

## 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) <sup>1</sup>	FISMA <sup>2</sup>		Every 3 years <sup>3</sup>	<a href="http://www.cms.hhs.gov/informationsecurity/downloads/CA_procedure.pdf">http://www.cms.hhs.gov/informationsecurity/downloads/CA_procedure.pdf</a>
System Security Plan (SSP)	FISMA	C&A	Every 3 years <sup>3</sup>	<a href="http://cms.hhs.gov/InformationSecurity/Downloads/ssp_meth.pdf">http://cms.hhs.gov/InformationSecurity/Downloads/ssp_meth.pdf</a>
IS Risk Assessment (RA)	FISMA	SSP	Every 3 years <sup>3</sup>	<a href="http://cms.hhs.gov/InformationSecurity/Downloads/RA_meth.pdf">http://cms.hhs.gov/InformationSecurity/Downloads/RA_meth.pdf</a>
Contingency Plan	FISMA	C&A	As needed	<a href="http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf">http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf</a>
Contingency Plan (CP) Testing	FISMA	C&A	Every 365 days <sup>4</sup>	<a href="http://cms.hhs.gov/InformationSecurity/Downloads/CP_Tabletop_template.zip">http://cms.hhs.gov/InformationSecurity/Downloads/CP_Tabletop_template.zip</a>
Privacy Impact Assessment (PIA)	FISMA	C&A	Annually by June 1st	<a href="http://intranet.hhs.gov/infosec/docs/policies_guides/PIA/PIA_Guide.pdf">http://intranet.hhs.gov/infosec/docs/policies_guides/PIA/PIA_Guide.pdf</a>
Security Test & Evaluation (ST&E)	FISMA	C&A	Every 3 years <sup>3</sup>	<a href="http://cms.hhs.gov/InformationSecurity/Downloads/Reporting_Standard.pdf">http://cms.hhs.gov/InformationSecurity/Downloads/Reporting_Standard.pdf</a>
Security Controls Testing	FISMA	C&A	A sub-set every 365 days <sup>4</sup>	<a href="http://csrc.nist.gov/publications/drafts/SP800-53A-spd.pdf">http://csrc.nist.gov/publications/drafts/SP800-53A-spd.pdf</a>
Plan of Actions & Milestones (POA&M)	FISMA	C&A	Nov 1, Feb 1, May 1 & Aug 1	<a href="http://cms.hhs.gov/informationsecurity/Downloads/poam_guidelines.pdf">http://cms.hhs.gov/informationsecurity/Downloads/poam_guidelines.pdf</a>
Corrective Action Plans (CAP)	FISMA	POA&M	1 <sup>st</sup> of every month	<a href="http://cms.hhs.gov/informationsecurity/Downloads/poam_guidelines.pdf">http://cms.hhs.gov/informationsecurity/Downloads/poam_guidelines.pdf</a>
Security Costs Budgeting	Clinger-Cohen Act <sup>5</sup>	Exhibit 300	Annually (generally in February)	<a href="http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf">http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf</a> contact OIS-EASG-DITIM for latest CMS guidance document

<sup>1</sup> 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

<sup>2</sup> FISMA - Federal Information Security Management Act of 2002

<sup>3</sup> 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 RA as part of their FMFIA questionnaire.

<sup>4</sup> Every 365 days, except leap year when it is required every 366 days

<sup>5</sup> Clinger-Cohen Act, formerly the IT Management Reform Act of 1996 (ITMRA)