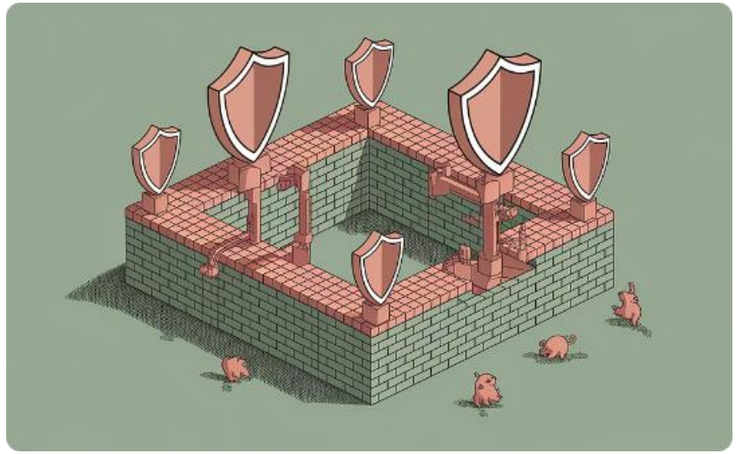
Security for Infrastructure vs. Application Projects

In an age of relentless cyber threats, data privacy regulations, and increasing reliance on cloud technologies, security isn’t optional—it’s fundamental. Whether you’re leading an infrastructure upgrade or launching a new app, understanding the distinct security considerations of each project type is critical for project success and organizational safety.

While both infrastructure and software development projects require strong security controls, they differ in scope, risk surfaces, stakeholders, and timelines. Here's what project managers need to know to keep both types of projects secure and compliant.

kW by Kimberly Wiethoff

Project Security: A Shared Responsibility



Why Security Matters

Cyber threats are relentless. Data privacy regulations are strict. Cloud technologies create new vulnerabilities.

Different Project Types

Infrastructure and application projects have distinct security considerations. They differ in scope, risk surfaces, and controls.

PM's Critical Role

You must orchestrate communication between teams. Enforce security checkpoints. Escalate concerns promptly.

Infrastructure Security: Guarding the Foundation

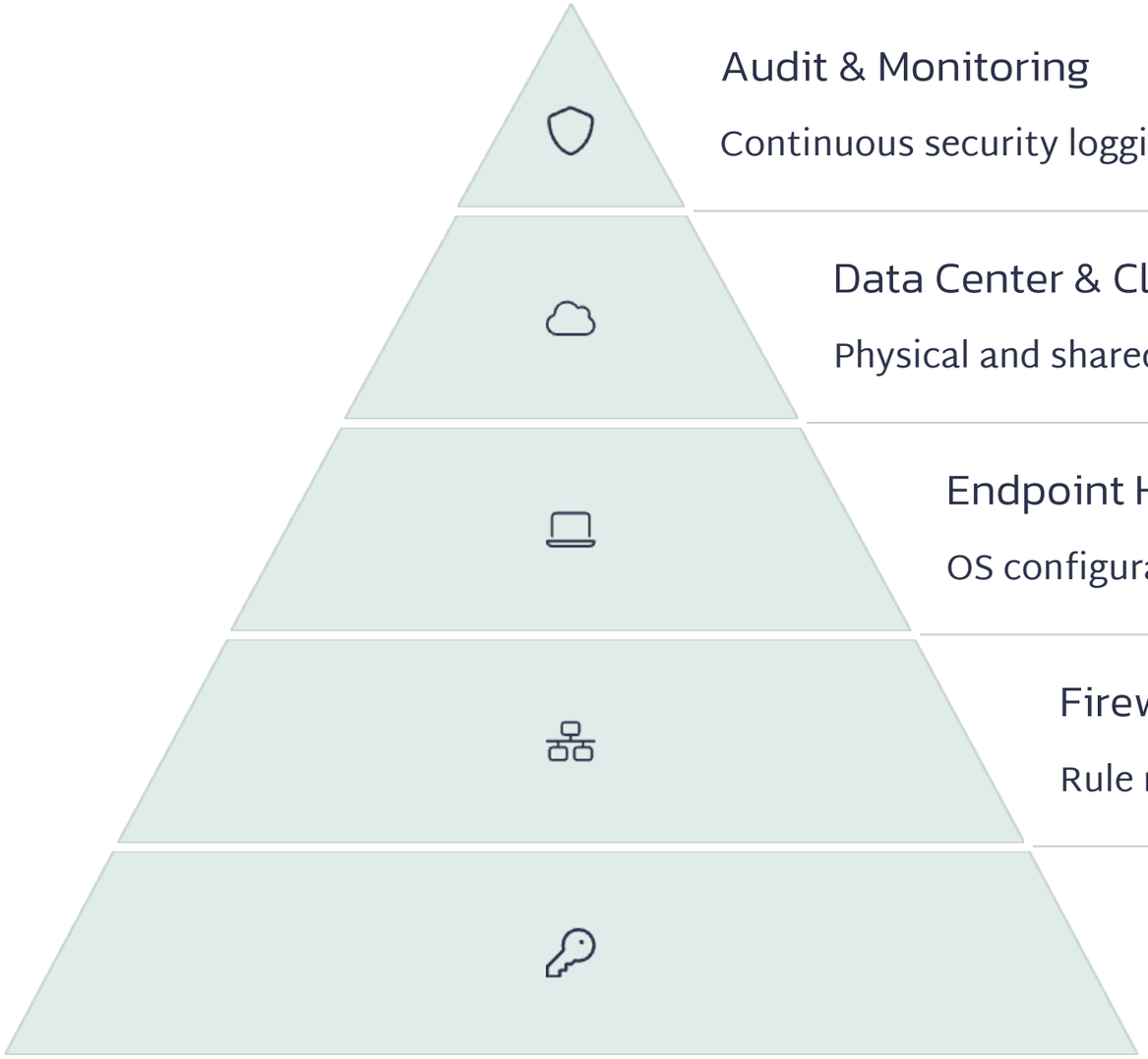
Infrastructure projects focus on the systems and environments that support all applications and business operations. Security in this context is primarily about **protecting the core technology stack** from threats and vulnerabilities.

