

Governance for System Integrators: PEGA

The establishment and enforcement of policies, procedures, and guidelines that guide the software development and deployment processes. Ensures that development teams follow best practices, security measures, compliance requirements, and operational standards. Monitoring, auditing, and enforcing these rules across the software development lifecycle.

Table of Contents

- [Architecture Review Board](#)
- [Account Management](#)
- [Environment Management](#)
- [508 Compliance](#)
- [Development Support](#)
- [Level Up](#)

Additional Resources

- [Pega Quality Gates: Level-Up!](#)
- [Pega Development Guidelines and Standards SOP](#)
- [How to Open a Change Request](#)
- [SNOW Change Request](#)
- [SI CD 508 SOP](#)
- [508 Mitigation Tracker](#)

Architecture Review Board

DTC requires all applications to go through an Architecture Review Board.

Who is the Pega ARB?

The Pega ARB is a team of architects and IT professionals responsible for evaluating and approving application designs to allow developers to build or modify Pega applications within the VA.

Pega ARB Goals

The Pega ARB provides governance through collaboration with SIs and CDs for application designs by:

- Identifying any risks, gaps, or concerns with application architecture and providing guidance to address them
- Promoting best practices in the following areas
 - Application structure
 - Data model
 - Case design
 - User access and security
 - Integrations
 - Deployment and DevOps
 - Reporting
 - User experience/interface)
- Ensuring applications are designed for reusability, extendibility, and scalability
- Providing guidelines for developing within VA
- Ensuring business goals and objectives are met
- Informing the system owner of upcoming applications

Pega ARB Process

1. Once triage and discovery are completed for a use case and an SI/CD is identified, the SI/CD will be provided a Technical Design Document template to share their solution design.
2. Once SI/CD has completed their solution design they will notify the DTC COE team via email with a copy of the completed Technical Design Document to: amanda.ross3@va.gov and ramakrishnamaraju.keertipati@va.gov

The DTC COE team will schedule ARB meeting within 5 business days.

Meeting Agenda:

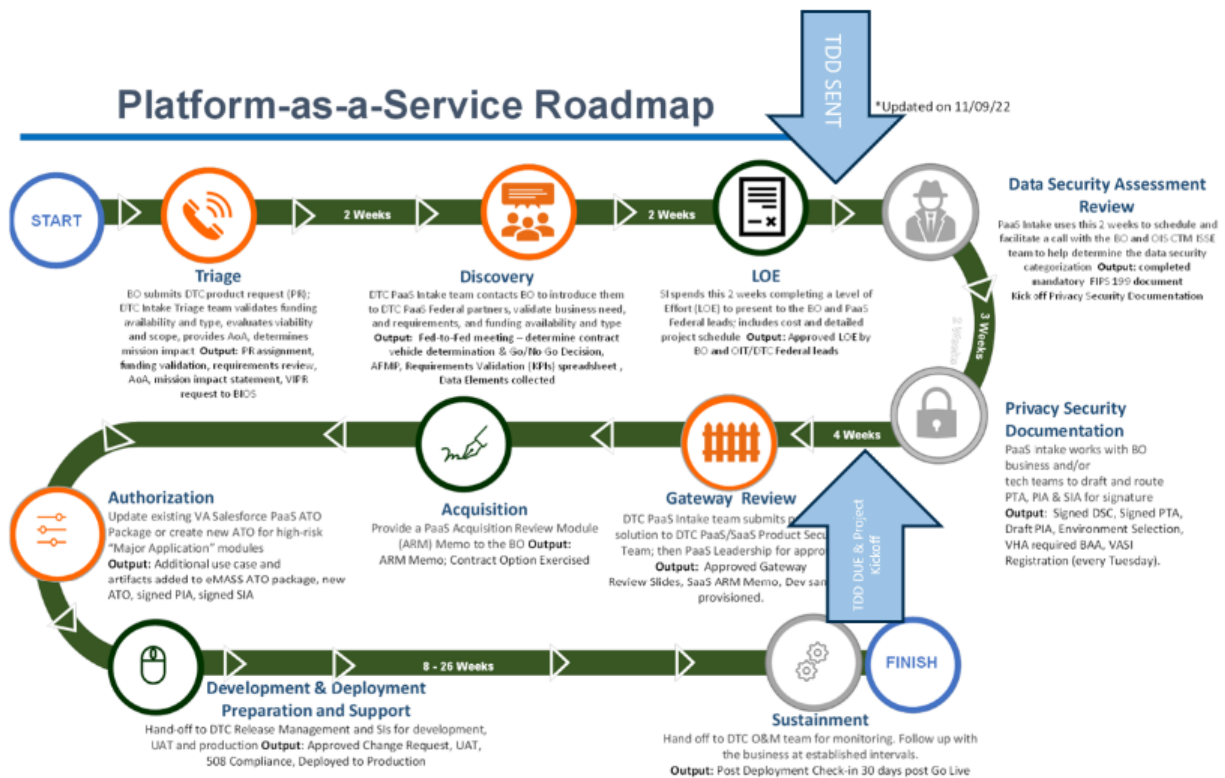
- Review Confluence documentation
- SI/CD summarization of use case and goals
- Review and collaboration on solution design
- Q/A from ARB Board
- Open discussion
- ARB decisioning (Approve or defer decisioning pending additional requested information/required changes)

