CMS Information Security (IS) System Compliance & Reference Chart

Artifact / Activity	Req't Citation	Req'd for	Compliance Frequency	References & Supporting Documentation
Certification & Accreditation (C&A)[1]	FISMA[2]		Every 3 years[3]	http://cms.hhs.gov/InformationSecurity/Downloads/ca_procedure.pdf
System Security Plan (SSP)	FISMA	C&A	Every 3 years[3]	http://cms.hhs.gov/InformationSecurity/Downloads/ssp_procedure.pdf
IS Risk Assessment (RA)	FISMA	SSP	Every 3 years[3]	http://www.cms.hhs.gov/informationsecurity/downloads/IS_RA_Procedure.pdf
Contingency Plan (CP)	FISMA	C&A	As needed	http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
Contingency Plan (CP) Testing	FISMA	C&A	Every 365 days	http://cms.hhs.gov/InformationSecurity/Downloads/CP_Tabletop_Test_template.zip
Privacy Impact Assessment (PIA)	FISMA	C&A	Annually by June 1st	http://intranet.hhs.gov./infosec/docs/policies_guides/PIA/PIA_Guide.pdf
Security Test & Evaluation (ST&E)	FISMA	C&A	Every 3 years[3]	http://cms.hhs.gov/InformationSecurity/Downloads/Assessment_Procedure.pdf
Security Controls Testing	FISMA	C&A	A sub-set every 365 days	http://csrc.nist.gov/publications/drafts/SP800-53A-spd.pdf
Plan of Actions & Milestones (POA&M)	FISMA	C&A	Nov 1, Feb 1, May 1 & Aug 1	http://cms.hhs.gov/informationsecurity/Downloads/poam_guidelines.pdf
Corrective Action Plans (CAP)	FISMA	POA&M	1st of every month	http://cms.hhs.gov/informationsecurity/Downloads/poam_guidelines.pdf
Security Costs Budgeting	Clinger-Cohen Act[4]	Exhibit 300	Annually (generally in February)	http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf contact OIS-EASG-DITIM for latest CMS guidance document

[1] Under very special circumstances an Authority to Operate (ATO) may be granted in lieu of an Accreditation until all C&A requirements are fulfilled by the Business Owner
[2] FISMA - Federal Information Security Management Act of 2002
[3] Every 3 years, or less as determined by the Chief Information Officer (CIO), unless there are major changes to a system, the system security level is increased, a serious security violation occurs or the threat environment changes. Business Owners must attest annually to the currency of the SSP and IS RA as part of their FMFIA questionnaire.
[4] Clinger-Cohen Act, formerly the IT Management Reform Act of 1996 (ITMRA)