enterprise Linux | 7.4 | No |
| Oracle | Database | 12c, 12.2 | No |

Platform Deployment: Identifies hardware (also in eMASS), operating systems, communication paths and protocols. Also identifies production deployment locations (also in SSPs).

Before Developing Solutions:

Defining and documenting the need and purpose for the information system/application. It is important to involve key Stakeholders and Business Partners in this early stage. General requirements for the information system/application are established, creating the foundation for security protections. System/application Characterization begins this phase by describing the information system in-depth. This description includes conceptual factors such as mission and function, as well as an inventory of hardware and software components. It should include interfaces with other systems/applications that will be used to define boundaries and interconnections. Integrating security into any organization/information system requires a thorough understanding of the environment.

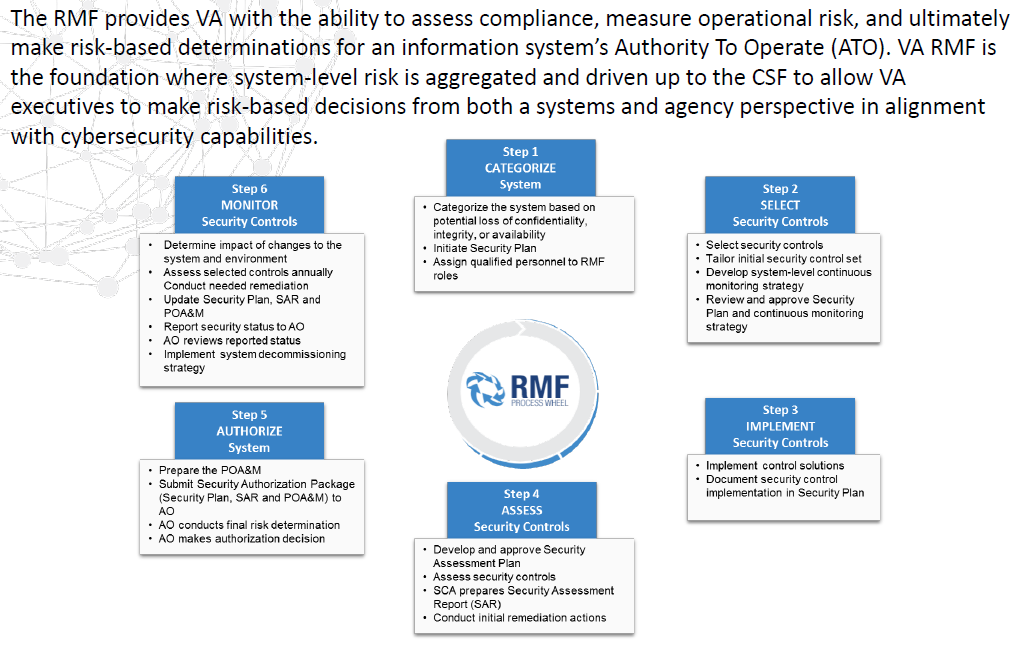
Additional Useful References:

* VAEC Turbot – Security Guardrails as executable patterns for the VAEC GSS <https://turbot.com/features/>
* Helm “charts” that provide templating syntax for Kubernetes YAML manifest documents <https://github.com/helm/charts>
* Open Policy Agent policies in OCP (coming soon): <https://www.openpolicyagent.org/>
* Reusable scripts for PowerShell or procedures using Azure/AWS portals <https://docs.ec.va.gov/Cloud-Learning/Azure/Deployment/Deploying-A-VA-Windows-VM-To-Azure.html>
* Approved secure configuration baselines and settings: <https://vaww.vashare.oit.va.gov/sites/itops/svcs/sma/BCM/Pages/BCM.aspx>
  + SNOW: <https://yourit.va.gov/va?id=sc_cat_item&sys_id=4894aef0dbedc0949b1534cc7c961902>
  + CM-6: <https://nvd.nist.gov/800-53/Rev4/control/CM-6>
* Design System Components: <https://design.va.gov/components/>

# Security Architecture Notes

ISRM BRD: <https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/brd/default.aspx>

