Technology Audit Checklist

AgileVision

Security & Compliance

Cloud Provider

- [ ] Cloud provider administrator accounts are protected with MFA (multi-factor authentication), strong password and are not being used for the actual work.
- [ ] MFA (multi-factor authentication) is enforced for all cloud provider users.
- [ ] Password requirements policy is in place and is automatically enforced.
- [ ] Password rotation policy is in place and is automatically enforced.
- [ ] Each user has a least possible minimum of permissions defined by their job function.
- [ ] Development credentials are disposable and short-lived.
- [ ] Credentials are not shared between users.
- [ ] Inactive credentials are identified, locked and periodically removed.
- [ ] Access logs are stored for at least 90 days.
- [ ] Logs are periodically inspected.
- [ ] Log anomaly detection mechanism is configured.
- [ ] Access to internal resources from the Internet is possible only via VPN.
- [ ] Access to the production cloud account restricted to a limited set of users.

Application

- [ ] No ports except for 80 and 443 are open on Internet-facing endpoints.
- [ ] Web application firewall is configured to prevent brute-force attacks, deny access to bots and scrapers.
- [ ] Underlying environments (VMs, containers) are regularly updated to include new security fixes.
- [ ] External dependencies are being updated on the regular basis.

Scalability and Flexibility

Infrastructure

- [ ] Autoscaling is properly configured for compute resources.
- [ ] Autoscaling is properly configured for database resources.
- [ ] Load balancers are used to properly distribute requests.
- [ ] Static web resources are hosted and cached by the CDN.
- [ ] Infrastructure scalability test plans are present and being regularly executed.

Application

- [ ] Application components are containerized for simpler orchestration.
- [ ] Application components have a stateless design where possible.
- [ ] Microservice-based architecture is used.
- [ ] Load tests are present and being regularly executed.

High Availability and Disaster Recovery

Infrastructure

- [ ] Multi-region deployment is used for the database layer.
- [ ] Multi-region deployment is used for the compute layer.
- [ ] Object storage is replicated to a secondary region.
- [ ] Infrastructure availability is being monitored and automated notifications are configured.
- [ ] RTO and PTO are defined and verified.
- [ ] Cloud provider support plan covers prompt response to incidents.
- [ ] Backups are replicated to multiple regions.

Application

- [ ] Dependencies between components are defined and documented.
- [ ] Zero-downtime deployment of the backend is implemented.
- [ ] Zero-downtime deployment of the frontend is implemented.
- [ ] SLAs are defined and honored.

Cost Management

Infrastructure

- [ ] Access to billing is present.
- [ ] Cloud account inventory is being maintained.
- [ ] Consolidated billing is configured.
- [ ] Cost optimization tools are enabled.
- [ ] Unused resources are reviewed and removed.

Application

- [ ] Per-invocation calls are optimized.
- [ ] Logging can be easily turned on and off by a component and verbosity level.
- [ ] Similar calls to external APIs are properly cached.

Development and Deployment Practices

Infrastructure

- [ ] Infrastructure is described as code and versioned.
- [ ] Compute layer is immutable.

Application

- [ ] Version control systems are used.
- [ ] Code review process is in place.
- [ ] Continuous Integration is present.
- [ ] Continuous deployment is present.
- [ ] Static code analysis incorporated.
- [ ] Automated code quality checks are in place.
- [ ] Documentation is present.