

Section	FedRAMP Artifact	Reference	Notes	LOE	Priority	Plus Static Content	Plus Static Example	Plus Static Instructions	
	General (Applies to two or more artifacts)		Create once. Use for all documents.						Primary Goal: Build modular so others, less knowledgeable in XSLT, can tweak and maintain. Secondary Goal: Get as far as we can with Wendell's help, such that the remaining work is easier to perform when he is no longer supporting FedRAMP.
	FedRAMP Stylesheet		Mine needs updating with new branding, plus tweaks.	Moderate	1			n/a	
	General static content capability			Moderate	1			n/a	
	General Hidden Instructions Capability			Moderate	1			n/a	
	General Content Presentation		Display of parts, static content, static examples, instructions	Moderate	1	Y	Y	Y	
	Title Page		Need new branding.	Low	3			Y	LOE - Low: Same assembly or simple variation of another transform.
	Prepared By/For			Low	3				LOE - Moderate: Different assemblies or more nuanced details.
	Document Revision History			Low	3				LOE - High: Large, very complex, or multiple files (via import) involved.
	How to contact us			Low	3	Y		Y	
	Content Approvals			Low	3				Priority 1: Foundational. Basis for most other transforms.
	Table of Contents		These are more meaningful later, when they can both summarize and provide links to other content	Moderate	4				Priority 2: Highly complex. Maybe impossible without Wendell's help.
	Table of Figures			Moderate	4				Priority 3: Other important or moderately complex Transforms.
	Table of Tables			Moderate	4				Priority 4: Less critical or easy to do ourselves later.
	Various POCs		Same general construct with ability to specify role and get results	Moderate	1				* We at least want Wendell's help for Priority 1 and 2.
	Applicable Laws/Regulations, Standards/Guidance		Same construct with filters for L&R, S&G, w and w/o PII Refs	Low	1	Y		Y	
	List of attachments		Ability to filter (ie - just policies and procedures)	Moderate	1	Y			
	System Security Plan (SSP)								Static content may include introductory text or other explanations that appear before (and sometimes after) the dynamic content. There should be an option as to whether the static content appears with the dynamic content or not. Placeholders are OK. We can fill in the actual static content later.
1	Information System Name and Title	Table 1-1		Low	3	Y			
2	Information System Categorization	Table 2-1		Low	3	Y			
2.1	Information Types	Table 2-2	Work with Table 15-9	Moderate	3	Y	Y	Y	
2.2	Security Impact Level	Table 2-3		Low	4	Y			
2.2	Baseline Security Configuration	Table 2-4		Low	3	Y			Static Examples are a special form of static content that would typically be shown, but could somehow be hidden. I'd like to have one mechanism for this, used everywhere, and have the option to include or exclude it with the other to static content. (hiding static content would hide this, but showing static content would allow this content to be hidden or shown within that static content). Would typically be presented the same as the dynamic content. Placeholder detail is OK.
2.3	Digital Identity Level		Should be worked with Att 3	Low	3	Y			
3	Information System Owner	Table 3-1	Uses POC Transform above	Low		Y			
4	Authorizing Officials		Uses POC Transform above	Low		Y		Y	
5	Other Designated Contacts	Tables 5-1, 2	Uses POC Transform above	Low		Y		Y	
6	Assignment of Security Responsibility	Tables 6-1, 2	Uses POC Transform above	Low		Y			
7	System Status	Table 7-1		Low	4	Y		Y	
8.1	Service Layers Represented	Table 8-1		Low	3	Y		Y	Static Instructions are a special form of static content that would typically be hidden, but could somehow be exposed. I'd like to have one mechanism for this, which is used everywhere, and have the option to include or exclude it similar to (but separate from) static content.
8.2	Cloud Deployment Model	Table 8-2		Low	3	Y		Y	
8.3	Leveraged Authorizations	Table 8-3		Low	3	Y		Y	
9.1	System Function or Purpose		Use General Content Presentation Above			Y		Y	
	System Locations			Low	3				
9.2, 9.4, 10.1	Diagrams (Authorization, Network, Data Flow)	Figure 9-1		Moderate	2	Y		Y	Each transform should have a title, with an option to include or exclude it.
9.3	Personnel Roles and Privileges	Table 9-1	Includes fill-in content at bottom (# of intern/external, etc.)	Moderate	2	Y	Y	Y	
10.2	Ports, Protocols and Services	Table 10-1	Work with Att 13: System Inventory (filter/variant)	Moderate	3	Y		Y	
11	System Interconnections	Table 11-1		Low		Y		Y	
13	Control Definition Display	Work together	From profile/catalog (sub-controls formatted differently)	Moderate	2				Work together, but keep Control Definition separate from Control Summary and Control Implementation Statement, so that it can also be displayed alone.
