Microsoft Power Platform

Administering and Governing the Power Platform for Enterprise

Contributors
Allen Geer, Patrick Bell, Vanessa Welgemoed, Taylor Steele

IT Professionals IT administrators and professionals responsible for managing and maintaining the technical infrastructure of an organization, including the Power Platform.

Business Analysts Professionals who analyze business requirements and use the Power Platform to create solutions for various business needs.

Developers Individuals involved in building custom applications using Power Apps and integrating them with other components of the Power Platform.

Data Analysts Professionals who use Power BI to analyze and visualize data for business insights.

Enterprise Architects Individuals involved in designing the overall architecture and strategy for deploying and utilizing the Power Platform in a large organization.

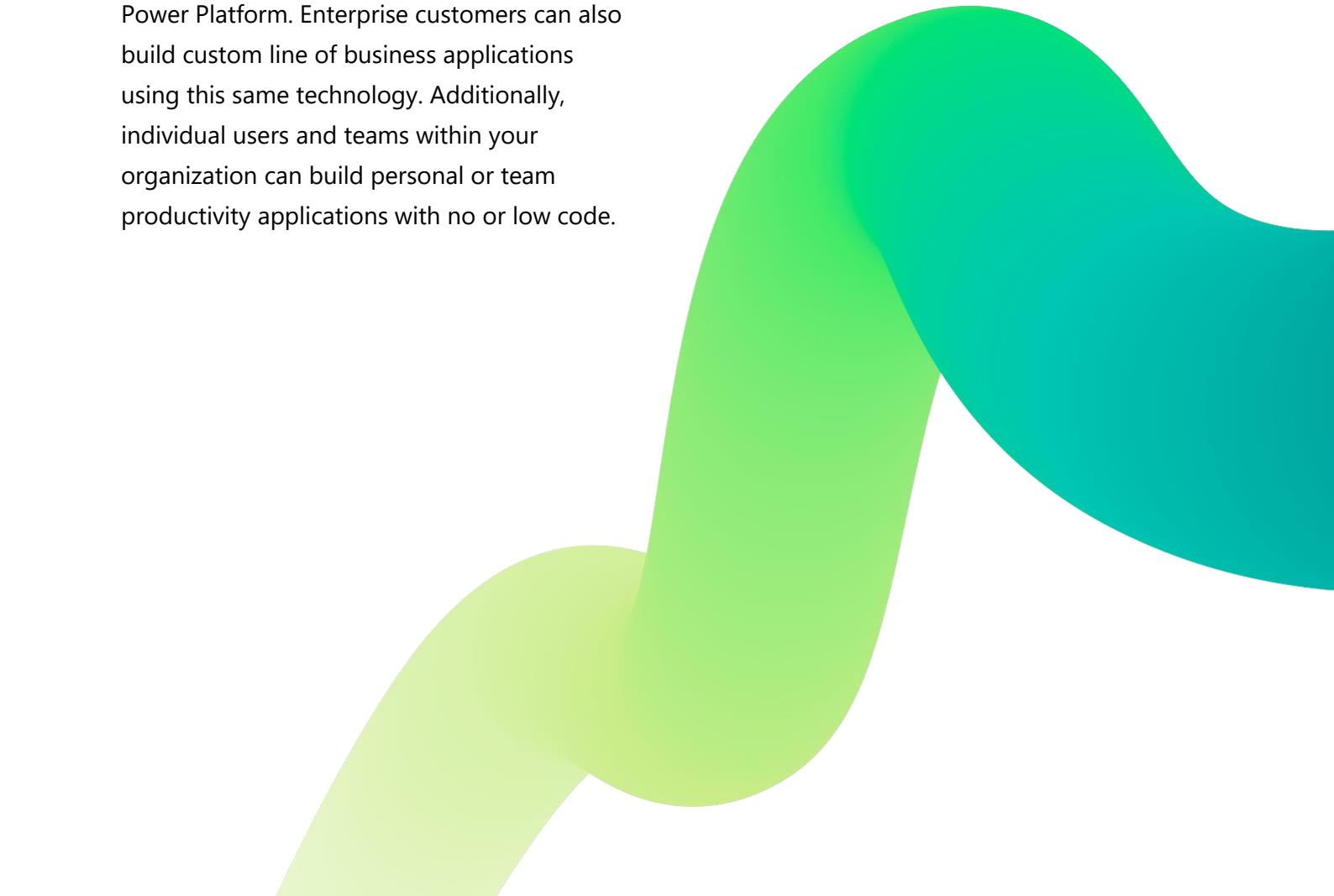
Decision-Makers Business and IT leaders who need to understand the capabilities and potential benefits of the Power Platform for their organization.

Introduction

Microsoft Power Platform is a productivity application development platform that delivers innovative business solutions across one seamlessly integrated platform. Power Apps, Power Automate, Power Pages, Microsoft Copilot Studio, Dataverse and Connectors allow organizations to quickly and easily build custom apps, workflows, websites, and intelligent bots driven by generative AI. Power BI allows any business to analyze and visualize real-time business performance.

Microsoft uses the platform to build their own first-party applications Dynamics 365 Sales, Service, Field Service, Marketing and Talent. These applications are built natively on the Power Platform. Enterprise customers can also build custom line of business applications using this same technology. Additionally, individual users and teams within your organization can build personal or team productivity applications with no or low code.

This whitepaper is targeted towards people responsible for planning, securing, deploying, and supporting environments and applications built on the Power Platform.



Purpose

This whitepaper is targeted towards people responsible for planning, securing, deploying, and supporting environments and applications built on the Power Platform. The goal of the paper is to help you understand what is currently in your environment, how to build a strategy to structure your Power Platform, how to proactively plan for applications being developed and deployed, and finally how to operate the platform effectively and securely day-to-day.

In this whitepaper, we will cover key concepts, features, and decisions that are necessary to administer an effective Power Platform instance. Where possible we will help you define and develop best practices for your organization to ensure successful deployment of the platform.

Scope

Unless specifically noted, all features mentioned in this whitepaper are available as of October 2023.

The following topics are out of scope for this whitepaper:

- Power BI and other parts of the broader Power Platform
- Power Apps fundamentals for building applications
- ISV deployment scenarios, which are handled differently from enterprise deployment scenarios.
- Performance tuning of applications
- Full deployment and management of first-party Dynamics 365 applications
- While many of the concepts presented in this paper apply to Dynamics 365 Finance, Dynamics 365 Supply Chain Management, and Dynamics 365 Retail, they are not directly covered.
- Third party solutions which integrate with Power Apps.

Please visit https://docs.microsoft.com/en-us/power-platform/ to learn more about these topics.

What's New

Since this whitepaper was last published in 2020, the Power Platform has undergone major changes that include a variety of new products and features that organizations will want to take advantage of in administering their platform. This version of the whitepaper has major additions and modifications in the following key areas:

In the last three years, the Power Platform has become a core "agility layer" for enterprises allowing organizations to quickly and efficiently build new apps and functionality using the data and services provided by mission critical core business systems. This practice of approaching the Power Platform as an extension to core business systems requires careful planning and consideration.

- Since the original whitepaper, the Common Data Service (CDS) has been rebranded as Dataverse. With Dataverse comes a variety of next-generation features that supply a versatile, state of the art data platform that will drive your entire ecosystem of Power Platform tools and applications.

- Organizations can now use managed environments to provide best practice governance, control, and deliver new capabilities to makers. The whitepaper will discuss best practices for how managed environments fit into an organization's environment strategy, and how to best configure and use the features of managed environments to operate a secure and governed platform.