3.The ARB will provide outcome of ARB review to federal system owner for awareness.

4. ARB approval is a requirement to pass Gateway Review in the DTC PaaS process, and gain access to a sandbox to start development.

Pega ARB Process Visual

ARB can occur any time after Discovery, and approval needs to be received prior to Gateway Approval.



Account Management

Within the VA Pega Platform, there are several types of user accounts. The table below outlines the various types and their purpose.

Account Types	Purpose
Pega COE Admin	This is the highest level of access to the Pega Gov cloud platform. This level gives access to the base platform level access. Only Pega COE Developers will have access to this level.
Pega COE Author	This access level is dedicated to COE Developers to develop and manage Enterprise/Platform level components.
Application Author	Application Author is granted to SI and Citizen Developer (CD) who are configuring any applications or components. Editing capabilities will be limited to that application only. Cross application access is NOT allowed.
Manager /Supervisor	Manager/Supervisor access level is defined at the application level that's specific to the application functionality. Cross application access is NOT allowed.
User Read /Write	This access level is granted to the application users that are requiring to creating a case and performing a task on the workflow. Cross application access is NOT allowed.
User Read Only	This access level is granted to the application users that is only required to view a case or run reports. Cross application access is NOT allowed.

Table 1: User Account Management

1. Establishing Security Groups

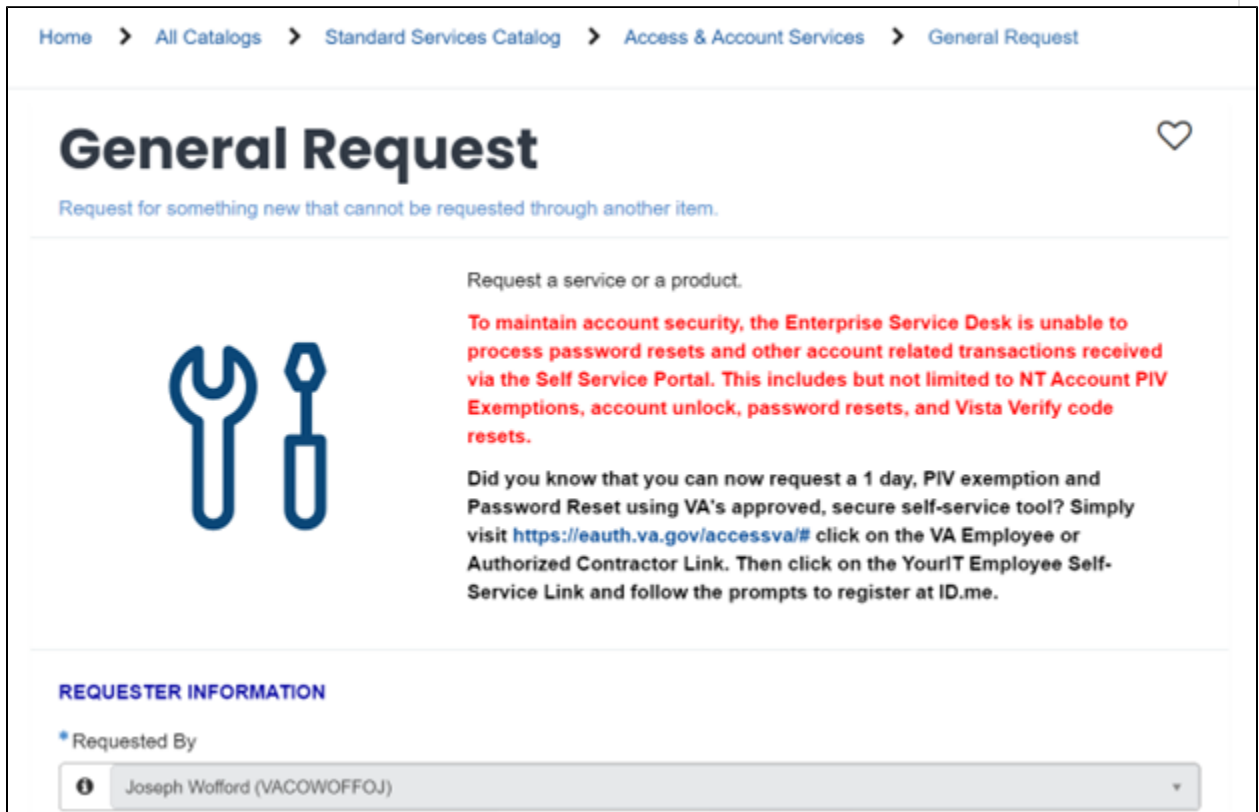
During the design review process, the SI/CD will work with the COE team to determine the required personas for their project. The DTC Pega COE will create the necessary security groups in Active Directory (AD) for the users to be added once the application goes live.

2. Establishing Accounts

A specific process needs to be followed to establish an account for each user within the system. The following steps must complete before a new account is established.

The user will complete a SNOW Request at: https://yourit.va.gov/va?id=sc_cat_item&sys_id=8738d403db1eff00b8a6f4821f9619d9