Cloud ATO Templates: <https://dvagov.sharepoint.com/sites/OITEPMOECSO/SitePages/Cybersecurity-in-the-VAEC.aspx>



**DevSecOps IA:** Security Categorization for DevSecOps Systems

**eMASS and Security Documentation**

<https://vaww.vashare.oit.va.gov/sites/ois/KnowledgeService/Pages/eMASS.aspx>

* Disaster Recovery Plan (DRP);
* ESECC/NCCB Review and Approval for any External Connection;
* Incident Response Plan (IRP);
* Information Security Contingency Plan (ISCP);
* Interconnection Security Agreement (ISA) (also could include ICD) [Follow NIST SP 800-47](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf)
* Memorandum of Understanding (MOU);
* Plan of Action and Milestones (POA&M) for Risk Acceptance or IA Control Deviation;
* Privacy Impact Assessment (PIA);
* Privacy Threshold Analysis (PTA);
* Secure Design Review (SDR);
* System Risk Assessment Report (SRAR);
* System Security Plan (SSP);
* **Technical Reference Model (TRM) Approval for Software; and**
* Wide Area Network (WAN)/Capacity Planning.
* **AOSB to be submitted with ATO Packet**

If applicable - **System of Records Notice (SORN).**  A SORN is a formal notice to the public published in the Federal Register about use of PII/PHI

**Security Testing and Scanning**

* Control Implementation;
* Hardware/Software (HW/SW) Security Review or Security Assessment;
* CSOC Nessus Scan (NEEDS TO BE MONTHLY);
* Secure Code Review;
* Security Configuration Compliance;
* Security Control Assessment;
* Secure Design Review/Threat Modeling;
* Web Application Security Assessment (WASA) and Penetration Testing

|  |  |
| --- | --- |
| Authorization SOP | [See Authorization SOP for Guidance](https://vaww.vashare.oit.va.gov/sites/ois/KnowledgeService/eMassDocumentLibrary/eMASS_Authorization_Requirements_SOP_Guide.pdf) |
| POAM Management Guide | [POAM Management Guide](https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/ATO%20Documents/POAM%20Management%20Guide.aspx) |
| Application Registration in VASI | [VASI and Instructions](http://vaww.ea.oit.va.gov/enterprise-architecture/va-systems-inventory/)  Web Registry  <https://vaww.va.gov/webregistry/index.cfm?action=welcome> |
| Application Registration for COTS VA Applications | [VA COTS Application and Instructions](https://wiki.mobilehealth.va.gov/display/OISSWA/How+to+open+an+NSD+ticket+to+register+a+VA+application) |

Continuous Monitoring: In each sprint or build, the software code and/or binaries should be scanned for common vulnerabilities or weaknesses, for secure configurations to ensure they meet the United States Government (USG) secure configuration benchmarks or Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), and on the network environment.

NOTE: Accredited systems subject to change control are configured according to product baselines (CM-6) which require a minimum number of audit events be logged (AU-2) to support after-the-fact investigations of security incidents

NOTE: All software and hardware must be imported into eMASS via the Inventory template. This helps initiate the CDM for each system as well as ICAMP and Security Configuration Compliance Data (SCCD) using BigFix. The ISCM IPT receives data and updates from VA stakeholders responsible for managing VA’s existing continuous monitoring capabilities and provides oversight to VA’s ISCM activities.

Leverage baselines and standards:

* Configuration Baseline: Related to all the resources within *a general operational environment* that support the same mission and functions. Baseline (IT product and information system) processes and compliance are audited by OIG. A secure configuration baseline includes a set of security control and configuration settings for an IT product applied to an operational environment as directed by NIST (SP 800-53 CM-6 Configuration Settings).
* Standard: An overarching view/topology of how a solution or technology should be implemented based on vendor best practices, VA policy and other technical or business requirements. Standards development, use and compliance are not audited by OIG.

**TRM:**

The TRM only provides enterprise-level decisions on software usage approval. **Regarding purchasing, installing and/or using a product, we recommend that you contact your local acquisition/procurement office, your local IT/ISO staff, and/or the Enterprise Service Desk at (855) 673-4357 or**[**https://yourit.va.gov/va**](https://yourit.va.gov/va)**for assistance**. Software used on the VA Network must be used in accordance with decision information given in the TRM.

