POWER PLATFORM GOVERNANCE

IRS Operational Governance Guidelines

Abstract

This document will provide an overview of how the IRS Power Platform Team plans to operate to ensure a high level of governance over the environment with a cyclical approach to ensuring long-term health and modernization of the IRS Power Platform Environment.

Guynes Daniel M (Contractor)
[Email address]

Power Platform Governance

Table of Contents

Table of Figures

Document Revision History

Editor	Date Edited	Comments
Daniel Guynes (contractor)	1.17.2025	Initial document creation
Daniel Guynes (contractor)	7.31.2025	Updated information across the document. Added the Summary of Regulations section as a bulleted governance reference that may be applied to the IRM.

References

Document or Site
Instructions for Power Platform Environments.docx

Power Platform Governance

Purpose

The purpose of this document is to define the governing responsibilities and tasks to be performed by the Power Platform Team (PPT) to maintain a healthy, up to date Power Platform environment. Furthermore, the intent of this document is to provide the operational model of the PPT to ensure continued success in governance currently and into the future.

In this document the Power Platform environment is meant to include Power Apps, Power Automate, and Power BI.

Commented [DL1]: Is this used other places, such as in Microsoft the "PPT" acronym?

Commented [DG2R1]: This is not official. I use this term all the time in conversation and context, and it provides me with an easy acronym.

Power Platform Governance

Summary

The PPT will operate in an Agile methodology, implementing SCRUM with 2-week Sprints to ensure that the PPT is administering the governance laid out in this document. We will use MS Project to implement a Sprint templated project plan. Using the Kanban boards available (built into the template), the PPT will run the two-week sprints in traditional Agile style including a Planning Session at the start of each Sprint, a Retrospective and Review at the end of the Sprint, and a Backlog Grooming near the end of the Sprint.

While all of IRS employees and IRS approved contractors are our customers, our PPT management and M365 management are our stakeholders.

Finally, the PPT will provide expert service to our customer base through Service Now tickets entered by IRS customers regarding the Power Platform environment. This includes but is not limited to:

- Environment creation and amendment.
- Continuous Integration / Continuous Delivery (CI/CD) Pipeline creation and amendment.
- Necessary manual Solution deployment.
- Security Group creation and amendment.
- Power Platform and Pipeline education and instruction.
- Troubleshooting deployment issues.
- Verification and validation of solutions.

Governance Policies

The IRS Power Platform Team will utilize the Microsoft provided template for Power Platform Governance and implement it according to this section.

Governance Dashboard

Using the CoE Starter Kit from Microsoft, the IRS PPT will maintain watch over the Power Platform's governance using a combination of the CoE BI Dashboard and the CoE Power Platform applications.

The CoE Power BI Dashboards provide a real-time glimpse into all core elements of Power Platform, and the CoE Power Platform applications provides the PPT the ability to fix or further identify governance issues.

Both CoE's should be updated quarterly to maintain a modern version to keep pace with the changes and enhancements offered by Microsoft, and to ensure that as the Power Platform changes regularly under Microsoft's development, our Power Platform Team maintains the tools to meet and govern those changes.

Environment Strategy

Guidelines for Creating Environments

The IRS PPT will use Service Now (a.k.a. IR Works) to provide IRS users the ability to request new Environments. Service Now forms will be created specifically for Environment Requests, which will provide specific questions regarding the intent and the content for the need for a new Environment.

Guidelines will be made available via the IRS Power Platform SharePoint Site pages to assist users in how to fill out the Service Now Power Platform Environment request, as well as definitions of the different environment types (Sandbox, Test, and Prod)

Guidelines for Administration of Environments

A guideline document (XXX) is available to all Power Platform Team Admins and provides step by step details and processes for implementation, maintenance and governance of Environments.

Commented [DL3]: *** IRS does **not** do Agile. WBS is by definition Waterfall.

e.g. if we can't adhere to 2 week deadline then we are not Agile.

Commented [DG4R3]: It is true IRS does not do Agile despite saying in many cases that they want to do it. However, I did create an Agile scrum process for our PPT group. However, generally speaking only myself and Sam really held ourselves accountable to it. I think it the right way to go, but we need a buy in from the PPT. We can still implement Agile with a WBS so long as the WBS is not the only driving source.

Commented [DL5]: We need to discuss this and make sure we can commit to 2-weeks.
Are we even doing sprints or SCRUM?
BU will be submitting IRWorks tickets.

PPT is Power Platform Team - which s our team, not the Enterprise or other BUs.

Commented [DL6R5]: *** we can't be devoted to (Agile) if we have many other ad hoc tasks. 🤔🤔🤔

Commented [DG7R5]: Agile was not including IRWorks tickets such as Environment, security groups requests. Those are daily items that are part of normal daily processes. The Agile process was more defined for project level items, su...

Commented [DL8]: IRWorks is ServiceNow

Commented [DL9]: Don't' have CI/CD now.
All other bullet points below seem fine.

Commented [DL10R9]: We, PPT, aren't fully aligned with Pipelines.

Commented [DG11R9]: Agreed - we do not have this yet, but the governance document must take into account ...

Commented [DL12]: Is Dashboard visible to end-users or only PPT team? ...

Commented [DL13R12]: Rishabh - what PPT Admins can do? ...

Commented [DG14R12]: Currently I believe only PPT has access. Where possible, we should make dashboards ...

Commented [DL15]: What is BI Dashboard? Same as above?

Commented [DL16]: Don't mention ServiceNow - use IRWorks.

Commented [DL17]: We should have link to other resources like Power Platform SharePoint site. ...

Commented [DG18R17]: Most of this information is loosely defined in the site. However, it is fragmented and ...

Commented [DL19]: This is same as Development, Test and Prod. ...

Commented [DG20R19]: Please expand on this. What Teams apps are you referring to, and what level of ...

Commented [DL21]: Two versions
1st Dev / Sandbox Environment. ...

Power Platform Governance

Process for Requesting New Environments

Requests for new Environments come from Service Now (IR Works) through filling out a form specific for Environment Requests.

The Service Now request may be found here: M365 Power Platform Services - Employee Center

Strategy for managing Teams Environments

IRS currently will not be providing Teams Environments to the IRS

Set up capacity soft limit for each environment

IRS currently has no soft-limit for environment sizes.

The PPT will maintain environment size oversight using the COE.

** ISSUE ** Currently there is no policy in place regarding environment audit logs, and how long environment audit logs will be maintained. The audit logs tend to be the largest aspect of most environments. PGLD, Cybersecurity, and Data Retention groups should be involved in this governance item.

Commented [DL22]: e.g. apps can be deployed to Microsoft Teams - also whether we allow or not.
q.v. Teams Admin Center.

Per Environment - there is a setting for Teams-enabled. *** Not an option at IRS.

Commented [DG23R22]: Per Craig, we were not supporting Teams Environments. If we are, then we need to work with Teams group to get clarity on how they want this to happen.

