Certificate Disaster Recovery Checklist

1. Preparation Before Recovery is Needed

- [ ] Maintain an up-to-date inventory of all certificates (location, type, owner, expiration).
- [ ] Ensure encrypted backups of all certificates and private keys are created and stored securely (onsite/offsite/cloud).
- [ ] Document access credentials and recovery procedures for certificate management systems and backup storage.
- [ ] Establish relationships and contact info with all Certificate Authorities (CAs) and vendors.
- [ ] Assign DR roles and responsibilities (primary and backup personnel).
- [ ] Create a communication plan for certificate-related incidents (internal and external).
- [ ] Keep a printed and digital copy of DR plans and critical contacts in secure, accessible locations.

2. Ongoing Maintenance

- [ ] Regularly update and validate certificate inventory (e.g., monthly/quarterly review).
- [ ] Test restoration of certificates and keys from backups at least quarterly.
- [ ] Monitor certificate expiration dates and set up automated alerts (90, 30, 7, 1 day).
- [ ] Review and update DR procedures after each test or real incident.
- [ ] Conduct regular DR drills simulating certificate-related incidents.
- [ ] Keep all contact and escalation lists current.

3. Actionable Steps During a Certificate Incident

- [ ] Identify affected certificates and impacted systems/services.
- [ ] Retrieve the latest backup of required certificates and private keys.
- [ ] Restore or re-issue certificates as per documented procedures.
- [ ] Revoke compromised or expired certificates as necessary.
- [ ] Redeploy updated certificates to all affected systems and verify service restoration.
- [ ] Communicate status and next steps to all stakeholders (internal, customers, vendors).
- [ ] Document actions taken and lessons learned for future improvement.

CERTMS

Implementation Guide & Best Practices

Certificate Inventory Management

Essential Inventory Fields

- **Certificate Common Name (CN):** Primary domain or service identifier
- **Subject Alternative Names (SANs):** All additional domains/IPs covered
- **Serial Number:** Unique identifier for tracking and revocation
- **Issuing CA:** Certificate Authority name and contact information
- **Issue/Expiration Dates:** Track lifecycle and renewal schedules
- **Key Length & Algorithm:** RSA 2048/4096, ECC P-256/P-384, etc.
- **Certificate Type:** SSL/TLS, Code Signing, Email (S/MIME), Client Auth
- **Storage Location:** Server name, file path, HSM slot, or key vault reference
- **Owner/Contact:** Responsible team or individual with contact details
- **Dependent Systems:** Applications, services, and endpoints using the certificate

> **Pro Tip:** Use CertMS to automate inventory discovery and maintain real-time visibility across your entire certificate ecosystem.

Backup & Storage Best Practices

Secure Backup Strategy

- **Encryption:** Always encrypt private keys using AES-256 or stronger encryption before backup
- **3-2-1 Rule:** Maintain 3 copies on 2 different media types with 1 offsite copy
- **Access Control:** Limit backup access to authorized personnel only; implement MFA
- **Password Protection:** Use strong, unique passwords stored in enterprise password manager
- **Backup Formats:** Store in PFX/PKCS#12 (with password) or PEM format with separate encrypted key
- **Version Control:** Maintain historical versions when certificates are renewed
- **Geographic Distribution:** Store offsite backups in different physical locations

Recommended Storage Locations

- **Primary:** Enterprise key management system (KMS) or Hardware Security Module (HSM)
- **Secondary:** Encrypted network storage with restricted access
- **Tertiary:** Encrypted cloud storage (AWS Secrets Manager, Azure Key Vault, etc.)
- **Emergency:** Encrypted offline storage (external drive) in physically secure location

Testing & Validation Procedures

Quarterly DR Test Scenarios

- **Scenario 1 - Certificate Restore:** Retrieve and install a backed-up certificate on a test server; verify SSL/TLS handshake
- **Scenario 2 - Emergency Reissuance:** Request and deploy a replacement certificate within your RTO (Recovery Time Objective)

- **Scenario 3 - Mass Expiration:** Simulate multiple certificates expiring simultaneously; test prioritization and deployment
- **Scenario 4 - Compromised Certificate:** Practice revocation, reissuance, and redeployment workflow
- **Scenario 5 - Backup System Failure:** Test retrieval from secondary/tertiary backup locations

