Architecture and Build Book for Power Platform Implementation

Overview of the Project

This Power Platform implementation project is designed to enhance the operational efficiency of a federal government agency. The project leverages the comprehensive capabilities of Power Platform components such as Power Pages, Dataverse, Power Automate, and Power Apps to create a robust, secure, and scalable solution tailored to the agency's needs.

Objectives and Goals

The primary objectives include improving data management, automating workflows, and providing secure, user-friendly CRM application. Key goals are to increase productivity, ensure data security, and enhance user experience by integrating various Power Platform features seamlessly.

Scope of the Implementation

The implementation covers the deployment and configuration of Dynamics 365 Customer Service Application installed in a Dataverse environment, Power Automate for workflow automation, and Model Driven Apps for custom applications. Additionally, it includes integrations with Azure services and compliance with FINTRAC (and Federal Government)) security standards.

2. System Architecture

This section provides an overview of the system architecture, highlighting the integration of Power Platform components with Azure services. It includes detailed descriptions of each component and their interactions to ensure a cohesive and efficient implementation.

2.1 High-Level Architecture Diagram

The architecture diagram illustrates the integration of Power Platform components with Azure services. It shows how Power Pages, Dataverse, Power Automate, and Power Apps interact with Azure B2C for authentication, Azure Blob Storage for data storage, SharePoint online for attachments, and a REST API for retrieving organization data (reporting entities).

2.2 Detailed Architecture Components

This section dives into the specific components of the Power Platform and Azure services, explaining their roles and how they integrate to form a comprehensive solution.

Power Platform

- **Power Pages**: Power Pages are used to create secure, accessible web portals that integrate with Azure B2C for authentication, ensuring user data protection and compliance with federal accessibility standards.
- **Dataverse**: Dataverse serves as a centralized data storage solution that supports relational data management, advanced security, and integration with other Power Platform components. Additionally, it includes the Dynamics 365 Customer Service app to enhance customer service management.
    - **Dynamics 365 Customer Service App**: This application provides comprehensive customer service capabilities, including case management, client management, and activity tracking. It integrates seamlessly with Dataverse to offer a robust CRM system.

    - **Case Management**: Allows tracking and managing of customer service cases from creation to resolution. It supports automation of case routing and escalation to ensure timely resolution.
    - **Client Management**: Manages information about organizations and contacts, providing a 360-degree view of the client. This feature helps in maintaining detailed records of all interactions and client-related information.
    - **Activities**: Includes emails, tasks, and other activities that are tracked and managed within the system. This ensures all communications and actions related to a client or case are logged and accessible.
    - **Service Hub and Workspace**: Provides a centralized interface for customer service representatives to access all necessary tools and information. The Service Hub offers features like knowledge base integration, service level agreements (SLAs), and performance metrics to enhance service delivery.
- **Power Automate**: Power Automate enables the automation of repetitive tasks and workflows, improving operational efficiency by integrating various services and applications.
- **Power Apps**: Power Apps provide a low-code platform for developing custom applications tailored to the agency's specific requirements, enhancing user experience and productivity.

Azure Services

- **Azure B2C**: Azure B2C manages user identities and provides secure, scalable authentication for Power Pages, ensuring that user access is controlled and compliant with security policies.
- **Azure Blob Storage**: Azure Blob Storage is used to store large files and media, integrated with Power Platform to ensure efficient data handling and accessibility.
- **REST API**: The REST API extends Power Platform functionalities, allowing for custom integrations and interaction with external systems within the same Azure tenant.

2.3 Integration Points

Integration points between Power Platform components and Azure services ensure seamless data flow and interoperability. For example, data from Dataverse is accessible in Power Pages, workflows in Power Automate can trigger actions in Power Apps, and Azure B2C handles user authentication for all components.

3. Security

This section covers the security measures and configurations implemented to protect the Power Platform environment. It includes identity and access management, data security, and compliance with governance standards.

3.1 Identity and Access Management

Entra ID Integration

Entra ID integrates with the Power Platform to manage user identities, roles, and groups, providing secure access control across all components. This integration ensures that only authorized users can access specific resources and perform actions based on their roles.

3.2 Data Security

Data Security in D365 CRM

D365 CRM employs role-based access control, field-level security, and encryption to protect data. Security roles define user access to different entities, while field-level security restricts access to sensitive data fields, ensuring comprehensive data protection.

Data Security in Power Pages

Power Pages use table and column permissions to secure data, ensuring that users only access data they are authorized to see. Web API security is enforced through authentication and authorization mechanisms, providing an additional layer of protection.

3.3 Compliance and Governance

Power Platform meets federal compliance requirements by implementing robust security and governance measures. These include data encryption, regular audits, and adherence to regulatory standards, ensuring that all data and processes are secure and compliant.