- Makers can now take advantage of Copilot features to greatly accelerate and augment their development workflow. This whitepaper will dive into how makers can use Copilot and outline key information about how Copilot functions to keep your organization's data secure.

- Since the last revision of the whitepaper, the Power Platform has released Power Pages, the next evolution of the Portals solution, an offering that helps organizations build highly customizable, low-code business websites backed by data in the Dataverse.

- Delivery of Power Platform solutions has been simplified with the new Power Pipelines available with managed environments. This whitepaper will walk through how administrators can configure their Power Pipelines to ensure that all their makers can take advantage of best practices around Application Life-cycle Management (ALM).

- Additionally, organizations can take advantage of the ALM Accelerator, which is a Power App that provides a simplified interface to implement best practice ALM on Azure Pipelines and Git source repositories.

- We will investigate new, critical features for managing environment sprawl and the default environment, such as Environment Routing which gives makers their own development environment instead of the entire organization using the shared default environment.
- The Centre of Excellence (CoE) Starter Kit has grown immensely since the last revision. We will investigate some of the critical CoE apps that can help organizations ensure they have a well governed environment.
- Power Virtual Agents now falls under Microsoft Copilot Studio. Copilot Studio brings together a set of powerful conversational capabilities, from custom GPTs, to generative AI plugins, to manual topics. Copilot allows users to easily customize Copilot for Microsoft 365 for your organization scenarios.

Overview

Power Platform is a product family that delivers innovative business solutions across one seamlessly integrated platform. Power BI, Power Apps, Power Automate, Power Pages and Microsoft Copilot Studio allow any business to analyze and visualize real-time business performance, quickly and easily build custom apps, automate workflows, deliver business websites, and integrate AI capabilities.

Power Platform supplies a low code interface for any user to quickly create custom apps while simultaneously providing robust tools for pro developers. This makes it possible to develop integrated and innovative solutions across Azure, Microsoft 365, Dynamics 365, and standalone applications. For enterprises, the platform serves as a core "agility layer" that allows organizations to quickly build new applications and experiences while leveraging the data and services provided by core business systems like SAP or Salesforce. At the intersection of these products lies digital transformation – giving the customer the power to innovate anywhere, while unlocking value everywhere.

Power Platform enables businesses to easily analyze data, create apps, automate workflows, and integrate AI.

Why do organizations use the Power Platform?

The Power Platform supplies a level of capability, security and supportability that allows organizations to quickly build, test and deploy applications and solutions leveraging their existing data and systems. In this way, it provides a layer of capability that is agile, adaptable, and cost effective for developing and testing new ideas and services for an organization. As previously mentioned, the Power Platform functions as an "agility layer" that allows organizations to quickly build apps and deliver them out to their intended audience.

One of the key features of the Power Platform is its ease of use. All the tools are low-code to no-code, meaning that makers do not need to write code to create working solutions. With appropriate governance in place this means that solutions are produced quickly and in standard, supportable ways. They are likely to have less bugs and can be quickly deployed to end-users to test ideas and assumptions.

Another reason organizations use the Power Platform is that it is easy to integrate with their enterprise data. From building an order tracking app for front line staff that leverages data in SAP, or an employee feedback app that leverages your employees HR file sitting in Workday, the Power Platform is built to integrate with your enterprise data safely and seamlessly – where it is. No migrations or synchronizations needed.

Addressing the shadow IT concern, many organizations are faced with the challenge of business units or individual users creating unofficial, often unsanctioned, IT solutions to address their specific needs. This phenomenon, known as shadow IT, can introduce risks related to data security, compliance, and system integration. The Power Platform offers a compelling solution to this challenge. By empowering users to develop their own solutions within a controlled and governed environment, organizations can harness the innovation and agility of shadow IT without the associated risks. Users can solve their individual and business needs, while IT keeps oversight, ensuring that everything developed aligns with organizational standards and best practices. This balance between user empowerment and IT governance ensures that innovation can occur anywhere within the organization, unlocking value everywhere.

Finally, organizations use the Power Platform because it is simple to use and scale reliably. Classic software development and operation typically involves many highly technical areas resulting in higher cost to operate and higher risk to maintain and update as business changes. By virtue of Power Platform being a standardized, robust, reliable offering, organizations no longer must worry about the

undifferentiated heavy lifting of building, deploying, and operating coded applications. Power Platform makes it simple for an individual maker to create and deploy solutions to an audience.

Dataverse

Dataverse, formerly known as the CDS, is a fundamental component of Power Platform that provides a secure and scalable storage solution for data. Power Platform applications, such as Power Apps, Power Automate, and Power BI, can seamlessly utilize Dataverse to store and manage data, making it a pivotal part of
the unified ecosystem for business application development.

A significant feature of Dataverse is its ability to store data in a relational manner, allowing for complex relationships, hierarchies, and structures that are crucial for complex business applications. The data within Dataverse is stored in tables, which are analogous to tables in other relational databases such as SQL. Each table can contain multiple columns and can have relationships with other tables. Additionally, the platform allows for the definition of business rules and logic at the data layer, ensuring that data operations maintain business-specific constraints and conditions.

Another core feature is the rich set of security mechanisms Dataverse provides. Data integrity and protection are vital for business applications, and Dataverse facilitates this through its robust security model. This model supports fine-grained permissions, role-based access control, and field-level security, ensuring that only authorized users can access or modify specific sets of data. Moreover, it is integrated with Entra, which further bolsters its security capabilities by aligning with a widely accepted identity service.

Lastly, Dataverse is known for its extensibility and integration capabilities. It provides a set of APIs that developers can use to interact with data, allowing for the creation of custom applications or integration with other systems. This feature is bolstered by a rich set of connectors provided by the Power Platform that facilitates integration with hundreds of applications and services, ranging from other Microsoft products like Dynamics 365, SharePoint Online and Azure services, to third-party solutions.

In essence, Dataverse's core features of relational data storage, security, and extensibility make it an invaluable asset within the Power Platform's ecosystem.

Power Apps

Power Apps are a pivotal component of the Power Platform, providing a tool for rapid application development tailored for both business users and professional developers. With a focus on creating business applications quickly, Power Apps aims to bridge the gap between IT departments and other business

units, reducing the time and complexity traditionally associated with app development.

One of the core features of Power Apps is its low-code approach to application development. Users can build fully functional apps with minimal coding, utilizing a user-friendly, drag-and-drop interface. This low-code environment empowers not just professional developers but also business users (often termed as "makers") to create bespoke applications tailored to their specific needs without waiting for extended development cycles.

Another defining characteristic of Power Apps is its seamless integration with other components of the Power Platform, especially Dataverse. This integration enables apps to store, retrieve, and interact with data effortlessly, ensuring consistency and reliability in the underlying data. Moreover, Power Apps can connect with a vast array of external data sources, from SharePoint Online and SQL Server to various third-party services, thanks to the myriad connectors available within the Power Platform ecosystem.

Furthermore, Power Apps is built with mobility in mind. In an era where business operations are increasingly shifting towards mobile platforms, Power Apps allows for the creation of responsive apps that work seamlessly across devices – be it a desktop, tablet, or smartphone. This ensures that business processes can continue uninterrupted regardless of the device or location, promoting flexibility and efficiency. In summary, Power Apps stands as a transformation tool in the Power Platform, offering rapid, low-code application development that integrates seamlessly with diverse data sources while ensuring mobility and responsiveness.

Power Automate

Power Automate is another integral piece of the Power Platform. It is a service designed to automate workflows and tasks across a multitude of applications and services. Its primary objective is to facilitate automation in business processes, enhancing efficiency and ensuring that repetitive tasks are handled automatically, reducing the manual overhead and potential for human error.