Key Areas to Manage:

- **Identity and Access Management (IAM):** Ensure least privilege access to servers, network devices, and cloud consoles.

- **Firewall and Network Security:** Coordinate rule reviews and approvals (e.g., via Entra or Cisco Firepower) early in the project.
- **Endpoint Hardening:** Enforce baseline OS configurations, encryption policies, and antivirus protocols.
- **Data Center & Cloud Security:** Confirm physical security for on-prem hardware and review shared responsibility models for AWS/Azure.
- **Audit Trails and Logging:** Plan for security monitoring and log retention from Day 1.

Infrastructure Security Fundamentals



Audit & Monitoring

Continuous security logging

Data Center & Cloud

Physical and shared security models

Endpoint Hardening

OS configurations and encryption

Firewall & Network

Rule reviews and approvals

Identity & Access

Least privilege principles

Application Security Essentials

In software projects, security revolves around **code quality, data protection, and secure development practices.** Breaches often stem from logic flaws, insecure APIs, or poor handling of sensitive information.

Key Areas to Manage:

Secure SDLC

Security gates in CI/CD pipelines

Third-Party Components

Software Bill of Materials (SBOM)

Data Privacy

Encryption in transit and at rest

API Security

Authentication and rate limiting

User Authentication

MFA and session controls

Key Differences: Infrastructure vs. Application

Security Area	Infrastructure Projects	Application Projects
Access Control	Admin access to systems and cloud	User authentication, role-based access
Threat Surface	Networks, servers, cloud services	Web UIs, APIs, code vulnerabilities
Compliance	SOC 2, ISO 27001, NIST	HIPAA, GDPR, OWASP Top 10
Tools Used	Firewalls, endpoint protection, SIEM	SAST, DAST, API security scanners
Security Timing	Early, during provisioning	Continuous, throughout SDLC

Infrastructure Security in Action

1

Assessment Phase

Conduct security architecture review. Document current state vulnerabilities. Define security requirements.

2

Implementation Phase

Apply hardening standards. Configure firewalls. Set up IAM with least privilege access.

3

Validation Phase

Perform vulnerability scans. Run penetration tests. Complete security sign-off checkpoint.

4

Monitoring Phase

Implement continuous logging. Configure alerts. Establish incident response protocols.

Application Security Workflow

Design

Threat modeling and security requirements.

