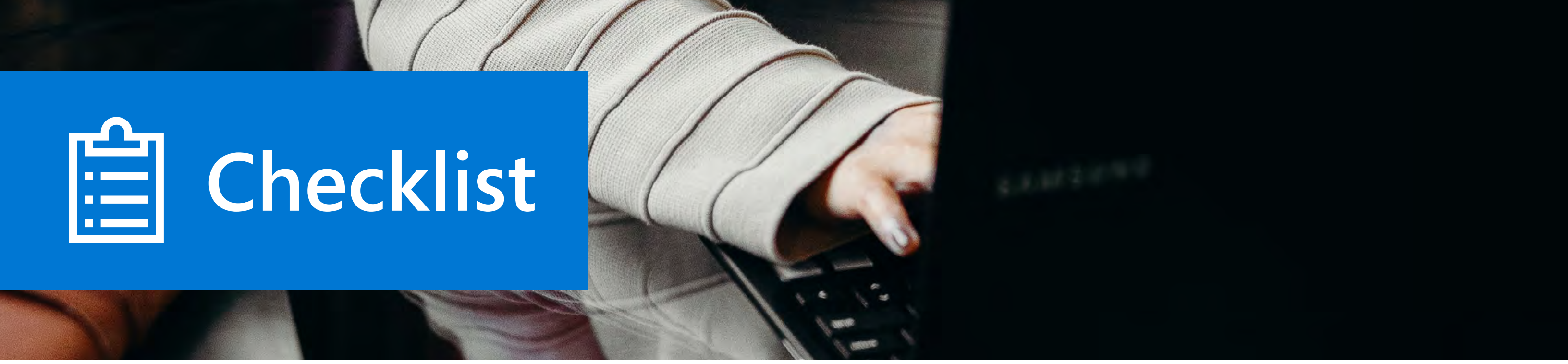

Checklist

☑ Privacy and compliance

□ Understand the responsibilities of the service provider as a data processer versus the customer responsibilities as the owner and data controller to ensure compliance on both sides.

□ Refer to the Dynamics 365 cloud service agreements and compliance documentation to understand the policies, procedures for handling data, disaster recovery strategy, data residency, encryption, and more.

☑ Identity and access

□ Establish an identity management strategy covering user access, service accounts, application users, along with federation requirements for SSO and conditional access policies.

□ Establish the administrative access policies targeting different admin roles on the platform, such as service admin and global admin.

□ Enforce relevant DLP policies and procedures to make changes or request exceptions.

□ Have necessary controls to manage access to specific environments.

☑ Application security

□ Understand the app-specific security constructs and model your security based on the native access control mechanisms rather than customizing the build.

□ Understand that hiding information from the view doesn’t necessarily remove access—there are alternate mechanisms to access and extract information.

□ Understand the impact of losing the security context when the data is exported.

□ Ensure the security model is optimized to perform and provides the foundation for further expansion and scale by following the security model best practices.

□ Have a process to map changes in the organization structure to the security model in Dynamics 365. This needs to be done cautiously in a serial way due to the downstream cascading effect.