13	Control Summary Information			Low	2				
13	Control Implementation Statement		Need to handle -1's differently	Moderate	2				
Att 1	Policies and Procedures		Use Lost of attachments above.						
Att 2	User Guide		Use Lost of attachments above.						
Att 3	Digital Identity Level	Table 15-5	Work with 2.3 Digital Identity level above.	Low	3	Y		Y	
Att 4	Privacy POC	Table 15-6	Uses POC Transform above			Y		Y	
Att 4	Applicable privacy laws and regs	Table 15-7, 8	Use Laws/Regs, Standards/Guidance Transform above			Y			
Att 4	Qualifying Questions			Low	4	Y			
Att 4	Designation			Low	4				

Section	FedRAMP Artifact	Reference	Notes	LOE	Priority	Plus Static Content	Plus Static Example	Plus Static Instructions	
Att 5 - 8	Rules of Behavior (ROB), Plans		Use/Filter List of attachments above						
Att 9	CIS Workbook		Already drafted. Needs update to MS3. Work with Ch 13	Moderate	2				
Att 10	Information Types	Table 15-9	Work with Table 2-2	Low	3	Y		Y	
Att 11	Sep of Duties Matrix		No clear format. Consider generating.?	Moderate	4				
Att 12	Laws and Regs		Use Laws and Regs above						
Att 13	System Inventory	Spreadsheet	Work with SAP: Components Slated for Testing	Moderate	1				
	Security Assessment Plan (SAP)								
2	Scope		Controls to be assessed	Moderate	2	Y			
2.1	System Information		[SSP] System Name and Title			Y		Y	
2.1	Location of Components		[SSP] System Locations and SAP Locally Defined	High		Y			
2.2	IP Addresses Slated for Testing	Table 2-3	New views of SSP Inventory Data (SSP: Att 13) - Work together	Moderate	2	Y		Y	
2.3	Web Apps Slated for Testing	Table 2-4		Low	2	Y		Y	
2.4	Databases Slated for Testing	Table 2-5		Low	2	Y		Y	
2.5	Roles slated for Testing	Table 2-6		Moderate	2	Y			
3	Assumptions		Use Generate Content Presentation above	Low		Y		Y	
4	Methodology		Use Generate Content Presentation above	Low		Y		Y	
5.1	Security Assessment Team	Table 5-1	Use POC Transform above			Y		Y	
5.2	CSP Testing POCs	Table 5-2	Use POC Transform above			Y		Y	
5.3	Test Tools	Table 5-3		Moderate	2	Y		Y	
5.4	Manual Testing	Table 5-4		Low	4			Y	
5.5	Schedule	Table 5-5		Low	3	Y		Y	
6	Rules of Engagement		Use Generate Content Presentation above	Low	3	Y		Y	
6.1	Disclosures		Use Generate Content Presentation above (plus IP addr)	Low	3	Y		Y	
6.2	Testing May Include		Use Generate Content Presentation above	Low	4	Y		Y	
6.3	Testing Will Not Include		Use Generate Content Presentation above	Low	4	Y		Y	
6.4	End of Testing		Use POC Transform above	Low	4				
6.5	Comm of Test Results	Table 6-1	Use POC Transform above	Low	4	Y			
6.6	Limitation of Liability		Use Generate Content Presentation above	Low	4	Y		Y	
6.7	Signatures		Use Content Approvers above	Low	3	Y			
App A	Acronyms		Not now						
App B	Test Case Procedure Workbook			High	2				
App C	Attachments		Use attachments above		4			Y	
App D	Pen Test Plan/Methodology		Use attachments above		4			Y	
	Security Assessment Report (SAR)								
	Assessment Summary (ExSum)		Will include elements below	High	2	Y			
1	Introduction		Use Generate Content Presentation above	Low	4				
1.3	Purpose		Use Generate Content Presentation above	Low	4				
1.4	Inclusion of Previous Assessment Results		This requires some discussion	Low	3	Y			
1.5	Scope	Table 1-1	Use SAP Transform, SAR Data						
1.5	System Information	Table 1-2	Use SSP Transform and data						
1.5	List of documents used		Use attachments filter above						
1.5	Site Names Locations	Table 1-3	[SSP and SAP] System Locations and SAR Locally Defined	High	2				
2.1	System Categorization		Similar to SSP						
2.2	System Description		From SSP (or locally defined)	Moderate	2				
2.3	Purpose of System		From SSP (or locally defined)	Moderate	2				
