Infrastructure checklist

1 Architecture

- ☐ Do you follow infrastructure as a code approach (Terraform, CloudFormation, etc)?
- ☐ Do you have infrastructure documentation? Is it up-to-date with your current infrastructure state?
- ☐ Is your infrastructure placed in a private network?
- ☐ Is your infrastructure self-recovery (instances in multiple availability zones)?
- ☐ Do you know all third-party services your application is integrated with?
- ☐ Is there any part of the application that may be a single point of failure?

2 Code

- ☐ Do you have unit/integrations/e2e/performance tests?
- ☐ Do you have CI/CD pipelines for automated testing and deployment?
- ☐ Do you have configured linter for your application code?
- ☐ Are you running linter/prettier checks for your code before commit changes/merge changes?
- ☐ Are you testing your code using static code analysis tools?
- ☐ Are you using maintained and secure versions of packages in your application?
- ☐ Are you using only industrial standards in cryptography (not your own)?

3 Monitoring

- ☐ Do you have a website monitoring service set up (Freshping, Pingdom, Downtime Monkey, etc)?
- ☐ Do you have CloudWatch / New Relic or other monitoring tools for your infrastructure set up?
- ☐ Is APM (Application Performance Monitoring) configured for all services?
- ☐ Are application logs available for viewing and retaining?
- ☐ Does the application have distributed tracing?
- ☐ Are all third-party services monitored?

4 Alerting

- ☐ Are infrastructure budget alerts configured?
- ☐ Are anomaly alerts configured?
- ☐ Are error alerts configured?
- ☐ Do you have responsible people for reacting to alerts?

5 Security

- ☐ Does the AWS root user have Two-Factor authentication enabled?
- ☐ Do all team members have Two-Factor authentication enabled on their accounts?
- ☐ Are you using automated security analysis tools?
- ☐ Is your database not accessible from the public network?
- ☐ Are you using secure storage for secrets and credentials (CI/CD secrets, Keybase, etc)?
- ☐ Does your Dockerfile have no security issues (if it is present)?
- ☐ Are the website SSL certificates updating automatically or is there a notification about certificates update?
- ☐ If you are using cloud computing instances: do the operating systems have the latest security patches installed?
- ☐ Do you know team members who have access to your infrastructure and what permissions they have?
- ☐ Do you follow the least privilege principle for user accounts?

6 Best practices

- [ ] If you are using Terraform: are you storing `terraform.tfstate` file separately from your Git repository?
- [ ] If you are using Docker: are you running an application under a non-privileged user?
- [ ] If you are using Docker: does your Dockerfile follow best practices?