A core feature of Power Automate is its vast collection of pre-built connectors. These connectors allow users to establish automated workflows between different services, be it within Microsoft's ecosystem—like SharePoint, Dynamics 365, and Microsoft 365—or third-party applications such as Twitter, Dropbox, and Google Workspace. This extensive range of connectors ensures that Power Automate can be a central hub for automating workflows, irrespective of the disparate technologies a business might be using.

The versatility of Power Automate is further showcased through its ability to cater to both simple and complex automation scenarios. For straightforward tasks, users can leverage

templates, which are predefined workflows tailored for common use cases. For instance, a user can quickly set up a flow that saves email attachments from Outlook to OneDrive.

However, for more intricate workflows, Power Automate provides advanced logic capabilities, like conditions, loops, and switches, enabling the crafting of nuanced automations tailored to specific business needs.

Security and compliance are also paramount in Power Automate. Given the potential sensitivity of data being processed and transferred across services, Power Automate emphasizes secure and compliant data handling. It integrates seamlessly with Microsoft's security infrastructure, ensuring that data remains protected throughout its journey. Moreover, the platform provides detailed audit logs, allowing administrators to monitor and review all automation activities.

Power Pages

Power Pages is a new product in the Power Platform that provides organizations with a way to build externally facing business websites. Power Pages are highly secure and ready to scale with any enterprise. Creating web pages through an easy to use low-code interfaces that will accelerate the design, build, and publishing workflow for both low-code makers and professional developers alike.

Power Pages, like other products in the Power Platform can take advantage of shared business data stored in the Dataverse. This allows makers to build everything from apps, workflows, intelligent virtual agents, and analytics visualizations that are exposed through Power Pages.

Power Pages also provides enhanced security and governance at its core. This allows authors to ensure that business data is secure. Power Pages can take advantage of site authentication with a variety of providers which can, in turn provides authorization scopes to business data. Power Pages supports modern Transport Layer Security (TLS) standards and is facilitated through the Azure App Service platform. This has a variety of compliance accreditations, including International Organization for Standardization (ISO), Security Operations Center (SOC), and Payment Card Industry Data Security Standard (PCS DSS).

For organizations servicing international, high-traffic sites, Power Pages can be set up to use content delivery networks, web application firewalls, and edge caching. By using Azure Front Door with Power Pages, organizations can offer global, low-latency business websites, taking advantage of the SaaS (software-as-a-service) platform.

Power Pages was formerly known as Power Apps Portals and Dynamics 365 Portals. The portals feature previously available in these

platforms, is now incorporated into Power Pages. This also means that tools such as the Power Pages Design Studio, Portals Management App, and the Power Platform Command-Line Interface (CLI) are compatible with Power Pages.

Microsoft Copilot Studio

Microsoft Copilot Studio is a low-code tool to customize Microsoft Copilot. Copilot Studio brings together conversational capabilities of custom GPTs, to generative AI plugins, to manual topics to easily customize Copilot for Microsoft 365 for your organization's scenarios.

Quickly build, test, and publish standalone Copilots and custom GPTs and manage and secure your customizations and standalone Copilots with the right access, data, user controls and analytics.

Built on the foundations of Power Virtual Agents (and other Microsoft Power Platform technologies) and designed to meet the needs of both IT professionals and makers, Copilot Studio integrates with Microsoft Azure OpenAI Studio, Azure Cognitive Services, Azure Bot Service, and other Microsoft conversational AI technologies.

One of the standout features of Copilot Studio is its no-code graphical interface. Users, even those without technical backgrounds, can design complex chatbot flows by simply dragging and dropping elements. This ensures that subject matter experts, who understand the nuances of the business or service provided, can take the reins in chatbot creation, crafting meaningful and effective dialogues without relying on a developer at every stage.

Integration is another strength of Copilot Studio. It ties seamlessly into the broader Power Platform ecosystem, especially Power Automate. This integration allows chatbots to trigger workflows or actions in other systems, extending the bots capabilities beyond mere conversation. For instance, a bot could not only answer a user's query about an order status but could start a refund process if needed, all within the same interaction.

Moreover, the analytics capabilities provided by Copilot enable organizations to continuously improve their bots. By examining how users interact with the bot, by identifying most frequently asked questions, and where users might be dropping off or expressing dissatisfaction, businesses can refine and optimize their chatbot's performance over time.

Copilot Studio empowers organizations to tap into the potential of AI-powered chatbots in a user-friendly manner, facilitating enhanced user interactions, streamlining processes, and providing robust integrative capabilities that align with today's digital-first business landscape.

Connectors

Connectors function as bridges between different services, enabling data to flow seamlessly across a diverse range of applications, databases, and other services. Whether you are looking to integrate data from cloud-based solutions, on-premises systems, or third-party platforms, connectors ensure that the Power Platform remains flexible and extensive in its data integration capabilities.

A key feature of connectors is their pre-built nature. Microsoft offers hundreds of ready-made connectors for the Power Platform, catering to popular services such as SharePoint, Dynamics 365, Azure SQL, Salesforce, Google Workspace, and many more. These connectors drastically simplify the process of data integration, allowing users to establish connections between the Power Platform and external systems with just a few clicks, without needing to dive deep into API intricacies.

In addition to the pre-built connectors, Power Platform also provides the capability to create custom connectors. Recognizing that businesses may have unique or niche systems that are not covered by the pre-built connectors. The platform provides tools for users to design their own connectors. This ensures that even proprietary or less common systems can integrate with the Power Platform, offering businesses unparalleled flexibility.

The robustness of connectors is also worth noting. They are not just simple data pipes but come with capabilities to handle authentication, error handling, and even data transformation in some cases. This ensures that data integration is not just possible, but efficient and reliable, reducing potential friction points when bridging multiple systems.

Connectors are the unsung heroes of the Power Platform, ensuring that data and actions can move effortlessly between a vast array of services. They encapsulate the platform's philosophy of accessibility, flexibility, and integration, providing users with tools to make the most of their data, irrespective of where it exists.

Managed Environments

Managed environments are a new premium capability of the Power Platform that allows customers to use best practices for governance and delivery of solutions in the Power Platform. Managed environments provide a variety of features that assist with limiting sharing, enforcing best practices, and implementing out-of-the-box ALM pipelines that help your makers easily deploy and manage solutions across various environments. Managed environments empower the governance and administration of the Power Platform at scale, unlocking more features tailored to those specific environments.

AI Features of the Power Platform

The Power Platform can also take advantage of recent advancements in Generative AI and machine learning. With Copilot, organizations can describe what they want their app, flow, or agent to do, in natural language, and Copilot will build it for them. This capability allows makers to be incredibly effective in generating even complex apps quickly and safely.

In addition to Copilot, AI Builder empowers users to integrate artificial intelligence capabilities into their apps and workflows without needing deep AI expertise. Through a user-friendly interface, AI Builder offers pre-built models for common scenarios, like form processing, object detection, and prediction, while also allowing customization based on specific data. This tool democratizes AI, bridging the gap between complex AI processes and everyday business applications, enabling organizations to harness the power of AI-driven insights and automation seamlessly.

Connectors are the unsung heroes of the Power Platform, they encapsulate the platform's philosophy of accessibility, flexibility, and integration.

Planning your Platform

Understanding Environments

In software development and deployment, the organization, management, and segregation of resources are pivotal to ensuring efficient workflows, security, and scalability. Power Platform addresses this need through the concept of "environments". These environments act as isolated containers, each hosting its own set of apps, data, and other components, ensuring that the different stages of the application lifecycle, from development to production, can be cleanly separated and managed.