Develop

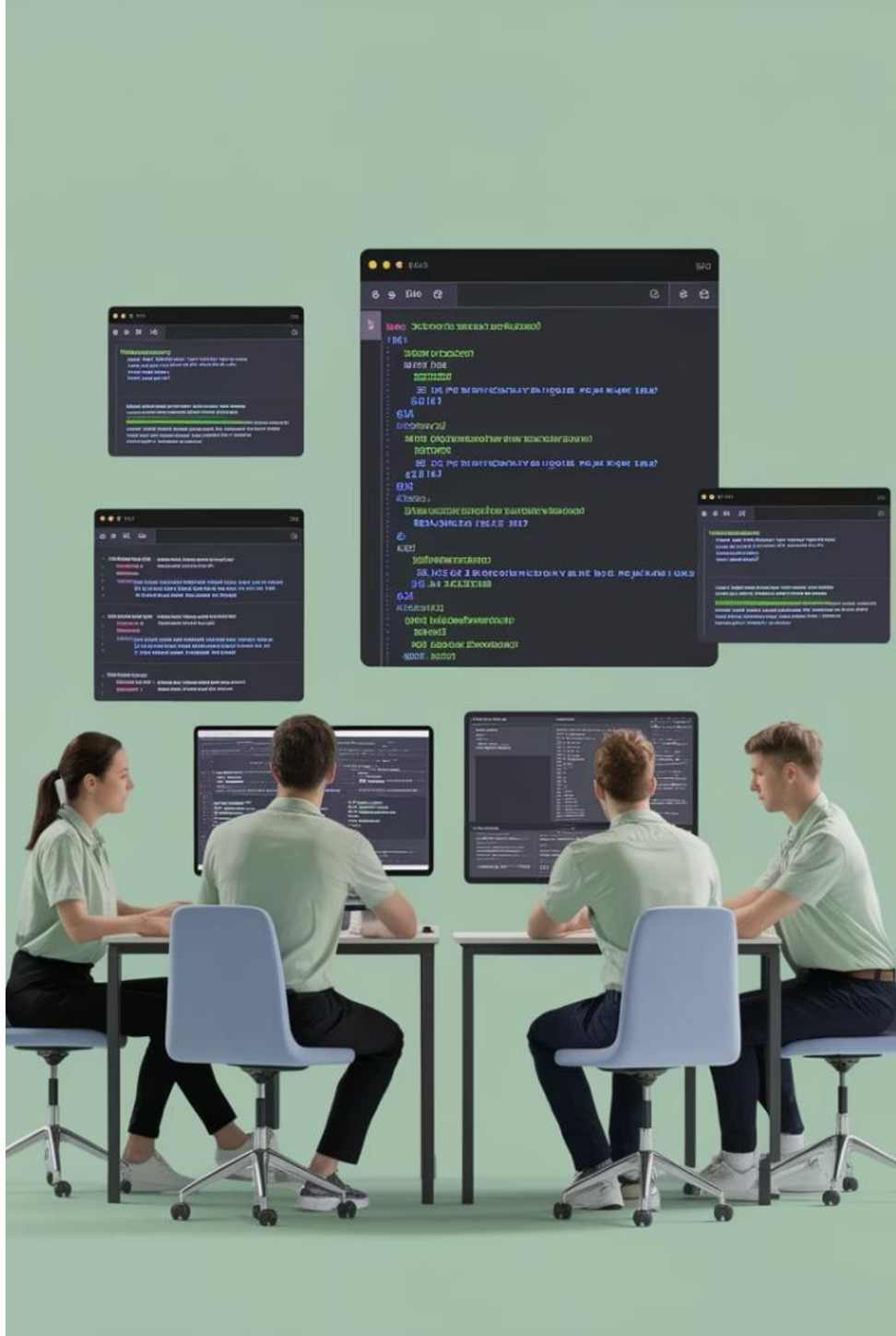
Secure coding and peer reviews.

