PR.IP – Implementation and Processes Assessment Materials

Organization: Alma Security
Function: PROTECT
Category: PR.IP – Implementation & Processes
Framework Reference: NIST CSF 2.0 (PR.IP-01 through PR.IP-04)

1. Scope

This assessment evaluates Alma Security's implementation and operational security controls across:

- AWS cloud infrastructure
- Kubernetes clusters
- Amazon Linux 2 and Ubuntu servers
- Windows domain controller (Redwood City)
- Postgres databases
- Active security initiatives (WAF, MFA rollout, S3 security hardening, SQL injection mitigation)

The objective is to determine whether configuration management, change processes, and secure development practices are formally defined and effectively implemented.

2. PR.IP-01 – Secure Configuration and Baselines

Control Objective

Systems are configured according to approved security baselines and hardened against known risks.

Assessment Procedures

1. Review documented security configuration standards.
2. Compare AWS account configuration against CIS benchmarks.
3. Validate Kubernetes cluster hardening settings.

4. Inspect Linux server baseline configurations.
5. Review Windows domain controller hardening checklist.
6. Confirm S3 bucket security baseline aligns with recent hardening efforts.

Evidence to Collect

- Security baseline documentation
- CIS benchmark comparison reports
- Server configuration exports
- Hardening checklists
- Architecture diagrams

3. PR.IP-02 – Change Management Process

Control Objective

Infrastructure and application changes follow a documented, approved, and traceable change management process.

Assessment Procedures

1. Review Change Management Policy.
2. Sample 5 recent infrastructure changes from JIRA.
3. Confirm documented approvals and security review.
4. Verify rollback procedures are defined.
5. Confirm emergency change procedures are documented.

Evidence to Collect

- Change management procedure
- JIRA change logs

- Approval documentation
- Rollback procedures
- Interview notes with DevOps team

4. PR.IP-03 – Patch and Vulnerability Management

Control Objective

Systems are regularly patched and vulnerabilities are remediated in accordance with defined timelines.

Assessment Procedures

1. Review patch management schedule for AWS, Linux, and Windows systems.
2. Inspect vulnerability scan reports.
3. Validate remediation timelines against policy.
4. Review SQL injection mitigation implementation status.
5. Confirm MFA rollout progress and enforcement.

Evidence to Collect

- Patch management reports
- Vulnerability scan results
- Remediation tracking logs
- MFA implementation documentation

5. PR.IP-04 – Secure Development & Infrastructure-as-Code

Control Objective

Secure development lifecycle and infrastructure changes are controlled, reviewed, and securely implemented.

Assessment Procedures

1. Review Secure SDLC documentation.
2. Inspect Infrastructure-as-Code templates (Terraform/CloudFormation).
3. Confirm peer code review requirements.
4. Validate WAF configuration aligns with documented security requirements.
5. Confirm S3 security configurations are deployed via IaC where applicable.

Evidence to Collect

- Secure SDLC policy
- IaC templates
- Code review records
- WAF configuration screenshots
- Security architecture diagrams

6. Observations to Evaluate During Assessment

During testing, the assessor should consider:

- Whether configuration drift exists between documented baselines and live systems
- Whether change approvals are consistently documented
- Whether patch timelines meet defined SLAs
- Whether security projects (WAF, MFA, S3 hardening) are formally tracked and validated
- Whether infrastructure-as-code includes security validation controls

7. Implementation Summary – Alma Security

Alma Security maintains documented configuration baselines for AWS, Kubernetes, Linux, and Windows systems.

Infrastructure changes are tracked through JIRA and require documented approvals.

Active initiatives include WAF deployment, MFA rollout, SQL injection mitigation, and S3 hardening efforts.

Infrastructure deployments are managed using Infrastructure-as-Code with peer review requirements to support consistency and repeatability.