Environments are the security boundary and the unit of management in the Power Platform. By delineating boundaries between different solution instances, environments prevent inadvertent overlaps, reduce the risk of errors, facilitate security management, and improve deployment efficiency. For instance, developers can work in an environment tailored for experimentation without the fear of disrupting live applications. At the same time, administrators can control access, allocate resources, and enforce policies differently for each environment, catering to its specific purpose and the needs of its users. With this foundational understanding, let us delve deeper into the primary types of environments within the Power Platform.

Each environment is tied to a single geographic location that is configured at the time the environment is created. By leveraging multiple environments in different regions, Power Platform supports multiple geographic deployments out of the box. Within each environment, the customer data for an environment does not leave the geography in which that environment is provisioned. Environments can be used for individual users or user groups, for intended purposes, for stages in the lifecycle of a solution or app, or for different audiences. Each environment can have different DLP policies applied to it, defining which connectors can be used and which connectors can or cannot be used in combination within the environment. Each environment has at the highest level a set of users that have the environment admin role. These users serve as the administrators of the environment.

There are 6 main environment types as of October of 2023:

1. Default Environments: are automatically created when a tenant is set up in Power Platform. It serves as a shared space and is the starting point for organizations. Within this environment, users can create resources, develop apps, and create flows. However, due to its shared nature, it is not suitable for specialized, sensitive, or business critical operations. Best practices recommend using this environment for personal productivity or non-critical solutions while utilizing other environments for more structured and controlled activities.

The default environment additionally plays a critical part in productivity enhancements for the Microsoft 365 suite. The default environment can leverage the entire suite of Microsoft 365 data connectors, allowing makers to build productivity applications and flows within the environment. By leveraging the default environment for these types of solutions, your organization to take advantage of a wide range of pre-built productivity tools and automations.

2. Production Environments: are tailored for live, operational solutions within an organization. These are the spaces where production solutions are deployed for end-users. Given their operational significance, they come with robust security and availability configurations, ensuring data integrity, reliability, and compliance. As production environments are connecting to live production data, it essential to ensure that changes and updates are managed carefully to prevent disruptions or unintended consequences.

3. Sandbox Environments: are designed explicitly for testing and development purposes. Here, developers can freely experiment, test, and make changes without affecting live operations. Once satisfied with the developments, they can then move or promote them to the production environment. A defining feature of sandbox environments is

their ability to be reset, allowing for a fresh start when needed. This reset capability ensures that any issues or unwanted changes can be rolled back easily, fostering an environment conducive to iterative testing and experimentation.

4. Trial Environment: as the name suggests, trial environments are temporary spaces, generally used for evaluation purposes. Organizations can use these to test out features, solutions, or ideas without committing to long-term changes or affecting their primary setups. Trial environments have a limited lifespan (often 30 days), after which they expire. This ephemeral nature encourages focused testing and ensures that non-permanent or experimental solutions don't clutter the organization's Power Platform configuration over the long term.

5. Developer Environment: are special use environments intended for Power Platform makers to create apps and flows in their own personal dedicated areas. Developer environments are intended to only be used by the developer that owns them, meaning that the solutions built within the developer environment are intended to move into supported environments once the developer is ready to share them with other members of the team.

6. Dataverse for Teams Environment: this is a special type of environment that is automatically created for a Microsoft Team when an app is created in the team or installed from the app catalog in Teams. These environments are responsible for storing the data used by the app and provide limited features and functionality outside of those that are for the Teams App development. Security in these environments is typically mapped to their corresponding role for the Microsoft Team.

Developing an Environment Strategy

As an initial stage of establishing a well governed Power Platform, your organization should undertake a formal development of an environment strategy. Building an environment strategy is not a prescriptive effort and must consider environments and work already created and used to date in the Power Platform, as well as future intended state. An environment strategy, broadly speaking, specifies how you deploy environments, for what purposes you will deploy environments and how you will govern each kind of environment dependent on their role. The environment strategy includes a set of governance configurations that apply to different environments depending on their role, business requirements, and the ALM strategy needed to enable solutions to be safely released into the environments.

Manage the Default Environment

The first part of an enterprise environment strategy is to manage the default environment. The default environment is

where makers create apps and flows by default. This can lead to significant risk and sprawl in large organizations. As an initial strategy, the default environment should be renamed to something more descriptive such as "Personal Productivity Environment" and a policy should be formed guiding makers in how it is used. By renaming the environment, it makes it clear that the usage is for individuals to create personal productivity solutions on the Microsoft 365 platform. The default environment cannot be disabled as it is used by various components within the Power Platform, primarily apps and flows created from Microsoft 365.

For example, Power Apps created from SharePoint lists will be automatically provisioned in the default environment. In some instances, you can change the default environment routing for Power Platform solution created via a Microsoft 365 interface. For example, it is possible to set a custom default environment for SharePoint Online Power App forms. By using the Managed Environments environment routing, premium feature, you can route new makers to their own personal developer environment. Thereby simplifying solution practices and enforcing more control over user routing. Environment routing helps to limit sprawl and helps share best practices through onboarding content and experiences.

To limit the risk of data loss from the default environment, a policy should be invoked that limits the connectors available in the default environment to business approved connectors such as SharePoint, Teams, and Outlook. New connectors should be blocked by default in this environment as well as custom connectors. A default environment administrator should be assigned to regularly maintain and monitor this environment and ensure it is being used sensibly.

Determine Major Environment Use Cases

As a first step to building an environment strategy, you should determine the major use cases for environments your organization will have. As a starting point, consider the following environment use cases:

- **Developer:** suitable for a single developer iterating on a small productivity solution while it is in development.
- **Power user environment:** this is an environment that is intended for use by advanced makers and developers that need access to more connectors than just those that are allowed in the default environment. It's important to develop a process for how users are evaluated, trained, and granted access to this environment.
- **Dedicated:** a core solution that will undergo development in multiple development or test environments and will be used by many people both internal and external to the organization.

- **Shared:** an environment that houses multiple medium complexity solutions.

Most organizations will have these core use cases and will need to design a process for how these environments are created, maintained, and administered.

Trial Environments

By default, one trial environment at a time can be created by paid and trial licensed users. These trial environments do not count against the tenant storage capacity and expire after 30 days if not converted to production environments. It is important to understand if not converted prior to the 30 days all resources including data in that environment are deleted.

For more details on who can create environments review the docs here:

https://docs.microsoft.com/power-platform/admin/create-environment - who-can-create

https://docs.microsoft.com/en-us/power-platform/admin/create-environment

It is **recommended to restrict trial environment creation** to only Microsoft 365 global admins, Dynamics 365 admins, and Power Platform admins from the Power Platform Admin Center.

Production Environments

By default, all licensed users will be able to create new production environments if the tenant has at least 1GB of Dataverse database storage capacity remaining.

It is recommended to restrict production environment creation to only Microsoft 365 global admins, Dynamics 365 admins, and Power Platform admins from the Power Platform admin center.

Determine how Environments are Managed

Once environments are created, they will likely require regular administration and maintenance. Activities such as adding and removing users from environments, adding connectors, and modifying configuration are all common day-to-day administrative tasks required. When the environment is created, a small group of administrators are assigned the administrator role for that environment. They will ultimately be the team responsible for responding to any requests to modify the environment. You must design how those requests will be raised, evaluated, and ultimately governed and approved so that your administrators can act. Some common patterns, such as modifying policies, can be automated using tools such as the CoE Starter Kits Request Policy Change feature of the Environment Request app.

Environment management is based on roles:

- Global admin/ Dynamics 365 service admin can manage any environment in the tenant.
- Licensed users need to have Environment administrator role to manage the environment.