Data Loss Prevention (DLP) Policies

Defining Connectors for each Environment

Connectors are defined for each Environment through the use of Data Policies, where connectors may be associated with each Data Policy. The PPT has put together 4 core Data Policies for Environments as follows:

- **Baseline**: All Environments are added to this Data Policy by default. This policy consist only of IRS approved non-premium connectors.
- **Default Plus Dataverse**: This is for all Environments that need the default connectors from the Baseline policy plus Dataverse, which has a premium license requirement.
- **SQL Plus Dataverse**: This is for all Environments that require the Baseline Connectors, Dataverse and a SQL premium connector.
- **Oracle Plus Dataverse**: This is for all Environments that require the Baseline Connectors, Dataverse and a SQL premium connector.
- **Other**: There are other Data Policies defined that are for unique premium connector requirements, or for customer Connectors that have been approved by IRS Cybersecurity and privacy.

Commented [DL24]: ?? Do we use SQL Plus or Oracle - with Dataverse or M365 / Power Platform??

Commented [DG25R24]: Yes we use and support SQL, Oracle, and I believe Sam has set up a PostgreSQL

Process for defining newly created Environments DLP

The PPT will meet to discuss the creation of new Data Policies when unique requirements that do not fit current Data Polices has been made and approved by proper authorities. If it is deemed that a new Data Policy is required a new Data Policy will be created in the Power Platform Admin Center by the PPT.

Process to update existing DLP Policies safely without impacting end users

The PPT will meet to discuss the amendment of an existing Data Policy if there is an effort to do so is brought up by a member of the PPT.

Process for Requesting New Connectors for Policies

Currently there is no specific format for requesting new connections for existing Data Policies. However, IRS users have used Service Now (IR Works) to request assistance with data connectors that are not readily available by default.

Security

Cross tenant isolation

This has been disabled at the Tenant level to ensure that IRS tenant is isolated and secure.

Power Platform Governance

Conditional Access Policies

Currently there are no conditional access policies in place for Power Platform Environments. Only IRS employees, IRS contractors, or special IRS credentialled personnel (i.e. Treasury, etc.) have access to the IRS tenant, and the IRS Power Platform environment.

Controlling Environment creation

Environment creation is limited to Power Platform Administrators and Global Admins (who have unlimited access across the tenant).

Security groups for each environment

Security Groups will be implemented via Microsoft Entra Admin Center by Power Platform Administrators.

Entra Security Groups will be created in the Microsoft Entra Admin Center and then attached via Teams within the Environments to implement role-based security per Environment.

Process for requesting user access into QA/Prod

When creating a Test (QA) or Production environment, the users will also request separate Entra Security Group requests via Service Now (IR Works). These Service Groups will be assessed by the PPT and implemented appropriately to the environment it is requested for.

By default, Security Groups are created for each Environment type as follows:

- Sandbox :
  - Maker Group
  - Admin Group
  - User Group
  - Pipeline Group (Optional)
- Test :
  - User Group
  - Pipeline Group (Optional)
- Production
  - User Group
  - Pipeline Group (Optional)

Additional Security Groups for custom Security Roles or other reasons are submitted to the PPT through Service Now (IR Works) requests and are assessed by the PPT for pertinence and security.

Strategy for managing guest user access

All Entra Security Groups created by the PPT will provide ownership to the IRS owners of the environment to allow for self-regulation of access to the environment for which the group is attached. Privacy and cyber security is a responsibility for all parties, and while the PPT reviews and works with IT Cyber and IT Privacy to support and approve Solution architecture and Environment requests, the IRS owners of the environment and solutions are responsible for managing access to their environment and being IRS employees or approved contractors, they have gone through the appropriate cyber awareness and privacy training.

License Management

Licensing is handled at the Entra Security Group level and not attached to individuals.

Currently, licensing is monitored regularly by the PPT, but licensing is assigned by another group.

Decide the License requirement to kick start your Power Platform Adoption

The license requirements for the IRS Tenant for Power Platform are controlled by a separate group within IRS and are maintained by that same group. An agreement between Microsoft and the IRS has been made to provide:

Commented [DL26]: ?? What are details for Conditional Access Policies.
➡️ Need more links to cross reference other documentation - including Microsoft.

Commented [DG27R26]: This empty as this is something I am not sure about but as part of the Microsoft Governance. This setting I believe is part of the Admin Settings for Power Platform Admin.

Commented [DL28]: Who are all the Global Admins? They can help solve other problems for us.
What is the channel used to contact Global Admins?

Commented [DG29R28]: I have no idea who Global Admins are (just know they exist), and we do NOT want them helping us unless they are tasked to do so. The Power Platform Team should be the only people doing anything with Power Platform Administration - otherwise there is a cross purpose issue and potential issues.

Commented [DL30]: 💚 This is same as Development Environment (IRS defined).

Commented [DG31R30]: Yes - but we use Sandbox because there is a "Developer" environment … and we are not providing those to IRS customers.

Power Platform Governance

- A specific amount of premium Power Platform licenses.
- All IRS employees and IRS Contractors with proper login credentials have basic default

Define a process for the users to request new license

The process to request a new license is not controlled by the Power Platform Team. This process is a separate process run by the IRS security team.

Users have the ability to log into IR Works (Service Now) or BEARS to request M365 related licenses.

App and Flow Management

Define App Classification criteria to decide which environment they will go to.

Set up App Compliance Process

Set up Inactive App/Flow Management Process

Set up orphaned App/Flow Management process

Define process for requesting new Enterprise App, promote an App to a different environment

Application Lifecycle Management

Define your Application Lifecycle Management Strategy

Monitoring and Analytics

Monitor your Platform in a regular basis to make sure nothing is going beyond as expected

The PPT shall utilize the Power Platform COE

Process for Setting up Auditing

Auditing is turned on by default when environments are created.

Developer Guidance, Upskilling, Communication and Support Plan

Create Developer guideline document with standards and best practices. Set up training sessions if needed.

Create a website with all Power Platform quick reference materials

Create a support model for supporting both developers and end users

Have a plan for Administrative tasks

Communication Plan

Commented [DL32]: Where is this documented? What criteria?

Commented [DG33R32]: This is loosely defined by Craig and exists in the M365 Central Power Platform site pages, but needs to be better defined and re-written.

Commented [DL34]: TODO - we need to define app compliance, inactive / orphaned artifacts and ALM strategy.

Commented [DG35R34]: Much of this can be maintained or tracked through COE

Commented [DL36]: 🔗 Web site for quick reference

Commented [DG37R36]: Should be part of the M365 Central Power Platform site pages. There is some limited stuff there now via Craig.