Below is a SAMPLE SNOW request and directions on completing it:



Home > All Catalogs > Standard Services Catalog > Access & Account Services > General Request

General Request

Request for something new that cannot be requested through another item.

Request a service or a product.

To maintain account security, the Enterprise Service Desk is unable to process password resets and other account related transactions received via the Self Service Portal. This includes but not limited to NT Account PIV Exemptions, account unlock, password resets, and Vista Verify code resets.

Did you know that you can now request a 1 day, PIV exemption and Password Reset using VA's approved, secure self-service tool? Simply visit <https://eauth.va.gov/accessva/#> click on the VA Employee or Authorized Contractor Link. Then click on the YourIT Employee Self-Service Link and follow the prompts to register at ID.me.

REQUESTER INFORMATION

* Requested By

Joseph Wofford (VACOWOFFOJ)

1. Fill in the required fields (the building number, floor number, etc. do not matter because this is a website being accessed).
2. In the Brief Description field specify '**Requesting Access to (NAME OF PEGA APPLICATION) AND** Name of the role you need to be assigned to **ROLE/PERSONA: (Application Author, Manager/Supervisor, User Read/Write, User Read Only)**
3. In the Request Assignment Group field select the appropriate group: **(NAME OF PEGA GROUP)**

Request for something new that cannot be requested through another item.

***Brief Description** ⓘ
Please briefly describe your request (in 160 characters or less) ✕

Requesting Access to EHRM-IO E2E Acquisition Hub

***Detailed Description** ⓘ
Please provide a detailed description of the service or item you are requesting (the more information you provide, the faster we can fulfill your request) ✕

Is there a System Name, EE Number or Hostname that can help us fulfill your request? ⓘ
If this information is known at this time, please enter it below. ✕

Request Assignment Group ⓘ
If you know the specific assignment group this request should be assigned to, please select below. If you do not know the specific assignment group, your request will be sent to the Enterprise Service Desk for review and assistance. ✕

ⓘ EHRM-IO PMO E2E Acquisition HUB Team ✕ ▼

Your form should resemble the form shown above.