No additional Power Apps / Power Automate plan license is required to manage environments.

View the service administration permission matrix here: https://learn.microsoft.com/en-us/power-platform/admin/use-service-admin-role-manage-tenant

The day-to-day management of an environment is performed by the environment admin role. It is best practice to assign at least three environment admins to each environment you create as well as build a process for continuously evaluating that all environments have active owners. The power to create and delete environments, however, is typically reserved for global admins, Dynamics 365 service admins, and the Power Platform admin role.

The expanding capabilities of Power Automate necessitate the introduction of Automation Platform Administration. Automation Administrators play a crucial role in establishing or aligning with Azure resource management, developing strategies for automation security and compliance, overseeing user access, managing capacity and licenses, formulating environment and data governance strategies, ensuring long-term sustainability, and addressing attrition and succession planning.

Managed Environments

Managed environments are a new feature of the Power Platform that allow customers to leverage best practices for governance and delivery of solutions in the Power Platform. Managed environments provide a variety of features that assist with limiting sharing, enforcing best practices, and implementing

Microsoft 365 Global Admin	Dynamics 365 Service Admin Power Platform Service Admin	Delegated Admin
Full administration to all services in tenant	Full administration to all Power Apps and Power Automate assets and environments Power Platform admin role	Full administration to all services in tenant Used for partners to provide support to customers Full support for Power Apps and Power Automate coming soon

out-of-the-box ALM pipelines that help your makers easily deploy and manage solutions across various environments.

The key features of managed environments are:

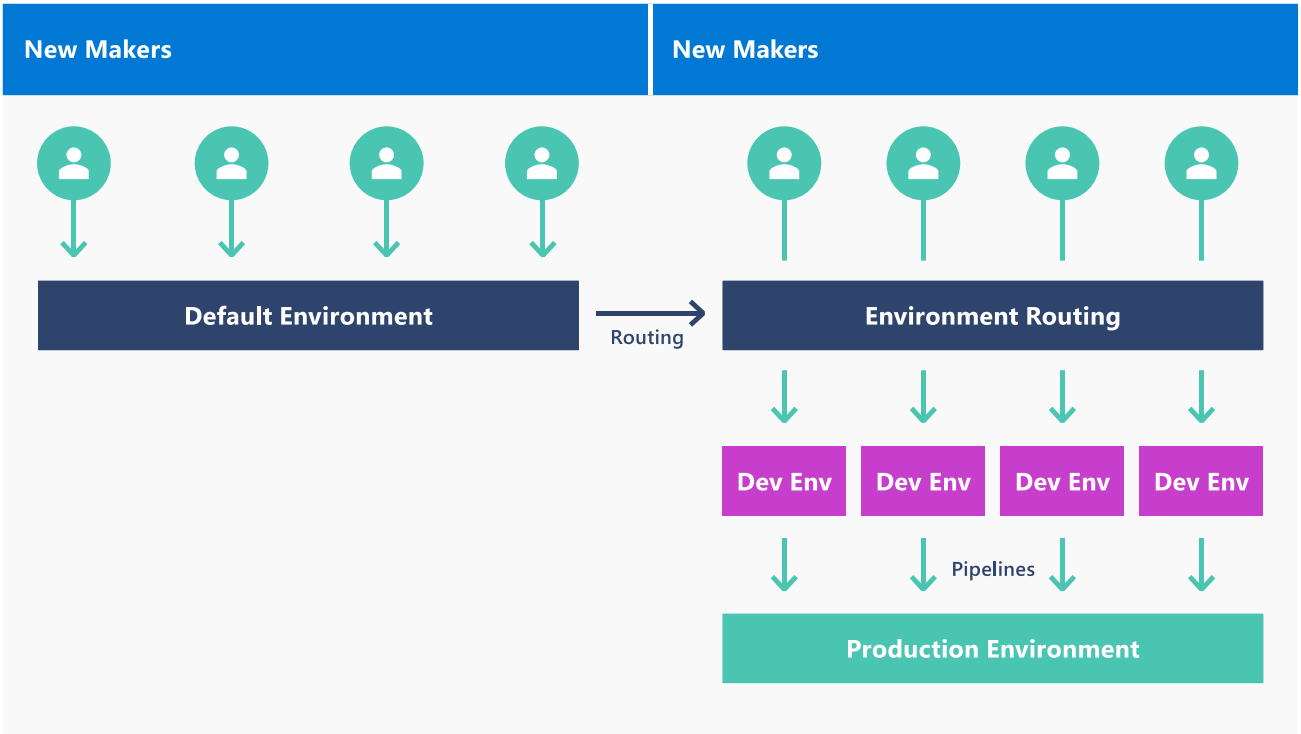
- **Limit sharing:** with managed environments you can set rules on how many people an app can be shared with, allowing you to control the spread of apps in development and default environments.
- **Enabling welcome content:** you can build customized welcoming experiences to developers using the environment – including training and onboarding content.
- **Advanced monitoring:** managed environments provided advanced usage analytics that is sent to administrators in a weekly email including the active number of apps, flows, and users as well as cleanup recommendations.
- **Data policies:** managed environments can have multiple Data policies applied to them and provide a feature to see only the policies applied to them.
- **Solution checker:** the solution checker will scan all solutions in the environment and can warn or prevent deployment of solutions with security issues or improper application of best practices.
- **Default environment routing:** allows administrators to automatically direct new makers into their own, personal developer environment.
- **ALM:** managed environments can make use of pipelines to deploy to non-development and non-production environments, such as deployment to a testing or staging environments.

Environment Routing

Environment routing is a feature of using managed environments leveraging Dataverse, and it allows an administrator to route new makers to their own developer default environments rather than the shared default environment. This allows you to route an entire team (or group) to a default environment specific to that team. This feature allows you to apply a set of core rules across the developer's personal default environments, that includes features like how many users any app can be shared with, healthy ALM practices, utilize pipelines to incorporate checks and balances and data policies.

Sharing limits

In Managed Environments, admins can restrict the extent to which users can share canvas apps. This governance restriction can limit the number of individuals or exclude sharing with groups. This is only available with Dataverse databases that sit within managed environments. Learn more about Limit sharing



Planning the Dataverse

The Dataverse is shared across all your environments but segmented according to environment. While this means that you can largely use the Dataverse as individual databases and file storage allocations and schemas in each environment, it also means that when you release multiple solutions into shared environments you must take care in terms of naming of tables, fields and files as conflicts can occur. You need to carefully plan your table naming strategy for applications that need to be released into shared environments to ensure that the risk of merging Dataverse tables and fields is minimized.

A sensible naming strategy can help prevent conflicts and make your use of the Dataverse scalable and supportable. A key best practice is to use a solution prefix for each table created within a solution. Use descriptive names for your columns and take care to ensure your makers are using descriptive naming standards.

Dataverse capacity starts at a baseline amount and increases an incremental amount for every per app, per flow, and premium license you have on the platform. This means that as an organization you should understand the impact new apps and users will have not only on your capacity, but also on the usage of that capacity.

Microsoft Teams, trial, preview, and developer environments do not count against your Dataverse capacity – which means that once solutions are moved into dedicated or shared

test and production environments, they then contribute to both increased incremental capacity and usage.