Power Platform Governance

SUMMARY OF REGULATIONS

Environments:

Support:

- Development (Sandbox) Environments
- Test (Production) Environments
- Production (Production) Environments

Unsupported:

- Trials (extra payment required)
- Development (under investigation)
- Teams Environments

Governance

- All requests for environments must have an official request from the IRS Ticket system (currently IRS Works (Service Now)).
    - A request for a Dev environment shall be a request for a Dev and Test environment.
    - A request for a Prod environment shall require the submission and approval of the System Architecture document.
    - All environments shall follow a naming convention as follows:
        - <BU>-<ShortProjectName>-Dev
        - <BU>-<ShortProjectName>-Test
        - <BU>-<ShortProjectName>-Prod
        - The <ShortProjectName> shall be agreed upon by the requesting group and the PPT.
        - The <BU> shall be agreed upon by the requesting group and the PPT.
- All Dev environments shall be Sandbox environments.
    - Dev environments shall NOT be managed
    - Dev environments may contain Dataverse
    - Dev environments may contain Premium or Custom Connectors
    - In a Dev environment, requests for Premium or Custom Connectors must be approved by (Security Change Management (?) group)
    - Dev environments shall have their own Entra Groups associated with it that do not cross over into other environments with the following exceptions:
        - PP Tenant Admins (PPT Admins)
        - Pipeline Deployment group (see Environment Security for more information)
- All Test environments shall be Production environments
    - Test environments shall be managed
        - Solution checker enforcement shall be set to ***Block***
        - "*Send emails only when a solution is blocked. If unchecked, you will also get emails when there are warnings*" should be left ***unchecked***
    - Test environments may contain Dataverse
    - Test environments may contain Premium or Custom Connectors
    - In a Test environment, requests for Premium or Custom Connectors must be approved by (Security Change Management (?) group)
    - Test environments shall have their own Entra Groups associated with it that do not cross over into other environments with the following exceptions:
        - PP Tenant Admins (PPT Admins)
        - Pipeline Deployment group (see Environment Security for more information)
- All Prod environments shall be Production environments

Commented [DL38]: ?? Do we (at all) allow Trials, Development and Teams Environment types?

Commented [DG39R38]: We are not allowing any of these unless higher ups override that initial decision. Trials really do not provide anything that we want. Developer environments could be used but are limited and may cause more problems. Teams Environments are not something we have supported since Craig, and I do not see us changing.

Power Platform Governance

- A Prod environment request may not be approved without a reviewed and approved System Architecture document for the first Solution to be used in the Production environment.
- Prod environments shall be managed
  - Solution checker enforcement shall be set to ***Block***
  - "*Send emails only when a solution is blocked. If unchecked, you will also get emails when there are warnings*" should be left ***unchecked***
- Prod environments may contain Dataverse
- Prod environments may contain Premium or Custom Connectors
- In a Prod environment, requests for Premium or Custom Connectors must be approved by (Security Change Management (?) group)
- Prod environments shall have their own Entra Groups associated with it that do not cross over into other environments with the following exceptions:
  - PP Tenant Admins (PPT Admins)
  - Pipeline Deployment group (see Environment Security for more information)

Environment Security

Support:

- Development (Sandbox) Environments
- Test (Production) Environments
- Production (Production) Environments
- Pipelines

Unsupported:

- The PPT shall not support individual security
- The PPT is not responsible for Dataverse security or the roles associated with Dataverse.

Commented [DL40]: ?? Do we (at all) allow Trials, Development and Teams Environment types?

Commented [DG41R40]: We are not allowing any of these unless higher ups override that initial decision. Trials really do not provide anything that we want. Developer environments could be used but are limited and may cause more problems. Teams Environments are not something we have supported since Craig, and I do not see us changing.

Governance

- All requests for Security groups (Entra Groups) must have an official request from the IRS Ticket system (currently IRS Works (Service Now)).
  - Dev Environment Security
    - They may request to have a Security group assigned to the Environment with the following requirements:
      - The members of the Power Platform Team must be included as part of the group for debug and support purposes
    - They may have:
      - 1 Admin Group
      - 1 Developer Group
      - 1 or more User groups
        - A User group may be generic, or for a specific custom Security Role related to Dataverse.
      - 1 Pipeline Group (only available when they request pipelines)
        - ** NOTE this is the same Pipeline Group as Dev and Prod
  - Test Environment Security
    - They may request to have a Security group assigned to the Environment with the following requirements:
      - The members of the Power Platform Team must be included as part of the group for debug and support purposes
    - They may have:
      - 1 or more User groups

- A User group may be generic, or for a specific custom Security Role related to Dataverse.
- 1 Pipeline Group (only available when they request pipelines)
  - ** NOTE this is the same Pipeline Group as Dev and Prod

- Prod Environment Security
  - They may request to have a Security group assigned to the Environment with the following requirements:
    - The members of the Power Platform Team must be included as part of the group for debug and support purposes
  - They may have:
    - 1 or more User groups
      - A User group may be generic, or for a specific custom Security Role related to Dataverse.
  - 1 Pipeline Group (only available when they request pipelines)
    - ** NOTE this is the same Pipeline Group as Dev and Prod
- Pipeline Security
  - They may have:
    - 1 Pipeline User group
    - This Pipeline user group will reside on all three of their pipeline environments (Dev, Test, Prod) – this is the only security group that may be used in multiple environments.
    - This security group is only for the use in a single environment group (dev, test, prod) but not across multiple environment groups.

Solutions

Support:

- Managed Solutions
- Unmanaged Solutions (in specific circumstances)

Unsupported:

- We do not support the movement of individual objects (i.e. Apps, Flows, Connectors, etc.) unless it is in the process of fixing a broken solution.
- We do not support the movement, ingestion, or editing of any solution from a source external to IRS unless approved by Cyber security and the Security Change Management Board.

Governance

- All objects to be moved from one Environment to another, must be in a Solution
- A Solution must have a single purpose, unless agreed upon by the users and the Power Platform Team.
- All objects passed between environments shall exist within a Solution unless specific requirements deem it necessary.
- To move custom Security Roles between Environments, a specific solution must be created for Security Roles to be moved by the PPT.
  - This will require coordination between the user group and the PPT.
- To move Data Flows between Environments, a specific solution must be created for Data Flows to be moved by the PPT
  - This will require coordination between the user group and the PPT.

Commented [DL42]: ?? Do we (at all) allow Trials, Development and Teams Environment types?

Commented [DG43R42]: We are not allowing any of these unless higher ups override that initial decision. Trials really do not provide anything that we want. Developer environments could be used but are limited and may cause more problems. Teams Environments are not something we have supported since Craig, and I do not see us changing.

Power Platform Governance

Pipelines

Support:

- Pipelines are created for a single Dev environment to a single Test environment to a single Prod environment (i.e. Dev to Test to Prod)

Unsupported:

- Multiple Pipelines from a single Development environment.
- Pipelines from the Personal Productivity environment.

Governance

- All requests for Pipelines must have an official request from the IRS Ticket system (currently IRS Works (Service Now)).
- Pipelines must be set up by a member of the PPT.
- Pipeline name should be in the same format of Environments: <BU>-<ShortProjectName>-Pipeline
- Deployment step should be generic for all Pipelines as follows:
    - For Dev to Test the Deployment name should be: Dev → Test
    - For Test to Prod the Deployment name should be: Test → Prod
- The <BU>-<ShortProjectName>-Pipeline group should be the only group associated to deploy the

Power Platform Management Settings

- Solution checker enforcement for Managed Environment should be set to ***Block*** for both Test and Production environments.
    - This will cause the deployment to fail ONLY when a 'critical' item check is encountered and fails. For all other levels (High, Medium, Low) it will still deploy.
    - Uncheck "Send emails only when a solution is blocked. If unchecked, you will also get emails when there are warnings."