3.4 Enterprise Security with Power Platform

This section elaborates on the enterprise security features of Power Platform as outlined in the white paper.

Cybersecurity Landscape

Power Platform's built-in security capabilities address the sophisticated cybersecurity challenges faced by organizations today.

Microsoft Security Foundation

Power Platform builds on Microsoft's comprehensive security foundation, leveraging products like Microsoft Defender, Microsoft Sentinel, Microsoft Entra, Microsoft Purview, Microsoft Priva, and Microsoft Intune to protect data and infrastructure.

Zero Trust Strategy

Power Platform supports a Zero Trust strategy, which includes verifying identities explicitly, using least privilege access, and assuming breach to minimize the impact of security incidents.

Security Development Lifecycle (SDL)

SDL in Power Platform involves phases such as requirements, design, implementation, verification, and release, supported by training and response activities to ensure secure application development.

4. Integrations

This section describes the various integrations between Power Platform components and external services. It explains how these integrations enhance functionality and ensure seamless data flow.

4.1 Power Pages and Azure B2C

Power Pages integrate with Azure B2C to provide secure user authentication. Azure B2C handles user registration, login, and password management, ensuring that user identities are managed securely and efficiently.

4.2 Dataverse and Power Pages

Dataverse integrates with Power Pages to provide a seamless data management experience. Data stored in Dataverse is accessible through Power Pages, enabling dynamic content display and data-driven applications.

4.3 SharePoint Online Integration

SharePoint Online integrates with Power Platform to manage documents and synchronize data. This integration allows users to store, share, and collaborate on documents within Power Apps and Power Pages, enhancing productivity and collaboration.

4.4 Azure Blob Storage Integration

Azure Blob Storage integration enables Power Platform to handle large files and media efficiently. Data stored in Blob Storage is accessible through Power Apps, Power Automate, and Power Pages, ensuring seamless data handling and retrieval.

4.5 Email Sync and Integration

Email integration with Power Platform allows for synchronized communication and data exchange. Power Automate workflows can trigger email notifications, while Power Apps can read and send emails, ensuring seamless integration with email systems.

4.6 REST API Integration

REST APIs extend the capabilities of the Power Platform by enabling custom integrations with external systems. APIs allow for data exchange, triggering workflows, and extending functionality beyond the built-in features of Power Platform.

5. SSL Configuration and Custom Domain for Power Pages

This section explains how to configure SSL and custom domains for Power Pages, ensuring secure communication and personalized access.

5.1 SSL Configuration

SSL configuration for Power Pages ensures secure communication between users and the web portal. By enabling SSL, all data transmitted between the user and the server is encrypted, protecting it from unauthorized access.

5.2 Custom Domain Configuration

Custom domain configuration allows Power Pages to be accessed through a personalized URL, enhancing the branding and accessibility of the web portal. This involves DNS settings and domain verification processes.

6. Licensing

This section provides an overview of the licensing options for Power Pages and Dataverse, ensuring that the implementation is cost-effective and scalable.

6.1 Power Pages Licensing

Power Pages licensing includes options for different subscription levels, providing flexibility based on the agency's needs. Licensing covers user access, storage, and additional features, ensuring that the implementation is cost-effective and scalable.

6.2 Dataverse Licensing

Dataverse licensing, particularly in the context of D365 Customer Service, includes various tiers based on data volume and user access. This ensures that the agency can choose a licensing model that meets its data management and budgetary requirements.

7. Backup Process and Strategy

This section outlines the backup and disaster recovery strategies to ensure data protection and business continuity.

7.1 Data Backup

The data backup strategy for Power Platform involves regular backups, retention policies, and the use of Azure Backup services. This ensures that data is protected against loss and can be restored in case of failure.

7.2 Disaster Recovery

The disaster recovery plan includes Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) to minimize downtime and data loss. Regular testing of the disaster recovery plan ensures readiness in case of an actual disaster.

8. Data at Rest using Customer Managed Keys (CMK) for Dataverse

This section explains the use of Customer Managed Keys (CMK) for encrypting data at

rest in Dataverse, enhancing data security and control.

8.1 Overview of CMK

Customer Managed Keys (CMK) provide enhanced data security by allowing the agency to manage its own encryption keys. This ensures that data at rest in Dataverse is protected and that the agency retains control over key management.

8.2 CMK Configuration

Configuring CMK involves setting up key vaults in Azure, assigning encryption keys to Dataverse, and managing key rotation policies. This ensures that data encryption is robust and compliant with security standards.

9. User Security & Access

This section details the security measures and access controls for both internal and external users, ensuring secure access to the Power Platform components.

