

# Satisfying FedRAMP AppSec Requirements With Synopsys Solutions

## The challenge

Cloud service providers (CSPs) and federal agencies need tools and services that enable them to satisfy the application security (AppSec) aspects of the [Federal Risk and Authorization Management Program \(FedRAMP\)](#) requirements. FedRAMP is a United States government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Per an [Office of Management and Budget memorandum](#), any cloud services offering that holds federal data must be FedRAMP-authorized.

## The solution

Synopsys has partnered with key [third-party assessment organizations](#) that perform initial and periodic assessments of cloud systems to ensure they meet FedRAMP requirements.

The [FedRAMP Security Controls Baseline document](#) provides an overview of the security controls, enhancements, parameters, requirements, and guidance listed in [FedRAMP system security plan templates](#).

CSPs and federal agencies must implement these security controls, enhancements, parameters, and requirements within a cloud computing environment to satisfy FedRAMP requirements. The security controls and enhancements have been selected from the National Institute for Standards and Technology (NIST) SP 800-53 Revision 4 catalog of controls. The selected controls and enhancements are for cloud systems designated as low-, moderate-, and high-impact information systems, as defined in [Federal Information Processing Standards Publication 199](#).

AppSec is a significant component of achieving FedRAMP compliance. The [Synopsys software integrity portfolio](#) includes AppSec tools and services that help address all AppSec-related FedRAMP needs and controls.

## The benefits

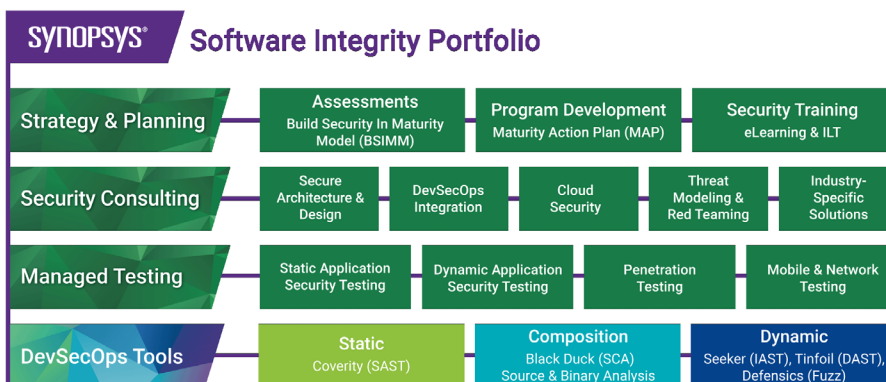
[Federal agencies](#) can save money and time by adopting innovative cloud services to meet their critical mission needs.

[CSPs](#) offer cloud services that allow federal agencies to meet their mission needs securely and quickly.

FedRAMP aims to:

- Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations
- Improve confidence in the security of cloud solutions and security assessments
- Achieve consistent security authorizations using a baseline set of agreed-upon standards for cloud product approval in or outside of FedRAMP
- Ensure consistent application of existing security practices
- Increase automation and use of near-real-time data for continuous monitoring

Synopsys AppSec solutions provide a cohesive, seamless way to build integrity into your software development process to manage risk and compliance, create operational efficiencies, reduce time to market, and minimize costs.



Synopsys tools and services provide full (●) or partial (◐) compliance for the following AppSec-related FedRAMP controls.