Commented [DL44]: ?? Do we (at all) allow Trials, Development and Teams Environment types?

Commented [DG45R44]: We are not allowing any of these unless higher ups override that initial decision. Trials really do not provide anything that we want. Developer environments could be used but are limited and may cause more problems. Teams Environments are not something we have supported since Craig, and I do not see us changing.

Commented [DG46]: Forget what the actual name of this is … will get the exact name and replace.

Commented [DG47]: While this may not be 100% necessary, it will allow us to easily identify the deployment step in Workflows to determine which deployment is being used.

Operational Objectives

The objectives of the PPT is to manage the Power Platform environment for the benefit of the IRS end user community. This includes but is not limited to CRUD[1] operations and offering high-level management support for development, test and production environments, as well as ensuring security, cyber and privacy checks, licensing checks, and platform maintenance to ensure normalization and best practice operations.

Commented [DL48]: ⁉ Sample of CRUS operation?

Commented [DG49R48]: CRUD = Create, Read, Update, Delete : basically stating that we are responsible for the Creation, Reading, Updating and Deletion of power platform environments.

PPT Operation Vision – 1.0 Services

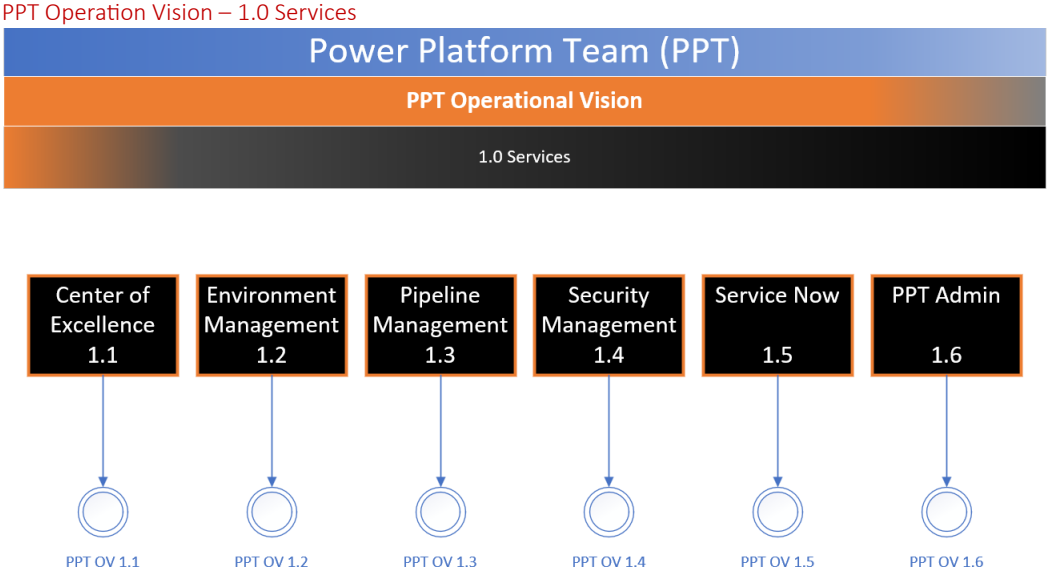

Figure 1: PPT Operational Vision 1.0 Services

Figure 1 shows the high-level operation services offered by the PPT. It is worth noting that we do not provide Power Application, Power Automate, Power BI, or any other power platform code assistance. While we do offer limited support, it is generally reserved for assisting Makers in understanding and how to manage their code for deployment between environments.

PPT Operation Vision – 1.1 Center of Excellence

The Center of Excellence (COE) for the Power Platform is a Microsoft built tool for Power Platform Tenant Administrators use (See Figure below). It provides views and tools that span the entirety of the Power Platform Tenant of IRS, providing important information to assist the PPT Admins in keeping the Power Platform Environment healthy and informed. For example, the COE identifies orphan apps and flows easily without complex custom flows, as well as shows AI use across all of the tenant, app and flow use, and who it is shared with and more.

[1] CRUD (or C.R.U.D.) means **C**reate, **R**ead, **U**pdate and **D**elete. It is a common terms used in software development.

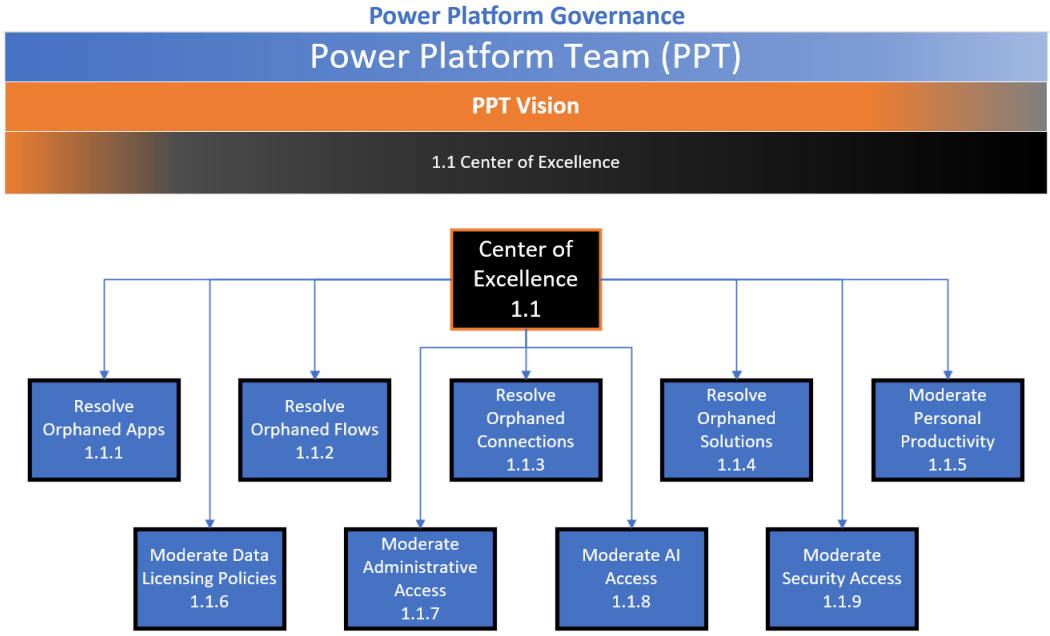

Figure 2: PPT OV 1.1

PPT Operation Vision – 1.2 Environment Management

Environment Management is one of the core areas the PPT Admins spend a great deal of time. This allows the PPT Admins to create, update, and potentially remove environments. It also allows us to defined their environment Settings, assign their environments to a Data Licensing Policy (DLP), attach Entra Security Groups and provide the appropriate environment permissions (security roles), and more. It is the backbone of the environment that the IRS end users build their apps, flows, data flows, connections and more.