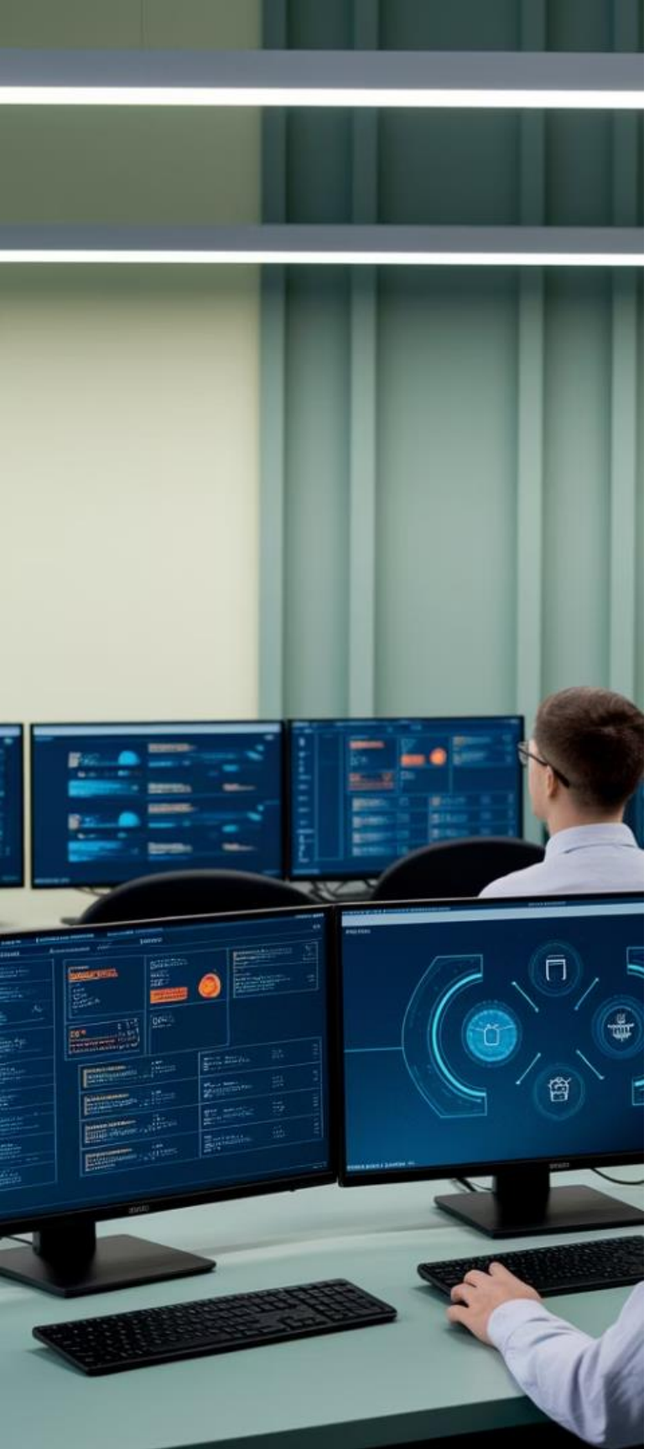
Test

SAST/DAST scanning and remediation.

Deploy

Final security validation and monitoring.





Security Tools Landscape

Infrastructure Security Tools

- Cisco Firepower for network protection
- Microsoft Entra ID for identity management
- Crowdstrike for endpoint security
- Splunk for security information management

Application Security Tools

- SonarQube for static code analysis
- OWASP ZAP for dynamic testing
- Snyk for dependency scanning
- Auth0 for identity and access management

Cross-Functional Tools

- Jira for security issue tracking
- Azure DevOps for secure CI/CD pipelines
- Nessus for vulnerability scanning
- Qualys for compliance checks

PM Security Checklist: Infrastructure Projects

Include Security SMEs from Day One

Involve InfoSec in project kickoff. Include network and system security specialists.

Document Security Requirements

Define security controls. Map requirements to compliance standards like SOC 2.

Schedule Security Checkpoints

Plan vulnerability scans. Set up security architecture reviews. Allow time for remediation.

Obtain Security Sign-Off

Require formal approval before production deployment. Document risk acceptance if needed.

PM Security Checklist: Application Projects

Establish Security Gates

Set up automated security checks in CI/CD pipeline. Define security acceptance criteria.

Plan for Authentication & Authorization

Choose appropriate auth mechanisms. Implement proper session management. Plan for MFA.

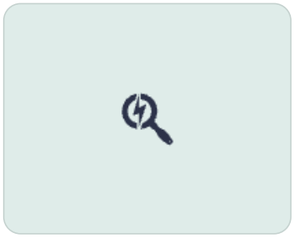
3 Integrate Security Testing

Schedule penetration tests. Run SAST and DAST scans regularly. Review results thoroughly.

Address Data Privacy Compliance

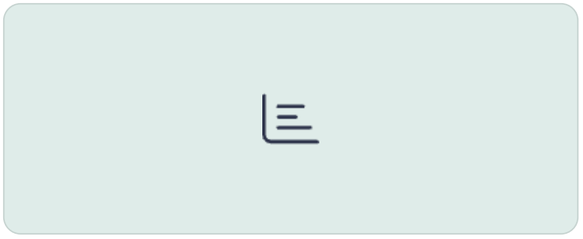
Document data flows. Implement encryption. Ensure GDPR and HIPAA compliance where needed.

