



Summary of Changes from SSP Template v2.1 to SSP Template v3.0 Moderate Impact

The table below summarizes the 15 additions or changes from SSP Version 2.1 (published 06/06/2014) to SSP Version 3.0 (published 06/20/2016). If the entry in the SSP Version 2.1 is blank, that means the language in the corresponding SSP V3.0 cell is new. Any questions on this list of changes should be sent to info@fedramp.gov. SSP version 2.0

Control ID	SSP Version 2.1 Control Description From	SSP Version 3.0 Control Description To
AC-2 (5) Control Enhancement		Added Guidance AC-2 (5) Additional FedRAMP Requirements and Guidance: Guidance: Should use a shorter timeframe than AC-12
AC-5 Separation of Duties	AC-5 Additional FedRAMP Requirements and Guidance: Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP.	AC-5 Additional FedRAMP Requirements and Guidance: Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP. Attachment 11 - Separation of Duties Matrix. Directions for attaching the Separation of Duties Matrix document may be found in the following section: 15.11 ATTACHMENT 11 - Separation of Duties Matrix.
AC-17 (9) Control Enhancement	AC-17 (9) [no greater than 15 minutes]	AC-17 (9) [15 minutes]
AU-3 (1) Control Enhancement	AU-3 (1) The information system generates audit records containing the following additional information: [FedRAMP Assignment: [session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon]]. Requirement: The service provider defines audit record types. The audit record types are approved and accepted by the JAB. Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.	AU-3 (1) The information system generates audit records containing the following additional information: [FedRAMP Assignment: organization-defined additional, more detailed information]. Requirement: [FedRAMP Assignment: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon]. The audit record types are approved and accepted by the JAB. Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.
AU-5 Response to Audit Processing Failures	AU-5 (b) Takes the following additional actions: [FedRAMP Assignment: low-impact: overwrite oldest audit records; moderate-impact: shut down].	AU-5 (b) Takes the following additional actions: [FedRAMP Assignment: organization-defined actions to be taken; (overwrite oldest record)].
AU-6 Audit Review, Analysis, and Reporting		AU-6 Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.
CA-2 (3) Control Enhancement	The organization accepts the results of an assessment of [Assignment: organization-defined information system] performed by [FedRAMP Assignment: any 3PAO] when the assessment meets [FedRAMP Assignment: the conditions of a P-ATO in the FedRAMP Secure Repository].	CA-2 (3) The organization accepts the results of an assessment of [FedRAMP Assignment: any FedRAMP Accredited 3PAO] performed by [FedRAMP Assignment: any FedRAMP Accredited 3PAO] when the assessment meets [FedRAMP Assignment: the conditions of the JAB/AO in the FedRAMP Repository].
CA-7 Continuous Monitoring		CA-07 Requirement: Operating System Scans: at least monthly Database and Web Application Scans: at least monthly All scans performed by Independent Assessor: at least annually.
CM-2 (1) Control Enhancement	The organization reviews and updates the baseline configuration of the information system: (a) [FedRAMP Assignment: Annually]; (b) When required due to [FedRAMP Assignment: when directed by the JAB]; and (c) As an integral part of information system component installations and upgrades.	The organization reviews and updates the baseline configuration of the information system: (a) [FedRAMP Assignment: at least annually]; (b) When required due to [FedRAMP Assignment: to include when directed by the JAB]; and (c) As an integral part of information system component installations and upgrades.
IA-2 (11) Control Enhancement	IA-2(11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].	IA-2(11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [FedRAMP Assignment: FIPS 140-2, NIAP Certification, or NSA approval]. Additional FedRAMP Requirements and Guidance: Guidance: PIV = separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials. FIPS 140-2 means validated by the Cryptographic Module Validation Program (CMVP).



Summary of Changes from SSP Template v2.1 to SSP Template v3.0 Moderate Impact

Control ID	SSP Version 2.1 Control Description From	SSP Version 3.0 Control Description To
MP-3 Media Labeling	<p>The organization:</p> <p>(a) Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and</p> <p>(b) Exempts [FedRAMP Assignment: no removable media types] from marking as long as the media remain within [Assignment: organization-defined controlled areas FedRAMP Assignment: parameter not applicable]</p> <p>MP-3(b) Additional FedRAMP Requirements and Guidance: Guidance: Second parameter in MP-3(b) is not applicable.</p>	<p>The organization:</p> <p>(a) Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and</p> <p>(b) Exempts [FedRAMP Assignment: no removable media types] from marking as long as the media remain within [Assignment: organization-defined controlled areas].</p> <p>MP-3(b) Additional FedRAMP Requirements and Guidance: Guidance: Second parameter in MP-3(b)-2 is not applicable.</p>
PL-8 Information Security Architecture	(b) [at least annually]	(b) [At least annually or when a significant change occurs] Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, page F-7.
SA-9 (1) Control Enhancement	<p>The organization:</p> <p>(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and</p> <p>(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [FedRAMP Assignment: see Additional Requirement and Guidance].</p> <p>SA-9 (1) Additional FedRAMP Requirements and Guidance: Requirement: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. For JAB authorizations, future planned outsourced services are approved and accepted by the JAB.</p>	<p>The organization:</p> <p>(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and</p> <p>(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].</p>
SC-15 Collaborative Computing Devices	<p>The information system:</p> <p>(a) Prohibits remote activation of collaborative computing devices with the following exceptions:[FedRAMP Assignment: no exceptions] and</p> <p>(b) Provides an explicit indication of use to users physically present at the devices.</p>	<p>The information system:</p> <p>(a) Prohibits remote activation of collaborative computing devices with the following exceptions:[FedRAMP Assignment: no exceptions] and</p> <p>(b) Provides an explicit indication of use to users physically present at the devices.</p> <p>SC-15 Additional FedRAMP Requirements and Guidance: Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.</p>
SI-4 (4) Control Enhancement	The information system monitors inbound and outbound communications traffic [FedRAMP Assignment: continually] for unusual or unauthorized activities or conditions.	The information system monitors inbound and outbound communications traffic [FedRAMP Assignment: continuously] for unusual or unauthorized activities or conditions.