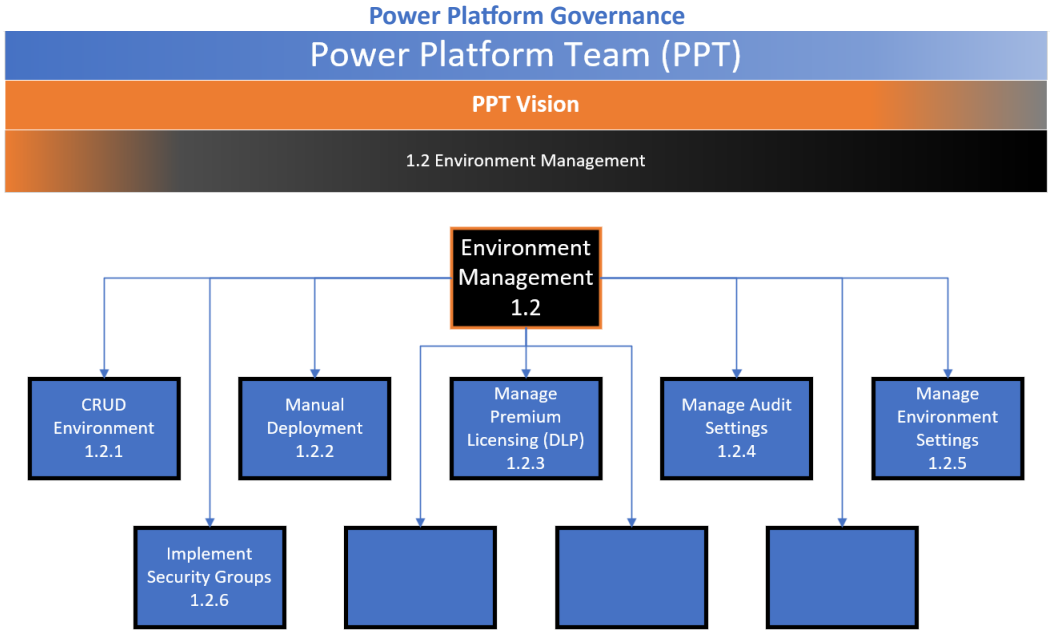

Figure 3: PPT OV 1.2[2]

PPT Operation Vision – 1.3 Pipeline Management

Pipelines are offered by Microsoft within the Power Platform Environment as an additional Dynamics 365 application module. Pipelines offer a CI/CD (Continuous Integration / Continuous Delivery) feature within the Power Platform Environment, allowing developers to self-deploy from Sandbox (development) to Test and Production environments. Unfortunately, while the Pipeline feature is robust, it is not at the level of traditional CI/CD pipelines such as Azure DevOps or Team Foundation Server, or other more robust systems built to handle large-scale custom-built applications such as C++, JAVA, or C# application solutions. As such, there are some issues that require manual interaction by the PPT Admins in certain cases, such as when the user needs to deploy custom Security Roles. However, as these are not often modified once the system is ready to go to production, the interjection of PPT Admins within the pipeline is minimal compared to the developer's self-deployment capabilities. It is hopeful that Microsoft will introduce a solution to negate this manual interjection in future Power Platform releases.

[2] The blank boxes are intentionally left there. This is still in review, and we left the boxes for future changes. They will be removed once the PPT/PPG agree on the images.

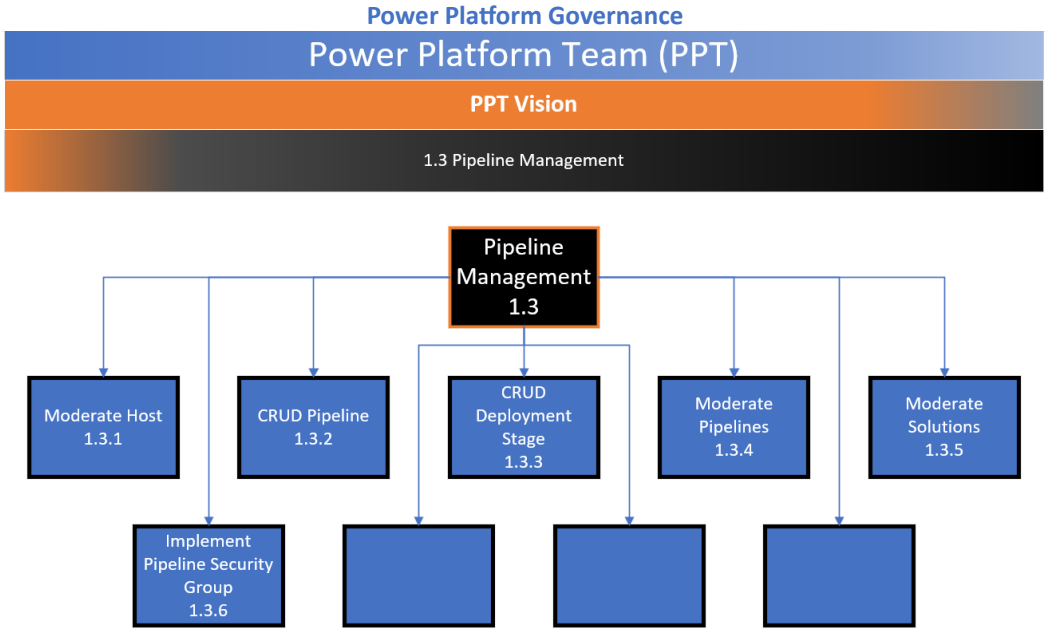

Figure 4: PPT OV 1.3[3]

PPT Operation Vision – 1.4 Security Management

Security Management has two sides. The first side is security management for each Environment built. The PPT Admins create and maintain Entra Security Groups and attach them to "Teams" within each environment and apply the appropriate security roles. This may include Admins, Makers and Users in the Sandbox environment.; or Users and several custom Security groups for each of the custom Security Roles they have. It also includes the creation and attachment of Pipeline Deployment groups necessary to perform pipeline deployments. The second side is insuring that no one has been given inadvertent access to parts of environments or part of the Power Platform Environment. Specifically insuring that access and permissions are limited in the Personal Productivity (default) environment, and to ensure that people are not using the default environment to run production level flows, or apps.

[3] The blank boxes are intentionally left there. This is still in review, and we left the boxes for future changes. They will be removed once the PPT/PPG agree on the images.