9.1 Internal Users

CRM Security Features

- **Security Roles**: Define user access to various entities and functionalities in D365 CRM. Roles are configured to ensure that users can only access data and perform actions necessary for their job functions.
- **Column Permissions**: Restrict access to specific data fields within entities. This ensures that sensitive information is only accessible to authorized users.

- **Teams and Entra ID Group Integration**: Integration with Entra ID groups and the use of teams in CRM allows for efficient management of user permissions and collaboration.

Entra ID Integration

Entra ID integrates with the Power Platform to manage internal user identities, roles, and groups. This integration ensures that only authorized users can access specific resources and perform actions based on their roles.

9.2 External Users

Power Pages User Security Features

- **Table Permissions**: Control access to entire tables of data in Power Pages, ensuring that users only see the data relevant to their role.
- **Column Permissions**: Provide fine-grained access control to individual data fields in Power Pages. This ensures that sensitive information is protected.
- **Web API Security**: Enforces authentication and authorization mechanisms to control access to data and operations through the API.

10. Power Pages Security

This section describes the security measures implemented in Power Pages to protect data and ensure secure operations.

10.1 Table Permissions

Table permissions in Power Pages control access to entire tables of data, ensuring that users only see the data relevant to their role. This enhances data security by restricting access based on user roles and permissions.

10.2 Column Permissions

Column permissions provide fine-grained access control to individual data fields in Power Pages. This ensures that sensitive information is protected, and only authorized users can view or edit specific columns.

10.3 Web API Security

Web API security in Power Pages involves authentication and authorization mechanisms to control access to data and operations. This ensures that API calls are secure and that only authorized applications can interact with the data.

10.4 IP Restrictions

IP restrictions in Power Pages allow limiting access to the application based on IP addresses. This feature helps ensure that only users from specified IP ranges (e.g., internal network) can access the development and staging environments, while the production site remains publicly accessible.

10.5 Entra ID Integration

Entra ID is used to scope access to Power Pages, ensuring that only users within the internal domain and network have access to non-production environments, while the production site can be accessed publicly.

11. Power Platform Environment Management

This section details the management of Power Platform environments, including descriptions of each environment and their configurations. Managed environments ensure that all critical issues are addressed, and Data Loss Prevention (DLP) policies are enforced.

11.1 Environment Overview

Environments are containers where you can store and control Power Platform resources, such as apps, automations, and connections. They help protect resources and data from unauthorized access and are tied to a geographic location, which can help comply with data location requirements. Each environment can have only one Dataverse database. Environments help apply detailed security controls, such as complex business application security models.

11.2 Environment Types

Different types of environments can be created to manage Power Platform resources according to security, compliance, governance, and user needs:

- **Default**: All new users can create resources in this environment.
- **Developer**: Personal environments only for the owner’s use.
- **Dataverse for Teams**: Linked to a specific team the first time an app is installed or created in it.

11.3 Environment Management

Steps to manage environments include:

- Assigning admins to Power Platform and Dynamics 365 roles.
- Restricting creation of new environments.
- Establishing a process for users to request new environments.
- Using security groups to protect environments.
- Establishing DLP policies at both the tenant and environment level.
- Minimizing the use of the default environment by using environment routing.
- Using environment groups and rules to apply settings to many environments at once.

11.4 Environment Table

A table listing all environments with details such as name, purpose, B2C app registration ID, SharePoint subsite, Blob Storage URL, Power Pages site URL, Dataverse URL, Entra ID group, and GIT branch in DevOps.

Environment	Purpose	B2C App Registration ID	SharePoint Subsite	Blob Storage URL	Power Pages Site URL	Dataverse URL	Entra ID Group	GIT Branch
Dev	Development	[B2C App ID]	[SharePoint URL]	[Blob Storage URL]	[Power Pages URL]	[Dataverse URL]	[Entra ID Group]	dev
Staging	Staging	[B2C App ID]	[SharePoint URL]	[Blob Storage URL]	[Power Pages URL]	[Dataverse URL]	[Entra ID Group]	staging
QA	QA	[B2C App ID]	[SharePoint URL]	[Blob Storage URL]	[Power Pages URL]	[Dataverse URL]	[Entra ID Group]	qa
UAT	User Acceptance Testing	[B2C App ID]	[SharePoint URL]	[Blob Storage URL]	[Power Pages URL]	[Dataverse URL]	[Entra ID Group]	uat
Release	Release	[B2C App ID]	[SharePoint URL]	[Blob Storage URL]	[Power Pages URL]	[Dataverse URL]	[Entra ID Group]	release
Prod	Production	[B2C App ID]	[SharePoint URL]	[Blob Storage URL]	[Power Pages URL]	[Dataverse URL]	[Entra ID Group]	main

