



(<http://www.va.gov>)

MENU

VA Technical Reference Model v 21.2

KWedge for Android

General **Decision** Reference Component Category Analysis

Vendor Release

Information (<https://www.oit.va.gov/Services/TRM/ForecastHelpPage.aspx#ReleaseInfo>)

The Vendor Release table provides the known releases for the TRM Technology, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.x	01/31/2020		

Current

Decision

Matrix (<https://www.oit.va.gov/Services/TRM/ForecastHelpPage.aspx#ForecastInfo>)
(10/26/2020)

Users must ensure their use of this technology/standard is consistent with VA policies and standards, including, but not limited to, VA Handbooks 6102 and 6500; VA Directives 6004, 6513, and 6517; and National Institute of Standards and Technology (NIST) standards, including Federal Information Processing Standards (FIPS). Users must ensure sensitive data is properly protected in compliance with all VA regulations. Prior to use of this technology, users should check with their supervisor, Information Security Officer (ISO), Facility Chief Information Officer (CIO), or local Office of Information and Technology (OI&T) representative to ensure that all actions are consistent with current VA policies and procedures prior to implementation.

The VA Decision Matrix displays the current and future VA IT position regarding different releases of a TRM entry. These decisions are based upon the best information available as of the most current date. The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and/or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Decision Matrix is considered unapproved for use.

Legend:

White	Approved: The technology/standard has been approved for use.
Yellow	Approved w/Constraints: The technology/standard can be used within the specified constraints located below the decision matrix in the footnote[1] and on the General tab.
Gray	Unapproved: This technology or standard can be used only if a waiver, signed by the Associate Deputy Assistant Secretary (ADAS), Enterprise Program Management Office (EPMO) or designee and based upon a recommendation from the STAT Working Group, has been granted to the project team or organization that wishes to use the technology.
Orange	Divest: VA has decided to divest itself on the use of the technology/standard. As a result, all projects currently utilizing the technology/standard must plan to eliminate their use of the technology/standard. Additional information on when the entry is projected to become unapproved may be found on the Decision tab for the specific entry.
Black	Prohibited: The technology/standard is not (currently) permitted to be used under any circumstances.
Blue	Planning/Evaluation Constraint: The period of time this technology is currently being evaluated, reviewed, and tested in controlled environments. Use of this technology is strictly controlled and not available for use within the general population. If a customer would like to use this technology, please work with your local or Regional OI&T office and contact the appropriate evaluation office displayed in the notes below the decision matrix. The Local or Regional OI&T office should submit an inquiry to the TRM (https://www.oit.va.gov/Services/TRM/TRMInquiryForm.aspx) if they require further assistance or if the evaluating office is not listed in the notes below.

Release/Version Information:

VA decisions for specific versions may include a ‘.x’ wildcard, which denotes a decision that pertains to a range of multiple versions.


For example, a technology approved with a decision for 7.x would cover any version of 7.(Anything) - 7.(Anything). However, a 7.4.x decision would cover any version of 7.4.(Anything), but would not cover any version of 7.5.x or 7.6.x on the TRM.

ToolPage.aspx?tid=14915&tab=2&minYear=2020	CY2021				CY2022		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3
7.x	Approved w/Constraints [2, 3, 4]	Approved w/Constraints [2, 3, 4]	Approved w/Constraints [2, 3, 4]	Approved w/Constraints [2, 3, 4]	Approved w/Constraints [2, 3, 4]	Approved w/Constraints [2, 3, 4]	Approved w/Constraints [2, 3, 4]

Decision Constraints

[1] Per the Initial Product Review, users must abide by the following constraints:

- To be used within VA, the underlying operating system, full disk encryption, or other third-party Fe (FIPS) 140-2 validated applications must be leveraged to protect VA sensitive information.

<Past (ToolPage.aspx?tid=14915&tab=2&minYear=2020)	<p>[2] Veterans Affairs (VA) users must ensure VA sensitive data is properly protected in compliance with all deployment using this technology should be reviewed by the local ISO (Information Security Officer) 6500 (https://www1.va.gov/Vapubs/viewPublication.asp?Pub_ID=793&FTtype=2).</p>	<p>CY2021</p>					
<p>Release</p>	<p>Q1</p>	<p>Q2</p>	<p>Q3</p>	<p>Q4</p>	<p>Q1</p>	<p>Q2</p>	<p>Q3</p>
<p>[3] Technology must remain patched and operated in accordance with Federal and Department security mitigate known and future security vulnerabilities.</p>							
<p>[4] This technology requires using a Universal Service Bus (USB) technology to transfer data into the re to be taken to protect data.</p>							
<p>Per the Initial Product Review, users must abide by the following constraints:</p> <ul style="list-style-type: none"> To be used within VA, the underlying operating system, full disk encryption, or other third-party Fe (FIPS) 140-2 validated applications must be leveraged to protect VA sensitive information. 							
<p>Note:</p>	<p>At the time of writing, version 7.3 is the most current version released.</p>						
							

- The information contained on this page is accurate as of the Decision Date (10/28/2020).

CONNECT

VA HOME

QUICK LIST

RESOURCES

ADMINISTRATION

U.S. Department of Veterans Affairs | 810 Vermont Avenue, NW
Washington DC 20420

Last updated validated on Wednesday, February 3, 2021