# Managing PKI

This playbook outlines the steps for establishing and maintaining a Public Key Infrastructure (PKI), which is vital for securing communication channels and authenticating information transfers.

### Step 1: Define Policy

Establish a PKI policy that outlines the roles, responsibilities, and technical requirements. This should include the Certificate Policy (CP) and Certification Practice Statement (CPS).

### Step 2: Select PKI Model

Decide on a PKI model that fits the organization’s requirements. Options include private, public, or hybrid PKI models.

### Step 3: Implement Hierarchy

Set up a certificate hierarchy. This typically includes a root Certificate Authority (CA), with intermediate CAs for management and scalability purposes.

### Step 4: Deploy System

Deploy the PKI system, ensuring appropriate hardware, software, and network configurations.

### Step 5: Issue Certificates

Start the process of certificate enrollment, generation, distribution, and revocation as per CP and CPS.

### Step 6: Ensure Security

Enforce strong security policies like multi-factor authentication and least privilege access to protect the CA and its keys.

### Step 7: Monitor PKI

Regularly monitor the PKI infrastructure for any irregularities or operational issues.

### Step 8: Update Policy

Review and update the PKI policies, practices, and configurations routinely to adapt to new threats and technologies.

### Step 9: Plan Disaster Recovery

Implement a disaster recovery plan to restore PKI operations in the event of a failure or breach.

### Step 10: Audit Regularly

Conduct regular audits of the PKI to ensure compliance with policies and to identify areas for improvement.

## General Notes

### PKI Documentation

Maintain detailed documentation for every aspect of the PKI, which is critical for troubleshooting, training, and operational integrity.

### Legal Considerations

Stay informed about the legal requirements and considerations relevant to PKI operations and certificate issuance in your jurisdiction.