COPADO

Whitepaper

How Copado Helps Federal Contractors, Systems Integrators, and DoD Vendors Meet CMMC 2.0 and NIST 800-171 Requirements

The **Cybersecurity Maturity Model Certification** (CMMC) 2.0 program is becoming a critical requirement for defense contractors handling Controlled Unclassified Information (CUI). CMMC 2.0 reduces the framework to three maturity levels and aligns Level 2 with all 110 requirements from NIST SP 800-171 Revision 2, which remains the current compliance standard for defense contractors under DFARS 252.204-7012.

Copado's DevSecOps platform provides a comprehensive solution that directly addresses the majority of CMMC 2.0 Level 2 DevSecOps requirements through its enterprise-grade security framework, integrated compliance capabilities, and automated security controls. Copado is the only DevOps platform for Salesforce to achieve FedRAMP, ISO 27001, SOC 2 Type 2, and GDPR compliance, demonstrating its commitment to the highest security standards required by federal agencies and defense contractors.

This white paper demonstrates how Copado helps government contractors comply with CMMC 2.0 by automating, enforcing, and monitoring the technical DevSecOps controls required by NIST SP 800-171, all within a FedRAMP-authorized Salesforce-native platform. It highlights how Copado's DevSecOps capabilities align with the security requirements outlined in NIST SP 800-171 Revision 2 and and support CMMC 2.0 compliance initiatives for Defense Industrial Base (DIB) organizations.

Introduction to CMMC 2.0 and NIST SP 800-171

CMMC 2.0 Framework Overview

The Department of Defense introduced CMMC 2.0 in 2021, reducing the original five-tier model to three levels:

1

Level 1 (Foundational)

Designed to protect Federal Contract Information (FCI) with 17 security controls based on FAR 52.204-21 standards.

2

Level 2 (Advanced)

Aligns with NIST SP 800-171 requirements and includes all 110 practices for protecting CUI.

3

Level 3 (Expert)

Reserved for contractors integral to DoD's most critical programs, adding 24 requirements from NIST SP 800-172.

Most defense contracts will be targeting Level 2.

NIST SP 800-171 Revision 2 Requirements Structure

NIST SP 800-171 Revision 2, forming the basis of CMMC Level 2, establishes 110 security requirements organized into 14 families covering access control, audit and accountability, configuration management, and other critical security domains. The framework establishes baseline security requirements for protecting CUI in nonfederal systems and organizations.

The 14 security requirement families include:

AC	**Access Control**
AT	**Awareness and Training**
AU	**Audit and Accountability**
CM	**Configuration Management**
IA	**Identification and Authentication**
IR	**Incident Response**
MA	**Maintenance**
MP	**Media Protection**
PE	**Physical and Environmental Protection**
PS	**Personnel Security**
PL	**Planning**
RA	**Risk Assessment**
SC	**System and Communications Protection**
SI	**System and Information Integrity**

Copado DevSecOps Platform Security Framework

Comprehensive Security Certifications

Copado maintains a dedicated Security Compliance team that implements and monitors a security framework consisting of policies, procedures, and controls that align with ISO 27001, SOC 2, FedRAMP, and GDPR requirements. This multi-framework approach demonstrates Copado's ability to meet diverse compliance requirements simultaneously.

Key certifications include:

FedRAMP Authorization

Copado achieved Federal Risk and Authorization Management Program (FedRAMP) authorization to operate (ATO) at the moderate impact level.

ISO 27001

International standard for information security management systems.

SOC 2 Type 2

Third-party audit conducted annually with compliance verified by independent assessment firms.

GDPR Compliance

European data protection regulation compliance.

Built-in Security Architecture

Copado provides enterprise-grade security for all stages of the development cycle with a built-in security framework, governance controls, and cybersecurity support. The platform integrates security throughout the DevOps lifecycle rather than treating it as an afterthought.

Core architectural security features include:

- AWS data centers complying with ISO 27001, PCI DSS Level 1, HIPAA, and SOC 1, 2, and 3
- AWS virtual private cloud deployment with external access blocked at the network level
- End-to-end encryption for data in transit and at rest
- Role-based access control with least privilege principles
- Automated vulnerability scanning and management

NIST SP 800-171 Revision 2 DevSecOps Requirements Mapping

The following sections detail how Copado's DevSecOps platform addresses the security requirements within NIST SP 800-171 Rev 2 that are directly relevant to development, security, and operations practices. While NIST SP 800-171 encompasses broader organizational security requirements, including personnel security and physical protection, Copado's platform addresses the technical and operational security controls essential to secure software development and deployment.

