CIS CG16 Implementation Checklist

All 14 safeguards with implementation guidance

Implementation Group 2 (IG2) Safeguards

- ■ 16.1 — Establish and maintain a secure application development process
- ■ 16.2 — Establish and maintain a process to accept and address vulnerabilities
- ■ 16.3 — Perform root cause analysis on security vulnerabilities
- ■ 16.4 — Establish and manage an inventory of third-party software components
- ■ 16.5 — Use up-to-date and trusted third-party software components
- ■ 16.6 — Establish and maintain a severity rating system for vulnerabilities
- ■ 16.7 — Use standard hardening configurations for application infrastructure
- ■ 16.8 — Separate production and non-production systems

Implementation Group 3 (IG3) Safeguards

- ■ 16.9 — Train developers in application security concepts and secure coding
- ■ 16.10 — Apply secure design principles in application architectures
- ■ 16.11 — Leverage vetted modules or services for application security
- ■ 16.12 — Implement code-level security checks
- ■ 16.13 — Conduct application penetration testing
- ■ 16.14 — Conduct threat modeling

Evidence Requirements

- ■ Document the SSDLC policy covering all six mandatory areas
- ■ Maintain training records for all development staff
- ■ Archive scan results (SAST, DAST, SCA) for audit trail
- ■ Record vulnerability remediation timelines and SLA adherence
- ■ Keep third-party component inventory current (monthly review)