Category		Description	Note	Level 1	Level 2	Level 3	Level 4	NIST SP 800-53 Assessment Methods		
Type of Testing		This is level of testing Technical or Non-Technical?		*Non-Technical*	*Technical*					
Title		Short description of this level of testing rigor.		**Assertion Appropriateness**	**Passive Compliance Verification**	**Basic Compliance Verification**	**Advanced Compliance Verification**	**Examine**	**Interview**	**Test**
Typical Use		This level of testing rigor will usually be used for…		*Status Check of Trusted System*	*Initial Form of Ongoing Authorization*	*Tailored-Scope ACT*	*Comprehensive ACT*			
Questions Answered		Does the documentation and configuration indicate a system that ***is likely*** to be acceptably compliant with security requirements? (Examine)		✓	✓	✓	✓	✓		
		Do **pre-existing** testing results and personnel interviews indicate a system that ***is likely*** to be acceptably compliant with security requirements? (Examine, Interview)			✓	✓	✓	✓	✓	
		Does **new** testing confirm the system ***is*** acceptably compliant with a ***sample*** of security requirements? (Test)				✓	✓			✓
		Does **new** testing confirm the system ***is*** acceptably compliant with ***all*** security requirements? (Test)					✓			✓
Goals Achieved		Determine if **assertions** made in documentation and passive data collection are compliant and appropriate. (Examine)		✓	✓	✓	✓	✓		
		Determine if **pre-existing** test results demonstrate that the system adequately complies with security requirements. (Examine)			✓	✓	✓	✓		
		Determine if **personnel** adequately understand the system, the security requirements, and their duties. (Interview)			✓	✓	✓		✓	
		Determine if **assertions** in documentation, **interviews**, and available **pre-existing** system test results are consistent with each other. (Examine, Interview)			✓	✓	✓	✓	✓	
		Determine if **known exploits** (CVEs, 0-days, etc.) are adequately addressed by the system documentation, personnel, and implementation. (Test)				✓	✓			✓
		Determine if the **Core** Controls are adequately implemented by the system. (Test)				✓	✓			✓
		Determine if a **random sample** of the **non-Core** Controls are adequately implemented by the system. (Test)				✓				✓
		Determine if **all non-Core** Controls are adequately implemented by the system. (Test)					✓			✓
Assertions Verified		*Assertion verification summary:*		*Assertions Not Verified*	*Assertions Verified Against **Existing** Test Results*	*Assertions Verified Against **New** Test of **Sample** of Controls*	*Assertions Verified Against New Test of **All** Controls*			
		Interviews			✓	✓	✓		✓	
		Existing Test Results	*NetSparker, Penetration Test, and Previous ACT Security Assessment (see "Tools Used" below).*		✓	✓	✓	✓		
		Known Exploits	*CVEs, 0-days, etc. for components and technologies known to compose the system.*			✓	✓			✓
		Core Controls				✓	✓			✓
		Non-Core Controls				sample	all			✓
Tools Used	Documentation	System Security Plan (SSP), Contingency Plan (CP), Information System Risk Assessment (ISRA), *etc.*		✓	✓	✓	✓	✓		
	Configuration Data	<Tool, *e.g.* InSpec>	*Not considered to be "tests" since they simply collect configuration and status data from the system, which is effectively a collection of assertions that must be verified through testing.*	✓	✓	✓	✓	✓		
		<Tool, *e.g.* DbProtect>		✓	✓	✓	✓	✓		
		<Tool, *e.g.* Nessus>		✓	✓	✓	✓	✓		
		Running Configurations (System)		✓	✓	✓	✓	✓		
	Interviews	Interviews of ISSM, ISSO, App Developers, DB Admins, Network Admins, OS Admins, Mainframe Admin, *etc.*			✓	✓	✓		✓	
	Implementation Data	<Tool, *e.g.* NetSparker>	*Considered to be "tests" since they report actual testing that was performedwithin a reasonable timeframe from this asssessment.*		✓	✓	✓			✓
		Penetration Test			✓	✓	✓			✓
		Previous ACT Security Assessment (Existing Data)			✓	✓	✓	✓		✓
		Vulnerability Assessment Tools (**This Assessment**)	*Vulnerability Assessment performed by the Assessment Team on this assessment.*			✓	✓			✓
System Access Needed		Type of access to the system required to complete testing.		none	none	full	full			
Assessor Role Level of Effort Estimate (vs. "today's ideal assessment")		M&O		0.7	0.8	1.0	1.0			
		Privacy		0.6	0.6	1.0	1.0			
		Application		0.0	0.1	0.6	1.0			
		Database		0.6	0.6	0.8	1.0			
		Operating System		0.6	0.6	0.8	1.0			
		Network		0.6	0.6	0.8	1.0			
		Mainframe		0.6	0.6	0.8	1.0			
How Automatable Is This? (Rough Estimates)	Compliance Checks	Technical		fully (minimal effort)	fully (moderate effort)	partial (significant effort)	partial (significant effort)			
		M&O		fully (significant effort)	fully (significant effort)	fully (significant effort)	fully (significant effort)			
	Appropriateness Checks	Technical		partial (significant effort)	partial (significant effort)	partial (significant effort)	partial (significant effort)			
		M&O		partial (significant effort)	partial (significant effort)	partial (significant effort)	partial (significant effort)			