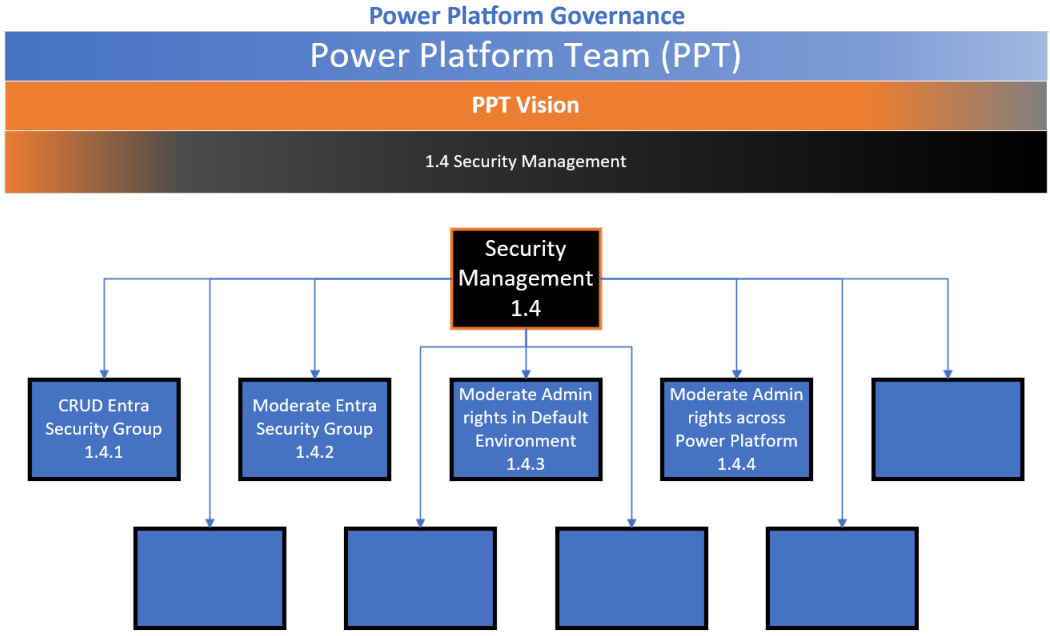

Figure 5: PPT OV 1.4[4]

PPT Operation Vision – 1.5 Service Now

The PPT has a page and several forms that are specific to Power Platform. For example, we have a form specific for Environment requests, one specific to security groups, and another for deployment requests. We maintain those forms and we service the tickets that come from it, as well as additional tickets that are assigned to us that came through other means within Service Now.

[4] The blank boxes are intentionally left there. This is still in review, and we left the boxes for future changes. They will be removed once the PPT/PPG agree on the images.

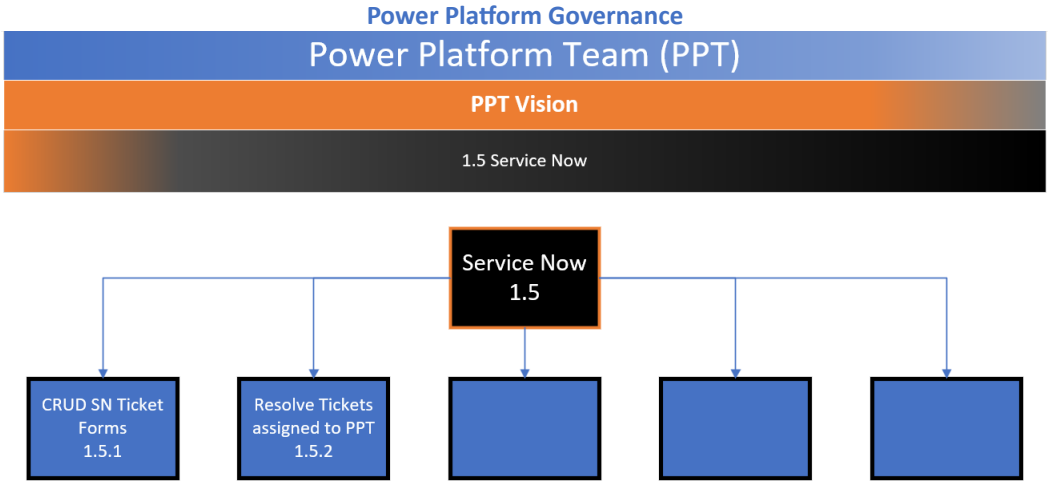

Figure 6: PPT OV 1.5

PPT Operation Vision – 1.6 PPT Admin

The PPT will ensure that IRS users may access the latest information pertinent to the Power Platform Environment, instructions, governance, processes and all pertinent documentation and information applicable to the IRS end user (customer) will be available through the M365 Central SharePoint site Power Platform section.

The Team will also utilize the SharePoint site beneath the PPT Team site (TM-IT-EOPS-M365 Power Platform Project) to maintain core documentation pertinent to the PPT such as step-by-step procedures of "How to" perform the core actions that make up our Operational Objectives.

Finally, the PPT will also have a measure to display Metrics to various audiences (TBD). Some metrics will be maintained within a MS Project Spring template, which provides operational burndown charts, such as Sprint burndown, personnel utilization, and more. Furthermore, we will provide base metrics such as: Power Platform usage to management, such as total Environments, Total Apps, Total Flows, Personal Productivity burndown, and pipeline metrics. Many of these metrics may be internal to the development team (PPT), while others will be available to the PPG (including stakeholders).

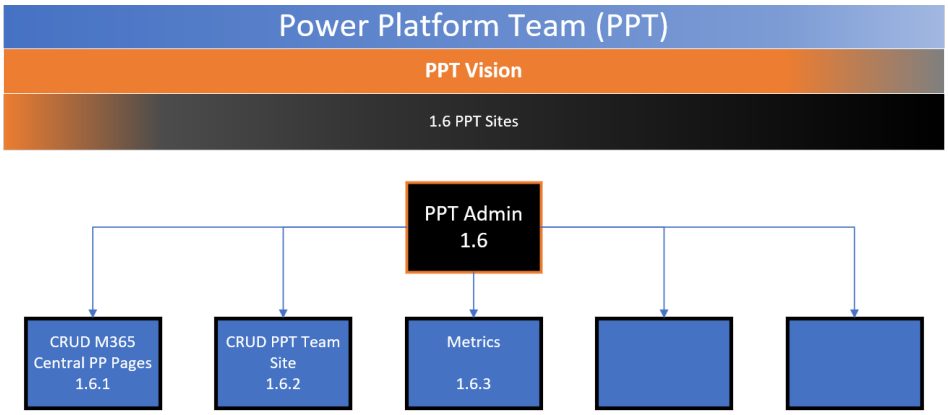

Figure 7: PPT OV 1.6

Power Platform Governance

Elements Of Governance

- Power Platform tenant-level Administration settings
- Individual Environments
  - Sandbox
  - Test
  - Production
  - Developer
  - Trial
  - Pipeline Host
- Microsoft Entra Security Groups
- Manual Deployments
- Pipelines
  - Host
  - Pipelines
    - Validation of Solution
      - Validation against architecture approval
    - Validation of UAT
    - Validation against app checker
  - Pipeline Deployment Groups
  - Special deployment accommodations for Security Roles
- COE Health and Monitoring
  - Ensure users are not using Default environment for production
  - Clean up Ghost objects
    - Apps
    - Flows
    - Connections
    - Environments
  - Monitor irregular behavior of apps, flows, or connections
  - Monitor irregular permissions.
  - Setting Solution Checker and App Checker requirements
- Solutions
  - Validating Architecture
    - TRB with Cyber and Privacy
    - Templated Architecture document
  - Setting Time and Version limits on re-validation of Architecture
  - Ensuring apps meet app checker

Operational Use Cases

Center Of Excellence (COE) 1.1

Resolve Orphaned Apps 1.1.1

Every Sprint a check will be made to see if there are Orphaned Applications. Any identified orphaned applications will be mitigated through contacting users who the app is shared with, or if it is attached to a dedicated environment. For those applications that are ghost, we will work with Privacy to determine proper disposal.