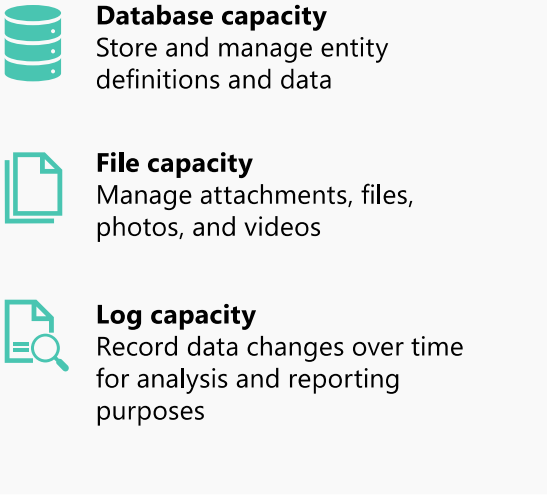
As a matter of governance, you should establish a review process when apps move from developer environments into production environments to evaluate the predicted data usage of the app and if the incremental capacity increase is sufficient to serve that solution. If it is not, you should purchase additional capacity. For many solutions, the incremental increases are sufficient in the testing environments, but once they are in production, they begin to store much more data. It is important to understand what this data growth looks like for the production version of the app and purchase sufficient Dataverse capacity to serve that solution.

You will be notified as an administrator when your Dataverse capacity is 85% used and again at 95% usage. Once you exceed your capacity you will no longer be able to create, copy, restore, or recover environments until you have 1GB of capacity available. Your solutions will continue to function and your Dataverse usage will continue to grow, but your ability to grow your environment footprint will cease until there is sufficient Dataverse capacity.

Understanding Power Apps

There are two distinct types of Power Apps: canvas apps and model-driven apps. In this section, we will drill deeper into what you should know about two types.

Storage capacity management Usage and entitlement across these categories



Model-driven apps require a Dataverse database and are built on top of the data modeled in that database. Model-driven apps create views and forms based on the data structure. Model-driven apps are mobile friendly and responsive out-of-the-box and allow business process flow guidance, which in general leads to them being used for heavy data maintenance or back-end operating teams.

Canvas apps on the other hand can be built with or without a Dataverse database. They use connectors to access data and services. Canvas apps can start from a blank screen like an artist's canvas and the creator manually lays out each screen. This allows the creator to have complete control over the placement of

controls in the app. Therefore, canvas apps are best suited to use cases where a specific user interface is required. For instance, applications used by field workers from their mobile devices.

Understanding Power Automate

Power Automate is a workflow service that allows automation tasks across multiple services using connectors or UI automation.

Power Automate cloud flows are started when a triggering event occurs, there are three types of triggers:

- Automated (when an event occurs)
- Scheduled (recurrence)
- Instant (button click)

Once triggered, the flow proceeds to execute the actions defined in the flow. Conditions are used to guide the flow to the proper actions. Cloud flows can be created:

- From blank
- From a template
- From Visio

Cloud flows created from a template can be modified and extended by the maker.

You can read more on how to create from Visio here: https://docs.microsoft.com/power-automate/visio-flows

Desktop Flows (RPA)

Extending Power Automate capabilities using desktop automation or robotic process automation (RPA) to automate legacy systems with prebuilt or custom user interface actions.

There are two distinct types of RPA automations:

- Attended and,
- Unattended RPA

Optimize resources and manage peak loads effectively through hosted infrastructure, utilizing an automated scaling mechanism and dynamic load balancing.

Process Mining

Identify and evaluate the business challenges linked to the process under analysis or improvement. A variety of pre-built templates are available for quick deployment, encompassing tasks from data ingestion to creating customized reports. Uncover possibilities for streamlining business processes and automation by utilizing data-driven prioritization and AI guidance. Take actionable steps based on insights to realize a return on investment (ROI) and institute continuous monitoring and enhancement of the process.

Copilot in Power Automate

With Copilot in Power Automate, you can speed up the creation, editing, and extension

of process automation by using natural language. Benefit from faster identification of optimization and automation opportunities through AI recommendations. Utilize built-in AI models to intelligently automate repetitive tasks related to documents and more. Additionally, transform raw data into compelling content responsibly, thanks to the built-in GPT support.

Understanding Power Pages

Power Pages is revolutionizing the way businesses create, host, and administer external-facing websites. Power Pages provides a comprehensive business solution that offers rich, customizable templates, a fluid design studio experience, and maker support via an integrated learning hub. These features make it a breeze to construct a website that tailors to your unique business needs.

With Power Pages, you get to enjoy the benefit of responsive, mobile-friendly websites that help extend your online presence. Furthermore, as a testament to its flexibility and versatility, Power Pages supports collaboration between makers and professional developers on fusion teams. Power Pages allows the utilization of Visual Studio Code along with the Power Platform CLI, to extend the functionality of Power Pages and create sophisticated and effective external-facing websites.

Power Pages leverages the shared business data stored in Dataverse, the same data used to build apps, workflows, intelligent virtual agents, reports, and analytics with other Power Platform components. This ensures a seamless and unified business operation, with data-driven decisions at its core.

Power Pages integrates neatly with other Power Platform components like Dataverse, Power Apps, Power Automate, Power BI, and Copilot. This feature significantly increases interconnectivity and interoperability, making Power Pages a holistic solution for your business website needs.

Understanding Connectors

Connectors are essentially proxy wrappers around the application programming interfaces (APIs) provided by services that allow Power Automate, Power Apps and Logic Apps to easily interact with the service. Connectors can be either public or custom. There are currently over 300 public connectors that can be used by all organizations. Examples of public connectors are Microsoft 365, Dataverse, Salesforce, SAP and more.

You may want to communicate with services that are not available as prebuilt connectors. Custom connectors address this scenario by allowing you to create (and even share) a connector with its own triggers and actions. Custom connectors are defined in the context

of an environment and are only available to apps and flows within that environment. Custom connector triggers and actions are made available within apps and flows.

Triggers are used by Power Automate to start the execution of the flow. Actions are used by apps and flows to perform a defined set of actions during execution.

The use of connectors is governed through DLP policies, and as a result DLP policies are the top-level governance control of what data and systems can be accessed from any given environment.

Integrating with your Systems and Data

The Power Platform is increasingly being used as an "agility layer" that extends functionality of core business systems and data. When establishing your Power Platform, you will want to ensure that you look at your environments through the lens of what data and systems they can and cannot connect to. It is not uncommon for Power Apps and Flows to be built, that leverage connectors into SQL Server databases, SAP systems, and custom API's.

Often organizations struggle with understanding where their data should be stored. It is advisable that data is stored in the system where it is managed. This means that instead of migrating and syncing your sales data from your CRM into a Dataverse table, you will leverage a connector into your CRM. Additionally, if you truly need to expose that data as a Dataverse table (e.g. to build a model driven Power App), you can expose that connector via a Virtual Table in Dataverse.

Virtual tables: is a definition of a table in the Dataverse platform without the associated physical tables for records created in the Dataverse database. Instead during runtime, when a record is required, its state is dynamically retrieved from the associated external system.

Create and edit virtual tables with Microsoft Dataverse - Power Apps | Microsoft Learn.

You will establish policies allowing "least privilege" rights to just the connectors that an environment needs. In this way you tightly control which environments have access to systems and data, and even to the level of which actions they can take on those systems. This fine level of governance control ensures that your environments are as secure as possible and protected from unintended and unallowed threats.

Principle of least privilege: every module in a system must only be authorized to access the minimal data and systems to perform their function).

Securing your Platform

It is important to understand the common needs of organizations as they focus on protecting their data in the Power Platform. The data protection and security landscape constantly evolve.

Organizations experience a growing sophistication and frequency of attacks to their infrastructure and data from both external and internal actors. Additionally, advances in machine learning and artificial intelligence are driving organizations to adopt "smart security" tools that automatically detect, classify, and protect sensitive data. Data access has become increasingly distributed, with organizations' workforces now spanning multiple global regions as well as serving team members who work remotely. And finally, the legal and regulatory landscape is constantly evolving and changing as new legislation and compliance requirements become necessary for organizations to abide by.

