Checklist for Application Security Managers

The world of application / product security is huge. It involves the whole system – every product, data store, domain, route, and user. Our team uses all of the items below and more to make it easier for our product engineers to introduce risk assessment early in the SDLC, identify helpful controls, and prioritize remediation where necessary.

Here's a list of artifacts that you and your team may need to create and regularly iterate on to help make your world smaller:

Program Evolution

- ☐ Guidance for conducting maturity model assessments
- ☐ Guidance for conducting regulatory and client contractual gap analyses
- ☐ Strategic planning and goal-setting documents for your team
    - ☐ Technical goals
    - ☐ Career development
- ☐ Defense in depth table

Secure Software Development Lifecycle

- ☐ Risk assessment recommendations for sprint planning
- ☐ Merge/pull request templates
- ☐ Pre-deploy risk assessment guidance
- ☐ New application or feature assessment checklists for developers

Culture & Community

- ☐ A list of available instructor-led, interactive or video training
- ☐ Regularly held office hours and/or community of practice meetings
- ☐ Application Security knowledge base with guidance documents and standards on topics such as:
    - ☐ API security recommendations
    - ☐ Administration dashboards for sensitive data
    - ☐ Application upgrades & currency standards
    - ☐ Authentication & access control especially business-accepted non-standard authentication schemes
    - ☐ Logging standards
    - ☐ Preferred libraries for authentication, access control & encryption
    - ☐ Rate limiting
    - ☐ Repository settings
    - ☐ Secure headers
    - ☐ Usage of cloud resources

- [ ] Zero-trust

New Application & Sensitive Feature Reviews

- [ ] Threat modeling instructionals
- [ ] Secure coding guidance checklist
- [ ] Rubric for grading applications (to be used by ASEs)

Internal Penetration Testing

- [ ] White-box report templates
- [ ] Preferred methodology and guidance for the following:
    - [ ] Regulatory gap analysis
    - [ ] Information Gathering & Reconnaissance
    - [ ] Authentication
    - [ ] Access Controls & Authorization
    - [ ] Application Logic
    - [ ] Session Management
    - [ ] Injection
    - [ ] Data Input Validation
    - [ ] Cross Site Scripting
    - [ ] Application Hosting
    - [ ] See OWASP WSTG & ASVS as needed

External Penetration Testing

- [ ] Request for quote templates
    - [ ] Preferred methodology (if needed)
    - [ ] Scope
- [ ] Matrix for assessing multiple vendors
- [ ] Report templates
- [ ] Bug bounty or responsible disclosure rules of engagement

Other Resources:

- https://owasp.org/www-pdf-archive/Owasp-ciso-guide.pdf
- https://www.nist.gov/cyberframework
- https://owasp.org/www-project-application-security-verification-standard/