11.5 Managed Environments

Managed Environments is a set of premium features that you can turn on in an environment to make it easier to manage at scale. When you turn on Managed Environments, you can use the premium governance and security features of Power Platform to get more visibility and control with less effort. Managed Environments isn’t a separate license. It’s an entitlement that’s included in the standalone Power Platform licenses. Managed Environments is turned off by default. When you turn it on, you unlock several security and compliance features, such as:

- Limit sharing
- Data policies
- IP firewall
- IP cookie binding
- Customer-managed keys

- Lockbox
- Data loss prevention policies for desktop flows
- Extended backups
- Solution checker enforcement

11.6 Environment Groups

When you activate Power Platform in your organization, you can create different environments for different purposes. You might want to group some environments together and apply the same rules to them. Environment groups allow you to place environments into logical groups and apply a common set of rules. This feature helps maintain consistency and security for environments.

11.7 Environment Strategy

You should have a strategy for how to create and manage your Power Platform environments. Your strategy should meet both security and compliance requirements and operational and administrative needs. It should support the application lifecycle management (ALM) processes of the different solutions you build on Power Platform. Key steps include:

- Assigning admins to Power Platform and Dynamics 365 roles.
- Restricting creation of new environments.
- Establishing a process for users to request new environments.
- Using security groups to protect environments.
- Establishing DLP policies at both the tenant and environment level.
- Minimizing the use of the default environment.
- Using environment groups and rules to apply settings to many environments at once.
- Using pipelines to automate and control the promotion of resources from development to other environments.

12. SDLC / ALM Using Azure DevOps

This section outlines the software development lifecycle (SDLC) and application lifecycle management (ALM) practices using Azure DevOps.

12.1 Azure DevOps Overview

Azure DevOps provides tools for managing the Software Development Lifecycle (SDLC) and Application Lifecycle Management (ALM). It integrates with Power Platform to facilitate version control, build automation, and continuous integration and deployment (CI/CD).

12.2 GIT Repositories

GIT repositories in Azure DevOps enable version control and collaboration on code and configurations. This ensures that changes are tracked, and multiple developers can work on the project simultaneously.

12.3 Pipelines

CI/CD pipelines in Azure DevOps automate the build, test, and deployment processes. This ensures that updates to Power Platform components are consistently and reliably deployed across development, staging, and production environments.

12.4 Solutions Management

Solutions management involves using unmanaged solutions for development and managed solutions for non-development environments. This approach ensures that

development changes are tested and validated before being deployed to production, reducing the risk of issues.

12.5 App Users and App Registrations

App users and app registrations in Entra ID ensure that service accounts are used for Power Automate flows and deployments. This enhances security by controlling access and ensuring that automated processes are executed with appropriate permissions.

13. Monitoring and Maintenance

This section details the monitoring and maintenance procedures to ensure optimal performance and reliability of the Power Platform.

13.1 Performance Monitoring

Performance monitoring involves using tools and metrics to track system performance, ensuring optimal operation and quick issue resolution. Regular monitoring helps identify and address performance bottlenecks.

13.2 Maintenance Procedures

Maintenance procedures include regular updates, patch management, and system health checks. These procedures ensure that the platform remains secure, up-to-date, and reliable.

14. Documentation and Training

This section outlines the documentation and training resources available to end-users and administrators, ensuring effective use and management of the Power Platform.

14.1 User Guides

User guides provide detailed instructions for end-users on how to effectively use Power Platform features and functionalities. These guides help users navigate the system and maximize its benefits.

14.2 Administrator Guides

Administrator guides offer comprehensive configuration and administration instructions for system administrators. These guides include best practices for managing and maintaining the platform.

14.3 Training Programs

Training programs include schedules, materials, and ongoing support resources to ensure that users and administrators are well-versed in using and managing the Power Platform. These programs help build proficiency and ensure successful adoption.

15. Appendices

This section includes additional resources, definitions, and change logs to support the implementation and ongoing management of the Power Platform.

15.1 Glossary

The glossary includes definitions of key terms and acronyms used throughout the document, providing clarity and reference for readers.

15.2 References

References list documents and resources that provide additional context and information related to the implementation. This section includes links and citations to supporting materials.

15.3 Change Log

The change log maintains a record of changes and updates to the document, ensuring transparency and traceability of modifications. This helps track the evolution of the document over time.

15.4 Configuration of Power Platform Tenant and Dataverse Environments

This section provides detailed descriptions of the configuration steps for the Power Platform tenant and setting up multiple Dataverse environments for development, testing, and production. It ensures a consistent and structured setup process.