FedRAMP				Synopsys		
Control family	Control sort ID	Control name	Baseline control	Coverage	AppSec tools	AppSec services
Awareness and training	AT-01	Security awareness and training policy and procedures	High Moderate Low LI-SaaS	◐		✓ <a href="#">AppSec program strategy</a>
	AT-02	Security awareness training	High Moderate Low LI-SaaS	◐	✓ <a href="#">eLearning</a>	✓ <a href="#">Instructor-led training</a>
	AT-03	Role-based security training	High Moderate Low LI-SaaS	◐	✓ <a href="#">eLearning</a>	✓ <a href="#">Instructor-led training</a> <a href="#">AppSec program strategy</a>
	AT-03 (03)	Security training   practical exercises	High	●	✓ <a href="#">eLearning</a>	✓ <a href="#">Instructor-led training</a> Social engineering
	AT-04	Security training records	High Moderate Low LI-SaaS	◐	✓ <a href="#">eLearning</a>	
Security assessment and authorization	CA-01	Security assessment and authorization policy and procedures	High Moderate Low LI-SaaS	◐		✓ <a href="#">AppSec program strategy</a>
	CA-02	Security assessments	High Moderate Low LI-SaaS	◐	✓ Multiple	✓ Multiple
	CA-02 (01)	Security assessments   independent assessors	High Moderate Low LI-SaaS	◐		✓ Multiple
	CA-02 (02)	Security assessments   specialized assessments	High Moderate	●	✓ Multiple	✓ Multiple
	CA-05	Plan of action and milestones	High Moderate Low LI-SaaS	◐		✓ <a href="#">AppSec program strategy</a>
	CA-07	Continuous monitoring	High Moderate Low LI-SaaS	◐	✓ <a href="#">Black Duck®</a>	
	CA-07 (01)	Continuous monitoring   independent assessment	High Moderate	◐		✓ Multiple
	CA-07 (03)	Continuous monitoring   trend analyses	High	◐	✓ <a href="#">Black Duck</a>	
	CA-08	Penetration testing	High Moderate	●		✓ <a href="#">Pen testing</a>
	CA-08 (01)	Penetration testing   independent penetration agent or team	High Moderate	●		✓ <a href="#">Pen testing</a>

FedRAMP				Synopsis		
Control family	Control sort ID	Control name	Baseline control	Coverage	AppSec tools	AppSec services
Configuration management	CM-03 (02)	Configuration change control   test   validate   document changes	High		✓ Multiple	✓ <a href="#">Pen testing</a>
	CM-04	Security impact analysis	High Moderate		✓ Multiple	✓ <a href="#">Pen testing</a>
	CM-05	Access restrictions for change	High Moderate			✓ <a href="#">AppSec program strategy</a>
	CM-07 (01)	Least functionality   periodic review	High Moderate			✓ <a href="#">Pen testing</a>
	CM-10 (01)	Software usage restrictions   open source software	High Moderate		✓ <a href="#">Black Duck</a>	✓ <a href="#">AppSec program strategy</a>
Identification and authentication	IA-05 (07)	Authenticator management   no embedded unencrypted static authenticators	High Moderate		✓ Multiple	✓ Multiple
Planning	PL-02	System security plan	High Moderate Low LI-SaaS			✓ <a href="#">AppSec program strategy</a> <a href="#">Architecture risk analysis</a> <a href="#">Threat modeling</a>
	PL-02 (03)	System security plan   plan/coordinate with other organizational entities	High Moderate			✓ Multiple
	PL-08	Information security architecture	High Moderate			✓ <a href="#">Architecture risk analysis</a> <a href="#">Threat modeling</a>
Risk assessment	RA-03	Risk assessment	High Moderate Low LI-SaaS			✓ <a href="#">Architecture risk analysis</a>
	RA-05	Vulnerability scanning	High Moderate Low LI-SaaS		✓ Multiple	✓ Multiple
	RA-05 (01)	Vulnerability scanning   update tool capacity	High Moderate		✓ Multiple	✓ Multiple
	RA-05 (02)	Vulnerability scanning   update by frequency / prior to new scan / when identified	High Moderate		✓ Multiple	✓ Multiple
	RA-05 (03)	Vulnerability scanning   breadth / depth of coverage	High Moderate		✓ Multiple	✓ Multiple
	RA-05 (04)	Vulnerability scanning   discoverable information	High		✓ Multiple	✓ Multiple
	RA-05 (06)	Vulnerability scanning   automated trend analyses	High Moderate		✓ Multiple	✓ Multiple
	RA-05 (08)	Vulnerability scanning   review historic audit logs	High Moderate			✓ <a href="#">Blue teaming</a>
	RA-05 (10)	Vulnerability scanning   correlate scanning information	High		✓ Multiple	✓ Multiple