Security Risk Management



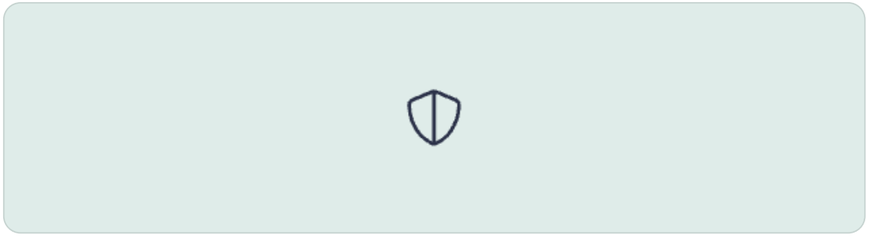
Identify Risks

Detect vulnerabilities and threats



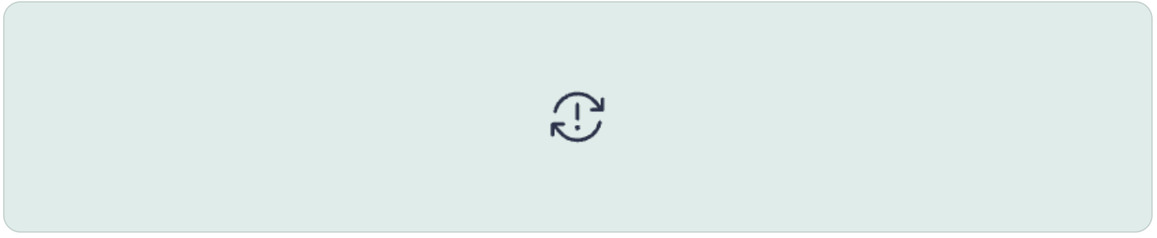
Assess Impact

Evaluate potential business consequences



Implement Controls

Apply appropriate security measures



Monitor & Review

Continuously validate effectiveness

Key Performance Indicators

100%

Security Compliance

All security requirements implemented

0

Critical Vulnerabilities

At production launch

24h

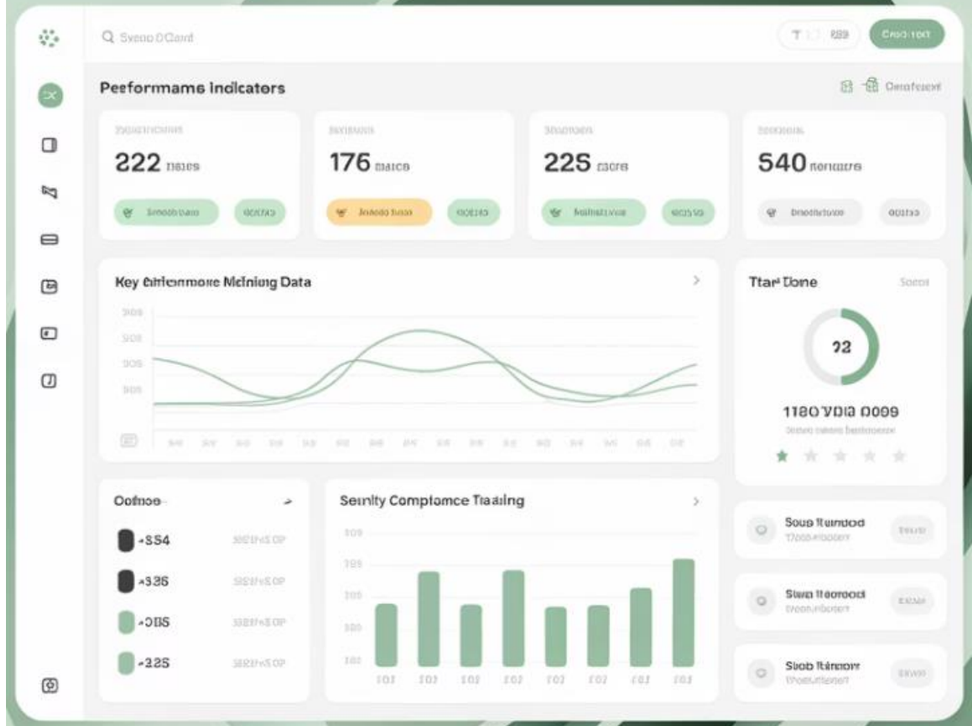
Remediation Time

For high security findings

95%

Automated Testing

Coverage of security controls



Action Steps for Project Managers

Engage Early

Include security from project inception. Don't wait until UAT or go-live.