Access Control (AC) Requirements

3.1.1 Account Management Copado addresses this requirement through comprehensive user account lifecycle management:

- Role-based, least privilege system access control, including granting and revoking access
- Formal quarterly review of all administrators and users
- Integration with organizational identity providers for centralized account management
- Automated account provisioning and de-provisioning based on role assignments

3.1.2 Access Enforcement The platform enforces approved authorizations through:

- Multi-factor authentication requirements for all user access
- Integration with enterprise single sign-on (SSO) systems
- Granular permission controls at the project and environment level
- Real-time access monitoring and alerting

3.1.3 Information Flow Enforcement Copado's Compliance Hub integrates into existing DevOps processes and automates compliance checks, monitoring and enforcing rules for metadata changes and identifying non-compliant changes before deployment.

Awareness and Training (AT) Requirements

3.2.1 Security Awareness and Training Copado supports security awareness through:

- Security awareness training for all employees upon hire and annually
- Adherence to the Copado code of conduct
- DevSecOps best practices training and documentation
- Security-focused community engagement and knowledge sharing

Note: Organizations must implement comprehensive security awareness programs that extend beyond DevSecOps practices to include organizational security policies and procedures.

Audit and Accountability (AU) Requirements

3.3.1 Event Logging Copado implements automated monitoring, logging, and system alerts to capture security-relevant events, including:

- User authentication and authorization events
- System configuration changes
- Data access and modification events
- Administrative actions and privilege usage

3.3.2 Content of Audit Records Audit records include comprehensive information such as:

- Event type, timestamp, and source location
- User identity and session information
- Outcome of the event (success/failure)
- Specific objects or resources affected

3.3.4 Audit Record Review and Analysis The platform provides visibility into compliance health and detects violations in real-time with a centralized dashboard, enabling:

- Automated analysis of audit logs for suspicious patterns
- Real-time alerting for security events
- Correlation of events across different system components
- Regular reporting to designated security personnel

Configuration Management (CM) Requirements

3.4.1 Baseline Configuration Copado's version control and configuration management capabilities support:

- Automated baseline configuration establishment and maintenance
- Git-based version control for all configuration artifacts
- Immutable infrastructure deployment patterns
- Configuration drift detection and remediation

3.4.2 Configuration Change Control Every change must go through Copado before moving from environment to environment, serving as the backbone of the development process. The platform provides:

- Mandatory code review and approval workflows
- Automated compliance scans across the DevOps process
- Change impact analysis and security assessments
- Rollback capabilities for unauthorized changes

3.4.6 Configuration Settings The platform enforces secure configuration settings through:

- Policy-as-code implementation
- Automated security scanning and validation
- Template-based deployment with security hardening
- Continuous monitoring of configuration compliance

Identification and Authentication (IA) Requirements

3.5.3 Multi-Factor Authentication Copado implements multi-factor authentication and replay resistance for non-local maintenance and diagnostic sessions, providing:

- Integration with enterprise MFA solutions
- Support for hardware tokens and biometric authentication
- Session management with timeout controls
- Device registration and trust verification

3.5.7 Authenticator Management The platform manages authenticators through:

- Integration with organizational identity management systems
- Automated credential lifecycle management
- Secure storage and transmission of authentication data
- Regular authenticator rotation and renewal processes

Incident Response (IR) Requirements

3.6.1 Incident Handling Copado maintains documented incident response and disaster recovery policies and procedures, with annual testing and team training. The platform supports:

- Automated incident detection and alerting
- Integration with organizational Security Operations Centers (SOCs)
- Forensic data collection and preservation capabilities

- Coordination with external incident response teams

3.6.2 Incident Reporting The platform provides:

- Real-time notification capabilities for security events
- Integration with external threat intelligence feeds
- Automated reporting to designated authorities
- Audit trails for incident investigation and analysis

Maintenance (MA) Requirements

3.7.1 System Maintenance Copado controls role-based, least privilege system access for maintenance activities, ensuring:

- Approval and monitoring of maintenance tools
- Malware scanning of diagnostic media and tools
- Controlled access to maintenance equipment
- Documentation of all maintenance activities

Media Protection (MP) Requirements

3.8.3 Media Marking and 3.8.7 Media Use Customer data is encrypted in transit and at rest, with regular backups performed and backup testing conducted annually. The platform implements:

- Full encryption of data at rest and in transit
- Secure key management practices
- Automated data sanitization procedures
- Controlled media lifecycle management

Physical and Environmental Protection (PE) Requirements

3.10.1 Physical Access Control and 3.10.6 Monitoring Physical Access While physical security is primarily an organizational responsibility, Copado supports these requirements through its cloud infrastructure partnership. Copado utilizes third-party, cloud-based data centers which maintain network architecture and data layer controls that meet the requirements of the most security-sensitive organizations. These controls include:

- Multi-factor physical access controls at data center facilities
- 24/7 surveillance and monitoring at hosting locations
- Environmental controls and monitoring
- Secure equipment disposal procedures

Note: Organizations must implement additional physical security controls for their own facilities and workstations beyond what Copado provides through its cloud infrastructure.