**Updated ATO:**

| Changes Likely Considered Significant or Major | |
| --- | --- |
| New Technology (New OS variant, including COTS and appliance, none of which currently exist in the environment) | Use of new external services (e.g., ticketing system, monitoring system) in support of the cloud service |
| New Cloud Service Offering or Feature | Removal of system components or service offering |
| FIPS 199 Categorization Change (e.g., Moderate to High) | PaaS or SaaS changing IaaS Provider |
| Adding/Removing security and privacy controls | New cryptographic modules or services, or changes to existing modules/services |
| Changing alternative (or compensating) security and privacy control(s) | New data center or moving to a new facility |
| New interconnection or changes to existing interconnection | Scanning tool changes |
| Upgrade of OS | New system monitoring capabilities or replacement of system monitoring capabilities |
| New Virtual Server(s) | New/upgrade of DBMS (SQL Server, Oracle, etc.) |
| New Code Release | New authentication mechanisms or changes to existing mechanisms |
| New boundary protection mechanisms or changes to existing mechanisms; changes to routing rules | Change in cloud service ownership that would result in major changes (e.g. change to contingency planning or incident response processes/capabilities) |
| Changed or updated backup mechanisms and processes | Movement of information system data to a different system boundary |

# Release Readiness Guidance

If an item is NA per the Release User Stories, please specify NA. DevSecOps Checklist: <https://docs.microsoft.com/en-us/azure/architecture/checklist/dev-ops>

* Links to Product Code Releases URLs
* User Stories (US) are completed and approved
* US Tests are created
* US Tests traced to Release User Stories
* Non-production testing is complete (functional, regression, integration, SQA, UAT, etc.)
* No open critical or high severity defects being implemented into production
* All open high exposure risks are mitigated
* AFMP completed and approved
* If applicable, IOC site Concurrence
* If applicable HPS AC Concurrence
* Architecture verified (TOUCH POINT WITH EA AND SOLUTION ARCHITECTURE)
* Section 508 addressed (mostly manual but uses TRM approved tools to support)
* Valid ATO (TOUCH POINT WITH EA AND SOLUTION ARCHITECTURE)
* Deployment, Installation, Backout, and Rollback (DIBR) procedures completed
* Operations Procedures completed (similar to Production Operations Manual)
* Operations RACI completed
* SLAs/OLAs completed and approved
* User Documentation complete

Example Continuous Deployment from MHV:

Pull Request is created to pull the release configuration into the pre-production environment so that configuration validation can occur. If pre-production validation of the release configuration works as expected (passes), a final pull request for promoting the release configuration into production is created which sets the stage for the production release of the release configuration. We recommend the product owner and business owners, production line manager, contract program manager be assigned as approvers for the promotion to production environments to support governance initiatives. All release artifacts should be accessible through the release branch documentation in the application catalog GitHub repository. Once all approvals have been received the schedule is set for production deployment. At the time identified for the release configuration to be promoted to the production environment, the RM/CM owner of the pull request will merge the changes into the master branch of the application catalog GitHub repository which will trigger the CD processes to update the production environment servers. The application is then smoke tested to ensure that the system is functional and ready for users to start using again.

NOTE: Need to be able to parameterize the disabling of the maintenance page in the case of production. We leave the maintenance page up while manual smoke testing occurs. If we can pass a flag to the CD process, then we should be able to skip the Disable Maint phase until we have had time to validate the application release configuration is functioning as designed. Once we are happy with the smoke test results, we should be able to run the release build without the flag - no changes should be applied to the environment because the environment already consistent with the application catalog - to cause the maintenance page to be disabled.

In the event that either the testing of the release configuration in either the pre-production or production environments fails, the systems will be rolled back to the previous healthy state of the application configuration using git / GitHub tools for rolling back the application catalog to a previous version. The description of how to do that is outside of the scope of this document but is well documented online.

In the event that there is a need to apply a patch or hotfix to an existing release or we need to create a release configuration on top of another release configuration, as would be done in a typical iterative workflow, we would simply base the branch for the release configuration in the application catalog from a previous release configuration branch.