Facilitate Communication

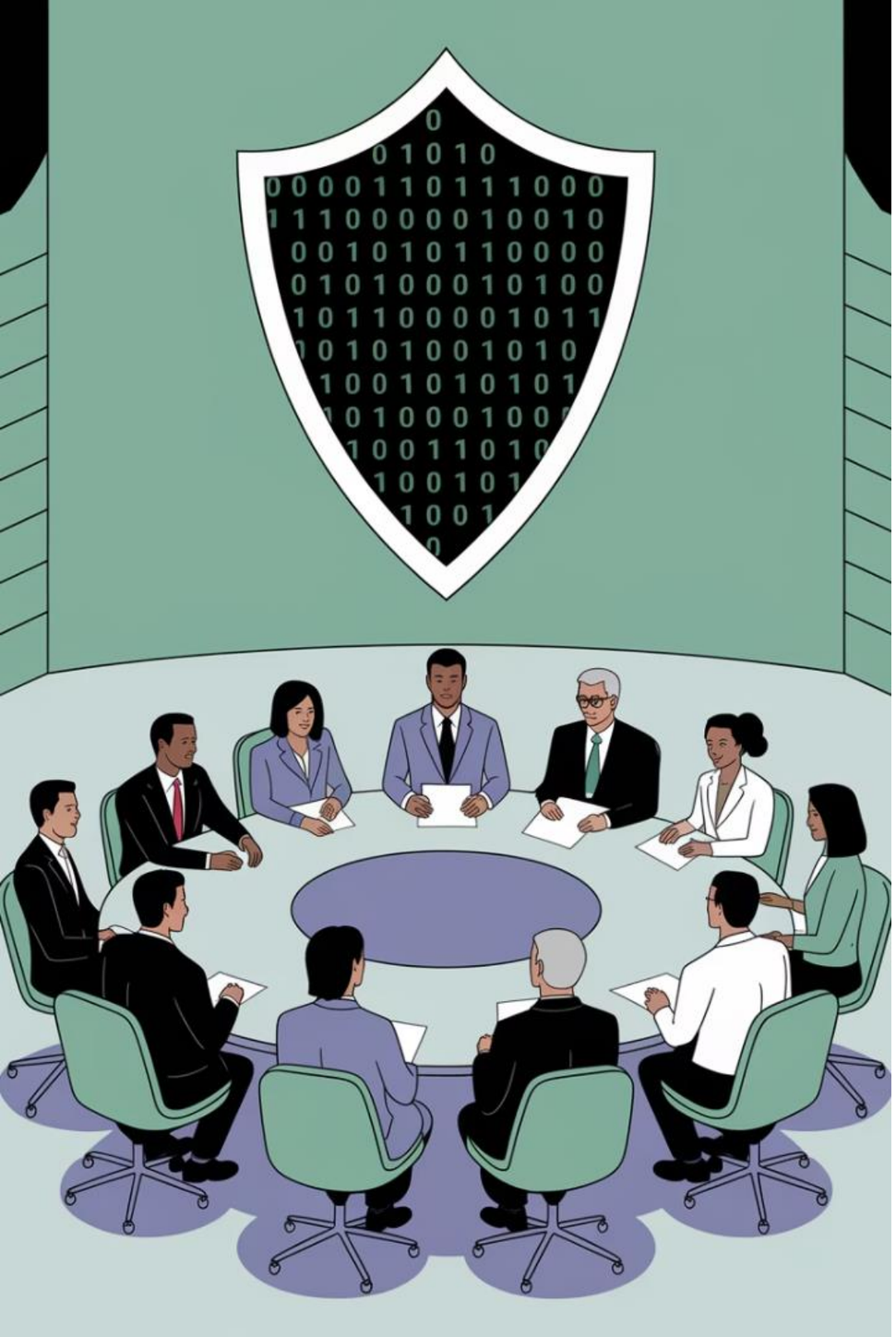
Bridge gaps between security and development teams. Ensure shared understanding.

Plan Security Gates

Integrate security milestones into project schedule. Allow time for remediation.

Educate Stakeholders

Help teams understand different security risks. Explain mitigation strategies.



Final Thoughts

Security is not a checkbox—it's a **shared responsibility** across both infrastructure and application project lifecycles. As a project manager, your role in **orchestrating communication, enforcing checkpoints, and escalating concerns** is critical to delivery and defense.