3	Assessment Methodology		Use SAP Transform on SAR data	Low	3				

Section	FedRAMP Artifact	Reference	Notes	LOE	Priority	Plus Static Content	Plus Static Example	Plus Static Instructions	
3.1	Perform Tests		Use Generate Content above	Low	4				
3.2	Assessment Deviatons	Table 3-1		High	2				
3.3	Identif of Vulns		Use Generate Content above	Low	4	Y			
3.4	Consideration of Threats		Use Generate Content above	Low	4	Y			
3.4	Threat Table	Table 3-3	Generate from FedRAMP Data	Low	3			Y	
3.5	Perform Analysis		Use Generate Content above	Low	4	Y			
3.6	Documented Results		Use Generate Content above	Low	4	Y			
4	Security Assessment Results		Use Generate Content above	Low	4	Y			
4.1	Security Assessment Summary: Risk Exposure Table (RET)	Table 4-1	Work with TCW below	High	2				
5	Non-Conforming Controls			Low	4	Y			
5.1	Risks Corrected During Testing	Table 5-1	Work with RET above (filter) / variant	Low	2	Y			
5.2	Risks with Mitigating Factors	Table 5-2	Work with RET above (filter) / variant	Low	3	Y			
5.3	Risks with Operational Requirements	Table 5-3	Work with RET above (filter) / variant	Low	3	Y			
6	Risks for Interconnecte Systems	Table 6-1	Work with RET above (filter) / variant	Low	3	Y			
7	Continued Authorization Recommendation		Use Generate Content above	Low	4	Y			
7	Risk Priorities	Table 7-1	Work with RET above (filter/sort) / variant	Low	3	Y			
App A	Acronyms		Not now						
App B	Security Test Case Procedures (TCW)		Work with RET above (filter) / variant	High	2				
App C	Scan Results: Inventory (Infrastructurte)	Table C-1	Use SAP Inventory above	Low	2	Y		Y	
App C	Scan Results: Raw (Infrastructurte)		Use Attachments above (filter)	Low	2	Y		Y	
App C	Scan Results: False Positive (Infrastructurte)	Table C-2		Moderate	4				
App D	Scan Results: Inventory (database)	Table D-1	Use App C above (filter)	Low	4	Y		Y	
App D	Scan Results: Raw (database)		Use App C above (filter)	Low	4	Y		Y	
App D	Scan Results: False Positive (database)	Table D-2	Use App C above (filter)	Low	4				
App E	Scan Results: Inventory (web app)	Table E-1	Use App C above (filter)	Low	4	Y		Y	
App E	Scan Results: Raw (web app)		Use App C above (filter)	Low	4	Y		Y	
App E	Scan Results: False Positive (web app)	Table E-2	Use App C above (filter)	Low	4				
App F	Assessment Results	Table F-1	Work with RET above (filter) / variant	Low	2				
App F	Assessment ResultsFinal Summary of Risks	Table F-2	Work with RET above (filter) / variant (also used in ExSum)	Low	2				
App F	Open POA&Ms	Table F-3	(Need to pull from POA&M)	Moderate	2	Y			
App F	POA&M Summary	Table F-4	(Need to pull from POA&M)	Moderate	2	Y			
App F	Summary of Vulns to be carried forward	Table F-5	(Need to pull from POA&M)	High	2	Y			
App F	Summary of Unauthenticated Scans	Table F-6	Use App C above (filter)	Low	4	Y			
App F	Other Tools Used		Use SAP List of Tools but SAR data	Low	4				
App F	Scan Results: Inventory (other)	Table F-7	Use App C above (filter)	Low	4	Y		Y	
App F	Scan Results: Raw (web app)		Use App C above (filter)	Low	4	Y		Y	
App F	Scan Results: False Positive (web app)	Table F-8	Use App C above (filter)	Low	4				
App F	Scan Results: Inventory (unauthenticated)	Table F-9	Use App C above (filter)	Low	4	Y		Y	
App F	Scan Results: Raw (unauthenticated)		Use App C above (filter)	Low	4	Y		Y	
App F	Scan Results: False Positive (unauthenticated)	Table F-10	Use App C above (filter)	Low	4				
App G	Manual Test Report	Table G-1	SAR data (blands SAP manual test list and SAR TCW)	Moderate	2				
App H	Aux Documents		Use Attachment List and filter	Low	4	Y			
App I	Penetration Test Report		Use Attachment List and filter	Low	4	Y			
App I	In-Scope Systems	Table I-1	TBD	Low	4	Y			