FedRAMP				Synopsys		
Control family	Control sort ID	Control name	Baseline control	Coverage	AppSec tools	AppSec services
System and services acquisition	SA-03	System development lifecycle	High Moderate Low LI-SaaS	●	✓ <a href="#">eLearning</a>	✓ <a href="#">AppSec program strategy</a> <a href="#">Instructor-led training</a> Staff augmentation
	SA-04 (01)	Acquisition process   functional properties of security controls	High Moderate	●		✓ <a href="#">Architecture risk analysis</a> <a href="#">Threat modeling</a>
	SA-04 (02)	Acquisition process   design / implementation information for security controls	High Moderate	●		✓ <a href="#">Architecture risk analysis</a> <a href="#">Threat modeling</a>
	SA-04 (08)	Acquisition process   continuous monitoring plan	High Moderate	●		✓ <a href="#">Architecture risk analysis</a> <a href="#">Threat modeling</a>
	SA-04 (09)	Acquisition process   functions / ports / protocols / services in use	High Moderate	●		✓ <a href="#">Architecture risk analysis</a> <a href="#">Threat modeling</a>
	SA-05	Information system documentation	High Moderate Low LI-SaaS	◐		✓ <a href="#">AppSec program strategy</a> <a href="#">Architecture risk analysis</a> <a href="#">Threat modeling</a>
	SA-08	Security engineering principles	High Moderate	●		✓ <a href="#">AppSec program strategy</a> <a href="#">Architecture risk analysis</a> <a href="#">Threat modeling</a>
	SA-09 (01)	External information systems   risk assessments / organizational approvals	High Moderate	◐	✓ Multiple	✓ Multiple
	SA-10	Developer configuration management	High Moderate	◐	✓ Multiple	✓ Multiple
	SA-11	Developer security testing and automation	High Moderate	●	✓ Multiple	✓ Multiple
	SA-11 (01)	Developer security testing and automation   static code analysis	High Moderate	●	✓ <a href="#">Coverity®</a>	✓ <a href="#">Secure code review</a>
	SA-11 (02)	Developer security testing and automation   threat and vulnerability analyses	High Moderate	●	✓ Multiple	✓ Multiple
	SA-11 (08)	Developer security testing and automation   dynamic code analysis	High Moderate	●	✓ <a href="#">Defensics®</a> <a href="#">Seeker®</a> <a href="#">Tinfoil™</a>	✓ <a href="#">DAST</a>
	SA-12	Supply chain protection	High	●	✓ Multiple	✓ Multiple
	SA-15	Development process, standards, and tools	High	●	✓ Multiple	✓ Multiple
	SA-16	Developer-provided training	High	●	✓ <a href="#">eLearning</a>	✓ <a href="#">Instructor-led training</a>
	SA-17	Developer security architecture and design	High	●		✓ <a href="#">Architecture risk analysis</a> <a href="#">Threat modeling</a>

FedRAMP				Synopsys		
Control family	Control sort ID	Control name	Baseline control	Coverage	AppSec tools	AppSec services
System and information integrity	SI-01	System and information integrity policy and procedures	High Moderate Low LI-SaaS	○		✓ <a href="#">AppSec program strategy</a>
	SI-02	Flaw remediation	High Moderate Low LI-SaaS	○	✓ Multiple	✓ Multiple
	SI-02 (01)	Flaw remediation   central management	High	○	✓ Multiple	✓ Multiple
	SI-02 (02)	Flaw remediation   automated flaw remediation status	High Moderate	○	✓ Multiple	✓ Multiple
	SI-02 (03)	Flaw remediation   time to remediate flaws / benchmarks for corrective actions	High Moderate	○	✓ Multiple	✓ Multiple
	SI-03	Malicious code protection	High Moderate Low LI-SaaS	○		✓ Custom
	SI-05	Security alerts, advisories, and directives	High Moderate Low LI-SaaS	○	✓ <a href="#">Black Duck</a>	
	SI-05 (01)	Security alerts, advisories, and directives   automated alerts and advisories	High	○	✓ <a href="#">Black Duck</a>	
	SI-06	Security function verification	High Moderate	○	✓ Multiple	✓ Multiple
	SI-10	Information input validation	High Moderate	●	✓ Multiple	✓ Multiple

## The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at [www.synopsys.com/software](http://www.synopsys.com/software).

**Synopsys, Inc.**  
185 Berry Street, Suite 6500  
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193  
International Sales: +1 415.321.5237  
Email: [sig-info@synopsys.com](mailto:sig-info@synopsys.com)

©2021 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at [www.synopsys.com/copyright.html](http://www.synopsys.com/copyright.html). All other names mentioned herein are trademarks or registered trademarks of their respective owners. January 2021