4. Click the 'Order Now' button.

Once a user has completed the account request, the request will be routed for the appropriate approvals. The CSC team will then review the request and verify that the appropriate approval has been received. The user will then be created and/or added to the appropriate security group (s) based on job requirements and enforcing the least privilege concept.

Please note, SNOW tickets have a minimum 48-hour processing window, however requests can take up to a week to process.

3. Modifying Accounts

If a user is requesting a modification to their account, they must submit an access request (via the VA User Account Request form) along with valid justification to the designated approval authority. Once the approving authority approves the request, the System/Module Administrator is notified, and the modification is made to the account.

SNOW Processing Window

Please note, SNOW tickets have a minimum 48-hour processing window, however requests can take up to a week to process.

SNOW Link: https://yourit.va.gov/va?id=sc_cat_item&sys_id=8738d403db1eff00b8a6f4821f9619d9

4. Disabling Accounts

Common user accounts are Locked and disabled after 45 days of inactivity automatically by the Pega platform. If your account is disabled due to 45 days of inactivity, request for your account to be unlocked by submitting a SNOW ticket.

SNOW Processing Window

Please note, SNOW tickets have a minimum 48-hour processing window, however requests can take up to a week to process.

SNOW Link: https://yourit.va.gov/va?id=sc_cat_item&sys_id=8738d403db1eff00b8a6f4821f9619d9

5. Deleting Accounts

Should an account need to be removed due to termination or reassignment of responsibilities, the account will be disabled at the same time (or just before) the employee is notified of their dismissal or upon receipt of resignation and the VA FIM offboarding process is inherited. The user will no longer be able to access VA Pega when their access to the VA Network and Single Sign On (SSO) are disabled. The user will be set to Inactive in VA Pega with specific security measures put in place, including the removal of permission sets, groups, queues, etc. which provide application access following 45 days of inactivity.

If a user account should need to be reactivated, the user MUST request a user account via the normal new user channels and appropriate access will be given.



SNOW Processing Window

Please note, SNOW tickets have a minimum 48-hour processing window, however requests can take up to a week to process.

SNOW Link: https://yourit.va.gov/va?id=sc_cat_item&sys_id=8738d403db1eff00b8a6f4821f9619d9

6. Project/Department Transfers

When a user is transferred to a different department or project within the VA Pega environment, application owner/business owner/lead system integrator should submit snow ticket to remove themselves from the current project AND submit another snow ticket to gain access to the new project.

This process is designed to ensure that privilege creep does not occur. Audits of User Deactivation, Reactivated Users, and migration of users will take place every 6 months. Application owners will be notified of usage information in order to verify active users.

SNOW Link: https://yourit.va.gov/va?id=sc_cat_item&sys_id=8738d403db1eff00b8a6f4821f9619d9

7. Auditing Accounts

The VA Pega Platform will utilize the Pega audit capabilities to audit the creation, modification, disabling, and termination actions of users and system/service accounts.

Application Development Teams are responsible for the creation of any test "dummy" users in DEV, TEST and STG. If test users are needed in STG, the appropriate setup instructions should be provided in the Deployment Plan for the DTC Pega COE Team. Test "dummy" users are not permitted in environments past TEST as those are full copy or Production environments which contain Protected Health Information / Personally Identifiable Information (PHI/PII), and individual access must be managed/monitored.

The following audit reports are available on the Pega Platform:

1. Report of "Locked Operators"
2. Report of "Disabled Operators"
3. Report of "Users Deactivated Over 90 Days Ago"
4. Report of "All Users by Application Type"

For additional information, see the links listed in additional resources at the top of this page.