Personnel Security (PS) Requirements

Personnel Security controls (3.9.1 Personnel Screening and 3.9.2 Personnel Termination) While personnel security is primarily an organizational responsibility, Copado supports aspects of these requirements through its platform capabilities:

- Integration with organizational identity and access management systems for automated account lifecycle management
- Automated user access revocation capabilities when integrated with HR systems
- Audit trails for personnel access and activity monitoring

Note: Organizations remain responsible for personnel screening, background checks, and establishing personnel security policies beyond the technical controls provided by Copado's platform.

Planning (PL) Requirements

3.12.4 System Security Plans Copado supports the development and maintenance of system security plans through:

- Automated documentation of system configurations and security controls
- Integration with compliance management workflows
- Template-based security documentation generation
- Version control for security documentation and policies

Note: Organizations must develop comprehensive system security plans that extend beyond the technical controls provided by Copado and include organizational policies, procedures, and risk management frameworks.

Risk Assessment (RA) Requirements

3.11.2 Vulnerability Scanning Copado implements automated vulnerability scans that run regularly and are addressed according to vulnerability management processes. The platform provides:

- Continuous vulnerability assessment across all environments
- Automated patch management processes
- Risk-based vulnerability prioritization
- Integration with threat intelligence feeds

System and Communications Protection (SC) Requirements

3.13.8 Transmission Confidentiality and Integrity Customer data is encrypted in transit and at rest within databases, implementing:

- TLS encryption for all communications
- End-to-end encryption for sensitive data flows
- Certificate management and validation
- Network segmentation and isolation

3.13.1 Boundary Protection The platform implements comprehensive boundary protection through:

- Network firewalls and intrusion detection systems
- Application-level security controls
- API security and rate limiting
- Secure communication protocols

System and Information Integrity (SI) Requirements

3.14.1 Flaw Remediation Copado proactively addresses security vulnerabilities, such as implementing industry-recommended mitigations for Log4j vulnerability (CVE-2021-44228). The platform provides:

- Automated security patch management
- Vulnerability scanning and assessment
- Coordinated disclosure processes
- Emergency response procedures for critical vulnerabilities

3.14.2 Malicious Code Protection The platform implements malware protection through:

- Multi-layered antimalware scanning
- Behavioral analysis and anomaly detection
- Quarantine and remediation capabilities
- Real-time threat intelligence integration

Copado's DevSecOps Capabilities Supporting CMMC 2.0

Integrated Compliance Hub

Copado's Compliance Hub makes it easy to maintain regulations, rules, and best practices by automating compliance scans across the DevOps process and identifying non-compliant changes before deployment. This capability directly supports multiple DevSecOps-related NIST SP 800-171 requirements including:

- **3.4.2 (Configuration Change Control):** Automated validation of changes against security policies
- **3.3.1 (Event Logging):** Comprehensive logging of all compliance-related activities
- **Continuous Assessment:** Ongoing evaluation of security control effectiveness

Security Planning

Copado supports your Security Action Plan for unique business needs, pairing organizations with dedicated, CISSP-certified security experts who assess current state and tailor plans to tackle compliance and security needs. This service supports DevSecOps-related requirements such as:

- **3.12.4 (System Security Plans):** Development of comprehensive security documentation for DevSecOps practices
- **3.11.1 (Risk Assessment):** Regular risk assessments and mitigation planning for development and deployment processes
- **Plan of Action and Milestones:** Structured approach to addressing security deficiencies in DevSecOps practices

Note: Organizations must supplement these DevSecOps-focused services with broader organizational security planning that addresses personnel, physical, and administrative security requirements.