Resolve Orphaned Flows 1.1.2

Every Sprint a check will be made to see if there are Orphaned Flows. Any identified orphaned flows will be mitigated through contacting users who the flows is shared with, or if it is attached to a dedicated environment. For those flows that are ghost, we will work with Privacy to determine proper disposal.

Commented [DL50]: Who are contacts in Privacy?

Commented [DG51R50]: Ask Ron Gutenberg, I believe we used his contacts.

Resolve Orphaned Connections 1.1.3

Every Sprint a check will be made to see if there are Orphaned Connections. Any identified orphaned connections will be mitigated through contacting users who the connections are shared with, or if it is attached to a dedicated environment. For those connections that are ghost, we will work with Privacy to determine proper disposal.

Resolve Orphaned Solutions 1.1.4

Every Sprint a check will be made to see if there are Orphaned Solutions. Any identified orphaned solutions will be mitigated through contacting users who the solutions are shared with, or if it is attached to a dedicated environment. For those solutions that are ghost, we will work with Privacy to determine proper disposal.

Moderate Personal Productivity 1.1.5

The PPT will instill regulations and limitation on the Personal Productivity environment to ensure that users do not use it in a productive manner.

Moderate Data Licensing Policies 1.1.6

To ensure that the DLP is being adhered to, the COE provides apps, flows and solutions that are operating outside of a DLP, which will be remediated appropriately. PPT will also regularly monitor changes in the premium licensing offerings to ensure that the IRS end users have access to the latest and greatest connectors within IRS licensing and Privacy/Cybersecurity approvals.

Moderate Administrative Access 1.1.7

To ensure that users do not have unnecessary access to environments, or objects within the Power Platform Environment, the PPT will utilize the features of the COE to identify misuse or mis-appropriated power to individuals, and work to remedy the situation. Furthermore, in coordination with management, and other groups, ensure that no unauthorized rights are given to users into the COE or Power Platform Admin center, and that those who have access due to greater rights are not using those powers in a unknowingly bad means within the Power Platform Environment.

Moderate AI Access 1.1.8

AI has not been approved for IRS but was briefly used in great quantities by several users and organizations early in the Power Platform adoption. The PPT will continue to vigilantly check any use of AI that circumvents the Power Platform Tenant AI settings.

Moderate Security Access 1.1.9

Security Access is a crucial element, and is spread between several aspects of the PPT Services offered. In relation to the COE, it is determining who has advanced access to the COE, who has advanced or individual access to Environments (should be via Entra groups), and making sure that

Power Platform Governance

Environment Management 1.2

CRUD Environment 1.2.1

One of the primary directives of the PPT is to create and modify Environments such as Sandbox, Test, and Production. This is done upon receiving a Service Now ticket, through the specific forms we have created.

Throughout the life cycle of the Environment, we will continue to monitor and manage the environment to ensure it stays within guidelines using the COE as a guide for identifying environments that may need adjustment or management based on COE findings, or at the request of end users and approval from necessary approvers.

Manual Deployment 1.2.2

While it is the intent to have Pipelines fully flushed out and developed to allow groups to self-deploy, currently and even once the Pipelines are set up, there will be times where we will need to manually deploy.

Commented [DL52]: Cross reference to manual steps or Microsoft documentation.

Commented [DG53R52]: The manual steps and pipeline deployments should be the same with minor or limited exceptions. Pipelines are only an automated version of what we do manually.

Manage Premium Licensing (DLP) 1.2.3

Whether or not the IRS acquires the necessary number of premium licenses for Power Platform for all of IRS or not, the PPT will continue to require Security Change Management approval before providing premium connector capability. This will ensure that all connectors that may point outside of IRS or connect to non-approved 3rd party software/services are vetted by Cyber and Privacy prior to being used.

Manage Audit Settings 1.2.4

Audit settings are not immediately available when creating an Environment but must be modified afterwards when the environment synchronizes with the tenant. As such, the PPT will remain vigilant to ensure that the audit logs for each environment are retained for the proper length of time.

Manage Environment Settings 1.2.5

When creating an environment, the environment settings are set (see *Instructions for Power Platform Environments.docx*) to ensure that the environment is secure and provides the end users with the appropriate capabilities.

Commented [DL54]: Links to steps to ensure that Environment is secure.

Commented [DG55R54]: The link is there - see Instructions for Power Platform Environments.docx

Implement Security Groups 1.2.6

Security groups are created to provide the necessary access (see *Instructions for Power Platform Environments.docx*). Sandbox environments allow maker and admin access, but the Test and Production environments are managed and allow only user and pipeline deployment access. Additional "User" groups may be created as necessary for any custom security roles related to the Dataverse tables that are implemented by the end user.

Pipeline Management 1.3

Moderate Host 1.3.1

The Host environment holds, maintains, and manages all the pipelines attached to it. Pipelines are defined with the host, and only exist within the host. PPT will maintain and manage the host and implement any necessary elements to monitor and provide approval and validation to pipeline deployments.

CRUD Pipeline 1.3.2

The PPT will create, read (provide information), update and delete (remove) all pipelines within the host environment. The PPT will also monitor and manage the pipelines as necessary to ensure they remain healthy and up to date with necessary information.

CRUD Deployment Stage 1.3.3

The PPT will provide CRUD operations in relation to Deployment Stages to ensure that all pipelines require deployment to Test prior to deploying to Production, and that all deployments stages across all pipelines follow standards laid out in the *Instructions for Power Platform Environments.docx* reference.

Moderate Pipelines 1.3.4

The PPT will implement Power Automate Flows within the Host environment to monitor all Pipeline deployment requests. While the Host monitors and keeps a history or deployment runs itself, the PPT will use the flows to capture information to ensure that if deploying to production the deploying pipeline group must show that they have performed proper UAT. Failures will be recorded, and emails will be sent to our group to ensure that we are aware and can chase down the issue, as well as ensure success.

Moderate Solutions 1.3.5

Using the same flows to intercede during the deployment process of pipelines, the PPT will ensure that the solution being deployed is a known and approved solution and has a valid approval status prior deployment.

Implement Pipeline Security Group 1.3.6

Pipeline security is separate and only available once an environment(s) has been associated in a pipeline. Once it is associated, a new Pipeline Entra Security Group is created and attached to each environment of the Pipeline, as well as to the Host where the Pipeline is shared with that Pipeline group, and given the Pipeline Deployment User security role, allowing them to perform the pipeline deployment.

Commented [DL56]: What does a Pipeline security group look like, naming convention?

Commented [DG57R56]: There is a Pipeline naming convention - see the Instructions for Power Platform Environments.docx

Security Management 1.4

CRUD Entra Security Group 1.4.1

This task is specific to our group and is directly related to the Environments. The PPT performs CRUD operations for the Entra Security groups that are associated with each environment, connecting them to their proper security roles on each environment.