Growing sophistication of attacks

Drive to leverage data to unlock A-driven scenarios

Data access demands from an increasingly dynamic workforce

Evolving regulatory and legal requirement

Organizations increasingly want to control how their data can be protected and kept secure. The Power Platform provides robust security controls in six major areas:

- **Access controls:** controlling what people and systems have access to what data
- **Data ex-filtration controls:** controlling and ultimately preventing data from leaving the platform
- **External threats:** monitoring, detecting, and preventing attacks from external actors
- **User visibility:** monitoring how users and systems are using data
- **Regulation and compliance:** ensuring that organizations abide by major regulatory requirements
- **Risk assessment:** a holistic and specific measurement of the organizations data risk

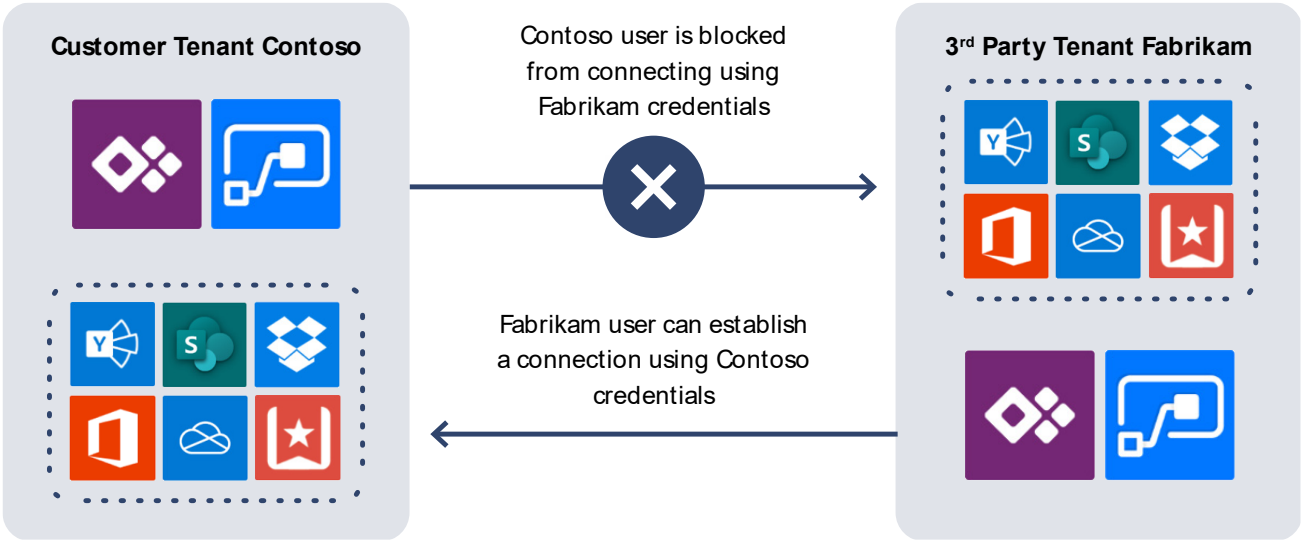
To maintain optimal security, diverse components such as security roles, Dataverse security, threat detection, and DLP policies come into play. Security roles help in establishing clear boundaries and access levels within the platform, enabling precise control over who can see and manipulate data and features. Additionally, by leveraging Dataverse security, organizations can secure data across various apps and deployments, safeguarding sensitive and critical information from unauthorized access and breaches.

Threat detection mechanisms contribute to identifying and mitigating potential vulnerabilities and attacks, fortifying the platform against unauthorized intrusions and data breaches. Implementing robust DLP policies is crucial in preventing sensitive information from being accessed or transmitted inadvertently, helping organizations to comply with regulatory requirements and protect intellectual property. All these components, when harmoniously integrated, create a fortified environment within the Power Platform, mitigating risks and elevating the integrity and reliability of organizational operations.

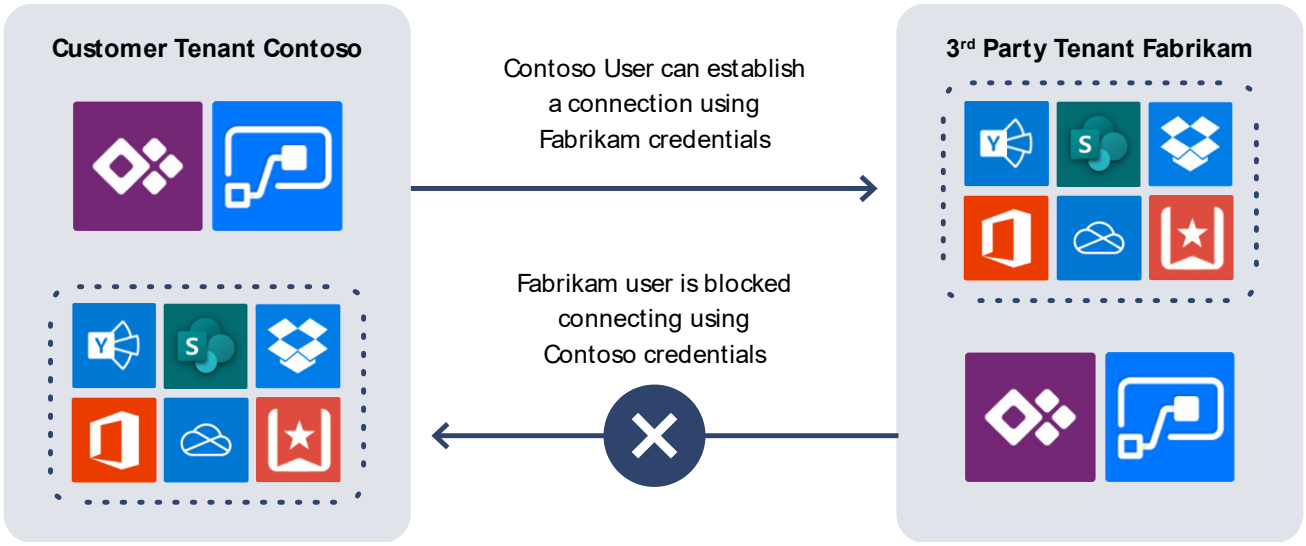
Securing your Tenant

Tenant Isolation (Cross-Tenant Inbound and Outbound Restrictions)

With tenant restrictions, organizations can control access to SaaS cloud applications, based on the Azure AD tenant the applications use for single sign-on. For example, you may want to allow access to your organization's Microsoft 365 applications, while preventing access to other organizations' instances of these same applications.



Restricting inbound cross-tenant connections restriction only applies to Power Apps and Power Automate



Restrict cross-tenant inbound connections

With tenant restrictions, organizations can specify the list of tenants that their users are permitted to access. Azure AD then only grants access to these permitted tenants.

Restricting **outbound** cross-tenant connections can be done using Tenant Restrictions (https://docs.microsoft.com/azure/active-directory/manage-apps/tenant-restrictions) that apply to all Azure AD Cloud SaaS apps, or at the API Hub level which would block outbound connections just for canvas apps and Power Automate flows.

Isolating your Network

Access to your data on the Power Platform can be regulated through a range of network isolation controls. At a basic level, the Power Platform allows you to provide controls that allow traffic, both inbound and outbound, to only come from specific IP addresses and host names. For tightly controlled environments, you can set these controls to ensure that your platform is only accessible from company networks and only connects to certain infrastructure within your corporate network. Another way this can be accomplished is through the use of service tags in conjunction with Microsoft Azure tools like Azure.