Validation Checklist

- Verify certificate chain is complete and valid
- Confirm private key matches public certificate
- Test certificate on target system (web server, application, device)
- Validate certificate is trusted by clients (browser, API consumers)
- Check certificate hasn't been revoked (OCSP/CRL check)
- Document test results and time to recovery

Incident Response Guidelines

Severity Classification

- **Critical (P1):** Public-facing services down, expired certificates blocking customer access, security breach
- **High (P2):** Internal services impacted, certificates expiring within 24 hours, compromised certificate detected
- **Medium (P3):** Certificates expiring within 7 days, non-critical service impact, backup system failure
- **Low (P4):** Routine renewals, planned maintenance, inventory discrepancies

Response Time Objectives (RTO)

- **P1 Critical:** Initial response within 15 minutes, resolution within 2 hours
- **P2 High:** Initial response within 1 hour, resolution within 8 hours
- **P3 Medium:** Initial response within 4 hours, resolution within 24 hours

- **P4 Low:** Initial response within 24 hours, resolution within 5 business days

Communication Templates

Internal Alert Example:

```
"URGENT: Certificate incident detected. [Service Name] certificate
expired at [Time]. Impact: [Customer-facing/Internal]. Severity:
[P1/P2/P3]. Response team mobilized. ETA to resolution: [Time].
Updates every 30 minutes."
```

Customer Notification Example:

```
"We are currently experiencing a service disruption affecting [Service
Name]. Our team is actively working on resolution. Expected
restoration: [Time]. We apologize for the inconvenience and will
provide updates every hour. Status page: [URL]"
```

Tools & Commands Reference

OpenSSL Quick Reference

```
# View certificate details
openssl x509 -in certificate.crt -text -noout

# Check certificate expiration
openssl x509 -in certificate.crt -noout -enddate

# Verify private key matches certificate
openssl x509 -noout -modulus -in certificate.crt | openssl md5
openssl rsa -noout -modulus -in private.key | openssl md5

# Test SSL/TLS connection
openssl s_client -connect domain.com:443 -servername domain.com

# Convert PEM to PFX
openssl pkcs12 -export -out certificate.pfx -inkey private.key -in
certificate.crt -certfile ca_bundle.crt
```

```
# Extract certificate from PFX
openssl pkcs12 -in certificate.pfx -clcerts -nokeys -out
certificate.crt
```

Monitoring & Alerting Tools

- **CertMS:** Automated certificate lifecycle management and monitoring
- **SSL Labs:** Online SSL/TLS configuration testing
- **Certificate Transparency Logs:** Monitor certificate issuance (crt.sh)
- **Nagios/Zabbix Plugins:** Certificate expiration monitoring
- **Custom Scripts:** Automated daily certificate checks and reporting

Contact & Escalation Matrix

Key Contacts Template

Role	Primary	Backup	Phone	Email
Certificate Manager	_____	_____	_____	_____
Security Team Lead	_____	_____	_____	_____
Infrastructure Manager	_____	_____	_____	_____
CA Account Manager	_____	_____	_____	_____
Executive Sponsor	_____	_____	_____	_____

Certificate Authority Contacts

- **Primary CA:** _____
  Support: _____
  Emergency: _____

- **Secondary CA:** _____
  Support: _____
  Emergency: _____
- **Internal CA:** _____
  Support: _____
  Emergency: _____

Post-Incident Review Template

Questions to Address

- What was the root cause of the incident?
- What was the timeline from detection to resolution?
- Were all affected certificates and systems identified correctly?
- Did backup and recovery procedures work as documented?
- What went well during the response?
- What could be improved for future incidents?
- Do any procedures need to be updated?
- What preventive measures can avoid recurrence?
- Were communication protocols effective?
- What training gaps were identified?

Action Items

- Document lessons learned and share with team
- Update DR procedures based on findings
- Schedule follow-up training if needed
- Implement preventive measures identified
- Update monitoring and alerting thresholds

- Review and adjust RTO/RPO objectives if necessary