Moderate Entra Security Group 1.4.2

The PPT will monitor and ensure that Entra Groups are being used appropriately in relation to Power Platform environments. In some cases owners leave and the Entra groups have no owner, in which case we receive a Service Now ticket to have a new Owner added. We also use COE to identify when groups are given unnecessary access, or may be outside of normal operating guidelines.

Moderate Admin Rights in Default Environment 1.4.3

The Personal Productivity (default) environment is widely used, and is available to all IRS personal with a G5 license. It allows them to create, update, delete and run Power Platform apps and flows, and more. Because the use of dedicated and BU specific environments came well after the default environment was released, there are hundreds if not thousands of apps and flows that users have created and many of them use them in production manner.

To combat this behavior, the PPT monitors usage and number of users on a app or flow. If it being used regularly or has a large or growing number of users, it is flagged and the PPT works with them to move the app or flow to a BU or dedicated environment.

Moderate Admin Rights Across Power Platform 1.4.4

The PPT uses the COE, works with IRS licensing personnel, and monitors all Admin level groups to ensure that users are not given or taking advantage of unnecessary access to Power Platform administration.

Service Now 1.5

CRUD Service Now Ticket Forms 1.5.1

The PPT has several Service Now forms that were created for specific requests such as new Environments, new Security Groups, and deployments. The PPT will continue to review and determine if the forms need amendment, removal, or new forms are needed for specific requests.

Resolve Tickets Assigned to PPT 1.5.2

The PPT continues to work Service Now tickets submitted for the Power Platform.

Power Platform Website 1.6

CRUD M365 Central PP Pages 1.6.1

The PPT team will perform CRUD operations and maintenance and monitoring of the M365 Central Power Platform section to ensure that the information remains relevant and up to date, and provides users with the necessary information and tools to use or make requests of the Power Platform Team.

CRUD PPT Team Site 1.6.2

The PPT will monitor and maintain the SharePoint Site beneath the *TM-IT-EOPS-M365 Power Platform Project* team. Here, the PPT will provide operational information and metrics, as well as Power Platform metrics that are pertinent to both the development team (PPT) as well as the stakeholders (Power Platform Group (PPG)).

Relevant data such as PPT instructions and How To documents will be maintained here through the Team, making it a knowledge base as well for the PPT and PPG.

Metrics 1.6.3

Metrics will be maintained to assist the PPT in quick looks access to see where the environment stands across many defining metrics. The PPG will also have metrics available that are more relevant to them to ensure they have a birds eye view of the operations of the PPT and the Power Platform Environment.

Capabilities: Rules, Regulations and Responsibilities

The Capabilities outlined in this section correlate to the Operational Objectives, and are in the following form:

- Responsibilities: This defines the core responsibilities and tasks that the Power Platform Team is responsible for within the IRS environment.
- Rules: Regulations that define the thresholds, limits, and time frames of much of what the PPT does.
- Regulations: Regulations that guide the Power Platform Team in implementation of Power Platform tasks.

Responsibilities

1.1 Center of Excellence (CoE)

-

1.2 Environment Management

-

1.3 Pipeline Management

-

1.4 Security Management

-

1.5 Service Now

-

1.6 PPT Admin

-

Future State of Power Platform Governance

While it seems like there is not a great deal to do to ensure governance is applied, the Power Platform Environment is a complex service that is wrapped and intertwined with

Appendix A: Pipeline API Process

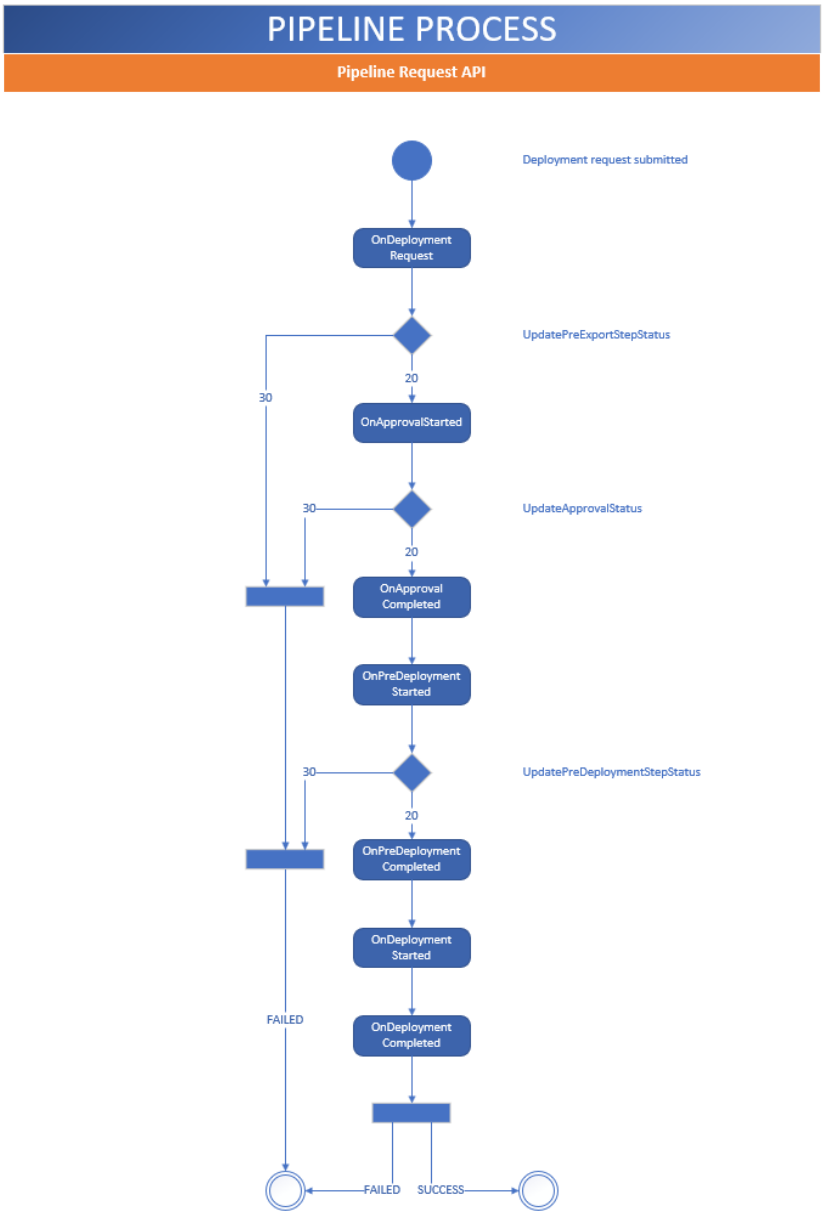

Figure 8

Power Platform Governance

power platform and power apps need to be under real governance

-how they are created

-how they are managed

-change in ownership?

-use case scenarios? easy/med/difficult

1. what are we doing for pipelines today

2. what are we not doing?

3. any needed contract support or tool we could use?

Who approves the actual apps? documentation?

Need responses to these questions by COB Wednesday next week.

What are we doing?

What are we not doing?- app checkers? reviews?

What are we planning to do?

Are there other tools that we can use to help provide governance?

What results are we trying to achieve?

What are the use cases?