Continuous Monitoring and Assessment

Copado undergoes annual third-party penetration testing and maintains continuous monitoring capabilities for its platform and services, supporting DevSecOps-related monitoring requirements:

- **Continuous Monitoring:** Ongoing security posture assessment of development and deployment pipelines
- **3.14.6 (System Monitoring):** Real-time detection of security events within the DevSecOps platform
- **3.3.4 (Audit Record Review):** Regular analysis of security logs and events related to development and deployment activities

Note: Organizations must implement broader continuous monitoring programs that extend beyond the DevSecOps platform to include all systems processing CUI.

Supply Chain Security

Copado expands its DevSecOps platform to integrate security, compliance, governance, and risk management into every stage of the delivery pipeline. This capability addresses DevSecOps-related supply chain requirements:

- **Supply Chain Risk Management:** Comprehensive supply chain risk assessment for development tools and dependencies
- **Supply Chain Controls:** Implementation of supply chain security controls within the development pipeline
- **External System Services:** Management of third-party service provider risks related to development and deployment services

Note: Organizations must implement comprehensive supply chain risk management programs that extend beyond development tools to include all suppliers and contractors handling CUI.

Implementation Recommendations

Phase 1

ASSESSMENT AND PLANNING

Organizations should begin by conducting a comprehensive gap analysis against NIST SP 800-171 Revision 2 requirements, leveraging Copado's dedicated CISSP-certified security experts to assess current DevSecOps practices and develop a tailored compliance roadmap.

Key activities include:

- Current state DevSecOps security assessment
- NIST SP 800-171 Revision 2 requirements mapping for development and deployment processes
- Risk assessment and prioritization for DevSecOps-related controls
- Development of implementation timeline for technical security controls
- Identification of organizational requirements beyond Copado's platform scope

Phase 2

CORE PLATFORM IMPLEMENTATION

Deploy Copado's DevSecOps platform with a focus on foundational security capabilities:

- Implementation of Compliance Hub for automated compliance monitoring of development processes
- Integration with organizational identity and access management systems
- Configuration of audit logging and monitoring capabilities for DevSecOps activities
- Establishment of secure development workflows and CI/CD pipelines
- Implementation of automated security scanning and vulnerability management

Phase 3

ADVANCED SECURITY INTEGRATION

Implement advanced DevSecOps security capabilities and continuous monitoring:

- Integration with Security Operations Center (SOC) capabilities for development environment monitoring
- Advanced threat detection and response procedures for development and deployment of pipelines
- Comprehensive vulnerability management processes for code and infrastructure
- Regular security assessments and penetration testing of DevSecOps environments
- Implementation of secure software supply chain practices

Phase 4

CERTIFICATION PREPARATION

Prepare for CMMC 2.0 assessment through:

- Documentation of all DevSecOps security controls and procedures
- Internal security control assessments focusing on development and deployment practices
- Remediation of identified gaps or deficiencies in technical security controls
- Coordination with Certified Third-Party Assessment Organizations (C3PAOs)
- Integration of DevSecOps security documentation with broader organizational security programs

Conclusion

Copado's DevSecOps platform provides a robust foundation for addressing the DevSecOps-related aspects of CMMC 2.0 Level 2 compliance through its comprehensive security framework, integrated compliance capabilities, and alignment with relevant NIST SP 800-171 Revision 2 requirements. As the only DevOps platform for Salesforce to achieve FedRAMP, ISO 27001, SOC 2 Type 1, and GDPR compliance, Copado demonstrates the security maturity and governance capabilities required by defense contractors for their development and deployment operations.

The platform's integrated approach to DevSecOps, combined with its extensive compliance certifications and security features, positions organizations to efficiently address the technical and operational security requirements of CMMC 2.0 while maintaining development agility and deployment velocity. However, organizations must recognize that Copado's platform addresses the DevSecOps components of CMMC 2.0 compliance and must be complemented by broader organizational security programs covering personnel security, physical security, and administrative controls.

By leveraging Copado's capabilities as part of a comprehensive security program, defense contractors can build a strong foundation for CMMC 2.0 certification while establishing sustainable DevSecOps practices that support long-term mission success. Organizations should view Copado's DevSecOps platform as a critical component of their overall compliance strategy, providing the technical controls and automation necessary for secure software development and deployment in CUI environments.

Organizations considering CMMC 2.0 compliance should evaluate Copado's DevSecOps platform as a strategic investment in both DevSecOps security compliance and operational excellence, providing the foundation for secure, scalable, and compliant software delivery practices essential for success in the Defense Industrial Base.

This white paper is based on publicly available information about CMMC 2.0, NIST SP 800-171 Revision 2, and Copado's DevSecOps platform capabilities as of June 2025. Organizations should consult with qualified security professionals and legal advisors for specific compliance guidance and implementation strategies.