Environment Management

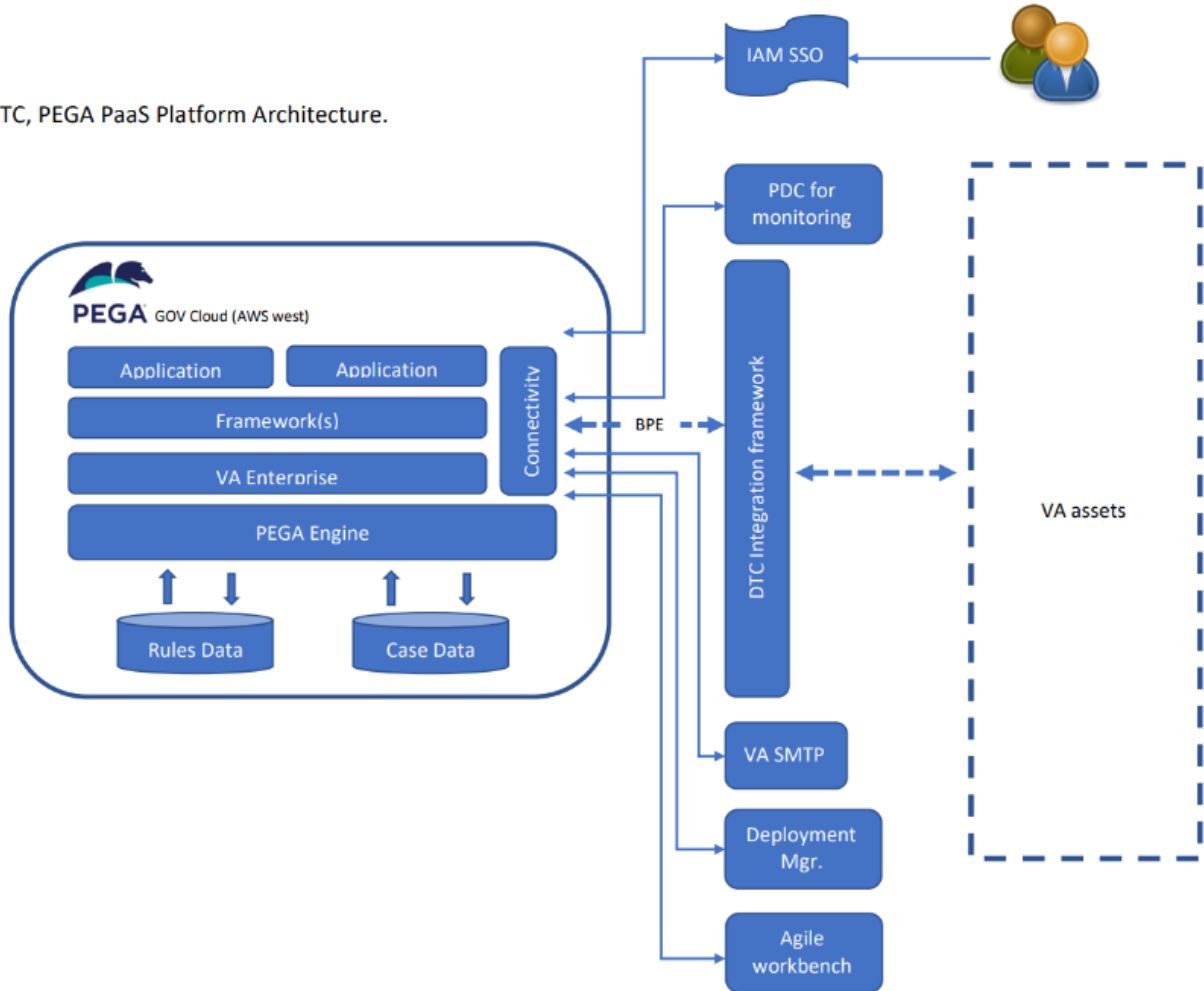
All Pega environments within the VA, including the development sandbox are managed by the DTC Pega COE Team.

