# Security Considerations for Infrastructure vs Application Projects What Project Managers Need to Know

**Published on 23 April 2025 at 14:44**

**Author: Kimberly Wiethoff**

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.

## 🛠️ 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.

🔄 *Example PM Action:* Include a security sign-off milestone before promoting any infrastructure changes to production.

## 💻 Application Security: Protecting the Code and Data

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:** Incorporate security gates in CI/CD pipelines (e.g., SAST, DAST scans).
* **Data Privacy:** Ensure encryption of data in transit and at rest, especially with PII or PHI.
* **API Security:** Authenticate and authorize integrations with OAuth, API gateways, and rate limiting.
* **User Authentication:** Use MFA, session controls, and password best practices in app design.
* **Third-Party Components:** Maintain a Software Bill of Materials (SBOM) to track vulnerabilities in open-source libraries.

🔄 *Example PM Action:* Schedule a penetration test before app launch and include results in the go-live checklist.

## ⚖️ Compare and Contrast: Security Focus Areas



## ✅ Takeaway for Project Managers

* Engage InfoSec early—**don’t wait until UAT or go-live.**
* Plan for security gates at key project milestones.
* Ensure both infrastructure and development teams are aligned on compliance requirements.
* Educate stakeholders on the different types of risks and how they’re mitigated.

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.

**#CyberSecurity #InfrastructureSecurity #ApplicationSecurity #ProjectManagement #DevSecOps #SecureSDLC #Compliance #ITPM #RiskManagement #InfosecPM**