Any enterprise level components, features, functionality required by SI/CD will follow DTC's standard sprint cycle. Enterprise reusability falls to the DTC team; prioritization and Service Level Agreements (SLA's) are determined based team bandwidth.

Environment Types

Environment Type	Purpose	Sandbox Type	Deployment Responsibility
Development	Available to SI/CD for development work	Developer Sandbox	DTC
Testing	Available for SI/CD to complete system and regression testing	NA	DTC
Staging	Available for SI/CD/Business team to complete UAT	NA	DTC
Production	Live environment	NA	DTC
Platform Support Environments (Agile Studio, Diagnostic Cloud, Release Manager)	Contain platform support toolkits that are used to support the first four environments	Used by DTC	N/A
Agile Studio	Available to SI/CD to manage sprints and agile processes	NA	DTC

DTC, PEGA PaaS Platform Architecture.



Architecture Diagram

508 Compliance

TASK	RESPONSIBLE PARTY	Timeline
Develop application using 508 guidelines and best practices	SI Team	Ongoing
Submit Request for Initial 508 Audit: Request 508 Audit Ticket	Business Owner/ SI Team	At Beginning of development
Schedule Initial 508 Audit	Business Owner/ SI Team	8 weeks prior to release to production
Conduct Audit	VA 508 Team	

Create a remediation plan using provided 508 remediation plan template and submit to Pega COE for review and approval (Template found in the additional resources tab at the top of this page)	SI Team	Within 2 weeks of audit return
Make 508 remediation's & perform a final self-accessed audit according to the WCAG 2.0	SI Team	Low & Medium remediation findings 4 months. Critical findings 1 month
Provide bi-weekly updates on remediation progress to Pega COE 508 POC	SI Team	
Submit for Re-Audit	Pega COE	6 months
Notify the Pega COE point of contact (Stuart Reece), through email or office hours, about the implementation of large-scale design changes that will impact previously released UI and update remediation plans accordingly to ensure continued compliance throughout the development life cycle. *Re-audit required for any subsequent large-scale releases.	SI Team	Ongoing

Additional support can be provided to SI/CD's through the established COE office hours. Conversely, additional meetings can be set as often as a per sprint basis as more workflows are created containing UI elements. If not already set, meetings should be established with the COE point of contact on SI/CD sprint basis to review efforts towards remediation.

For a full overview of 508 compliance, please see the additional resources tab at the top of this page.

Development Support

Once a request has received gateway review (step 7 in the DTC intake process), access to the development environment is provided. While the system integrator or citizen developer is working through development and testing of their solution, the DTC Pega COE team will be readily available for guidance and support to include design, architectural review and release management. The DTC team will also Conduct quality audits on the design, architecture, and code periodically. The DTC will provide additional support for the CDs in training, application design and implementations including assistance with integrations and complex process flows and activities. The DTC Pega COE team offers weekly office hours for drop-in support and Q&A.

For system integrators or citizen developers who desire additional training about the Pega platform, Pega offers online self-paced courses at: [Pega Academy Home](#) | [Pega Academy](#).

Level Up

What is Level Up?

Level-Up is the DTC's quality gates initiative. It improves established VA processes and supports a community of accountability across all contributors through measurable improvements. The 3 focus areas are:

Code Quality and Release Readiness

Verifies code released in production is reliable, bug-free, and performant.

Unit Test Coverage, Quality & Performance

Ensures individual components are tested, improving the longevity and quality of the codebase.

Secure Development

Ensures platforms are safe and secure, reducing security breaches/attacks.



Level Up Metrics

Secure Development

Secure Development

Total Score:

Measure	Description	Value		
		Exceeds	Meets	Does Not Meet
Engagement & Collaboration	Engages and is available for intake process, defined requirements, defined data elements, provides level of effort and project schedule	Fully engaged, proactively provides requirements to SIIT team, follows SIIT process, engages in process requirements VALUE 10	Fully engaged, proactively provides requirements to SIIT team, follows SIIT process, all with internal requirements VALUE 5	Not engaged and/or missing requirements, analysis VALUE 0
508 Audit	508 Commercial Off the Shelf (COTS) audit was completed and defects identified were submitted for support	Audit performed and NO high findings were discovered at time of presentation VALUE 5	Audit performed and all findings identified were remediated VALUE 5	No audit was not performed, or findings identified were not input to support VALUE 0

Secure Development

Secure Development			Total Score:	
Measure	Description	Value		
		Exceeds	Meets	Does Not Meet
Engagement & Collaboration	Engages and is available for intake process, defined requirements, defined data elements, provides level of effort and project schedule	Fully engaged proactively provides requirements to SOC team, follows SOC process, engages in process requirements VALUE 35	Fully engaged proactively provides requirements to SOC team, follows SOC process, all with retained requirements VALUE 30	Not engaged and/or missing requirements, available VALUE 25
508 Audit	508 Commercial Off the Shelf (COTS) audit was completed and defects identified were submitted to support	Audit performed and NO high findings were discovered from production VALUE 9	Audit performed and all high findings were not retained VALUE 8	No audit was not performed, or defects identified were not input to support VALUE 0

Code and Quality Release

Code and Quality Release

Total Score: _____

Measure	Description	Value		
		Exceeds	Meets	Does Not Meet
Guardrail score	Scoring tool called Guardrail Platform that guides implementation to successful application	100% Guardrail Score Value 1	Minimum of 95% score Value 3	Less than 95% Guardrail score Value 0
Defects Identified at Release	Number of defects identified in the IBM iSourceCheck with impact of 'Fail'	No defects identified Value 1	1-2 Issues identified (not 20% of Identified) Value 3	1 or more moderate/high impact defects 3 or more identified issues 3 or more critical issues 3 or more critical defects Value 0
End User Acceptance Received	Confirmation of end user acceptance was received within 3 month of release date	Status reflects "Implemented & Approved in Prod"	Status reflects "Implemented & Approved in Prod" but not user acceptance Value 1	Status reflects anything other than "Implemented & Approved in Prod" Value 0
Release Readiness	Results of system/integration testing provided, user stories provided, evidence of UAT testing provided, deployment & transition plan provided	S/PROVIDED: Results of system/integration testing, user stories, evidence of UAT testing, an archive with no redundancy, engages in process improvement Value 1	S/PROVIDED: Results of system/integration testing, user stories, evidence of UAT testing, an archive with no redundancy Value 3	Missing one or more required documents, provided incomplete documents OR documentation was lacking/misread multiple times Value 0
Application Playbook	Provides overview of application and follows OTC provided template	S/PROVIDED: Application playbooks align with the template and included additional content around solution dimensions Value 10	S/PROVIDED: Application playbooks align with the template and met/reexceeds standards Value 5	Application playbooks provided but missing one or more required elements or provided less than 50% Value 0

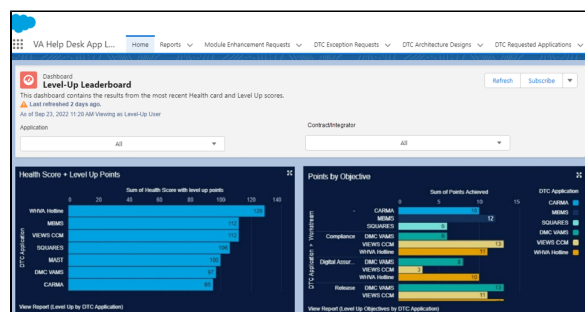
How to Level Up?

1. Refer to DTC COE SOPs for guidance on DTC required timelines, processes and minimum requirements: [DTC PEGA Confluence](#)
2. Refer to DTC COE Level Up Standards for requirements on leveling up
3. Continue delivering exceptional solutions to VA

Scores are determined and reported when an application deploys a new release, releases a new enhancement or comes back into sustainment.

Level Up Leaderboard!

Coming soon! Teams can check their progress on the home tab of the VA Help Desk application. Below is a sample of what to expect. Check back soon for updates on Pega's leaderboard!



Revision History

Revision Date	Changed By	Notes
05 Dec 2023	Jen Wisniewski	Page created.