Firewall and Network Security Groups. By using service tags, you can control network level access at a service level instead of an IP and port level – minimizing the complexity of updates and configuration.

https://learn.microsoft.com/en-us/power-platform/admin/connector-endpoint-filtering

Configuring IP Firewalls

Organizations can secure their Dataverse data through a new preview feature called IP Firewall. The IP Firewall essentially acts as a firewall only allowing access to Dataverse data from certain IP address ranges. This means that access to the data can be limited to only a specific server, cluster, or office location.

This feature is only available with Dataverse databases that sit within managed environments and is currently in preview. To learn more about how to configure IP Firewall.

https://learn.microsoft.com/en-us/power-platform/admin/ip-firewall

Block Cookie Replay Attacks

Data security in Dataverse can be compromised through the theft or hijacking of a user's "cookies". An unauthorized user achieves a session hijack by copying a valid session cookie from an authorized user and then reusing that cookie on another computer to gain unauthorized access.

To block this, administrators should enable IP address-based cookie binding, which will bind a cookie to the IP address which requested it. This means that if the user's cookie is compromised, it will not be usable on an unauthorized machine that has a different IP

address. This feature is only available with Dataverse databases that sit within managed environments. To learn more about this feature and how to enable it.

https://learn.microsoft.com/en-us/power-platform/admin/block-cookie-replay-attack

Continuous Access Evaluation

Continuous Access Evaluation (CAE) is a new feature to the Dataverse that aims to prevent the unauthorized use of access tokens. Access tokens are typically granted by the platform for a period that is configured by administrators. This means that should the status of a user's access change in the time since the token was issued but before it has expired, the user will have unauthorized access until it expires and fetches a new, limited token.

To prevent this, administrators can enable Continuous Access Evaluation which will validate a user's access token every time it is used, regardless of the expiration. This can prevent exfiltration threats and allow administrators to make real time adjustments to a user's authorization and roles. This feature is only available with Dataverse services and is currently in preview. To learn more about Continuous Access Evaluation.

https://learn.microsoft.com/en-us/power-platform/admin/continuous-access-evaluation

Conditional Access

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

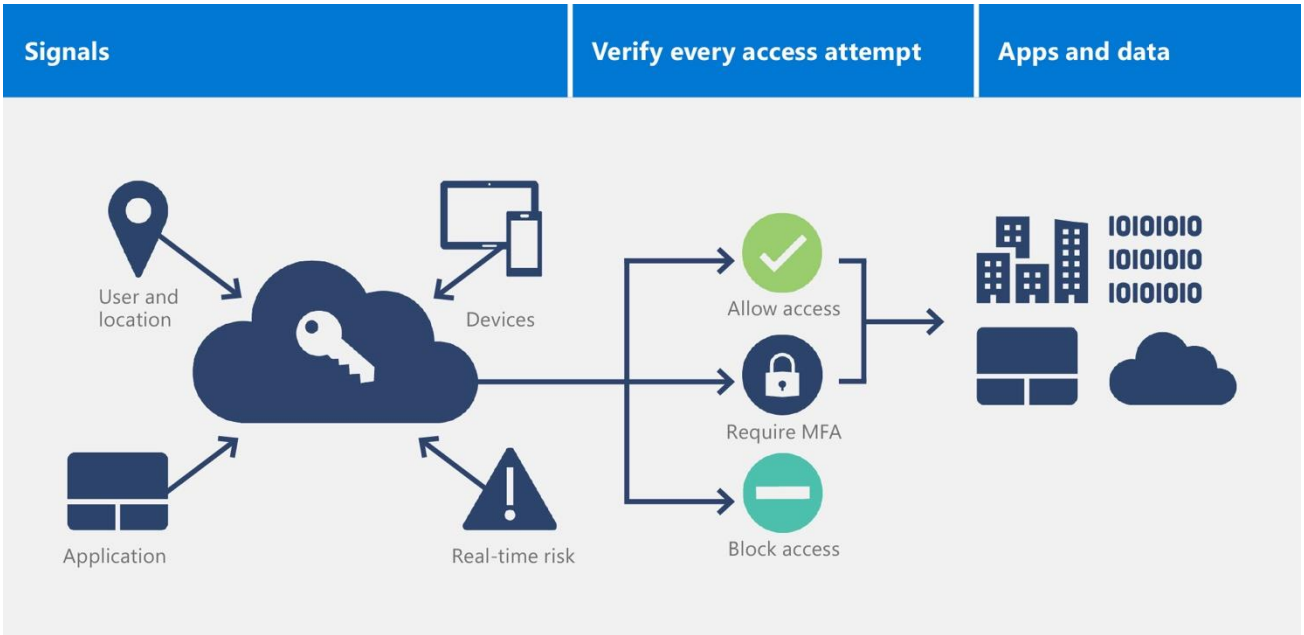
Administrators are faced with two primary goals:

- Empower users to be productive wherever and whenever
- Protect the organization's assets

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed. Conditional Access policies are enforced after the first-factor authentication has been completed.

Privileged Identity Management

You should make use of Entra ID's Privileged Identity Management (PIM) to manage access to highly privileged roles such as the Power Platform administrator role, production environment administrator roles, Dataverse System Administrator and System Customer roles. Using PIM, allows you to provide just in time privileged access to the administrative capabilities of the Power Platform. Your administrator will request access to elevate to



the administrator role. Using PIM you can assign the user to the necessary administrator group for a time bound period. The request, the approval, and the actions taken are then recorded in the audit log for compliance purposes. To learn more about PIM: Plan a Privileged Identity Management deployment - Microsoft Entra | Microsoft Learn

Protecting Business Data

Understanding Data Loss Prevention

Data Loss Prevention (DLP) policies enforce rules for which connectors can be used together and which are blocked and not usable at all. Connectors are classified as business, non-business or blocked. A connector in the business group can only be used with other connectors from that group in the same app or flow. A connector that is blocked can't be used by any app or flow.

- DLP policies act as guardrails to help prevent users from unintentionally exposing the data
- DLP policies can be scoped at the environment and tenant level offering flexibility to craft policies that are sensible and don't block productivity
- Environment DLP policies cannot override tenant wide DLP policies
- If multiple policies are configured for one environment, the most restrictive policy applies to the combination of the connectors
- By default, there are no DLP Policies implemented in the tenant
- Policies can't be applied at the user level, only at environment or tenant

- DLP policies are connector aware but do not control the connections that are made using the connector by default.
- Using endpoint filtering configuration on the connector policy, you can control and limit which services the connector can connect to
- All actions can be performed by default with a connector, but using action control policies allows you to restrict actions. For instance, you can limit the SQL Connector to execute only stored procedures and no other SQL commands
- PowerShell and admin connectors can manage policies
- Users of resources in environments can view policies that apply

By default, all connectors are considered part of the no business data allowed list (non-business) and no connectors are included in the business data only group. This effectively means that all connectors can be used with other connectors on non-business data.

When new connectors are added, they are added to the default category which is no business data allowed. Choose the default policy for your organizations use cases – for example in a highly controlled and restricted enterprise, your default policy might be restrictive and only allow a limited number of connectors. It is important to weigh the agility of your makers against risk. You can leverage very restrictive policies in production and sensitive environments, and policies that allow safe experimentation in developer environments. It is recommended to have a process in place to analyze new connectors and add them to the appropriate category – for example, a Power Automate flow could inform you of new connectors prompting you to categorize them.

The blocked group allows you to block a connector all together completely. For example, if you place the X (Twitter) connector in the blocked group, nobody would be able to create a Power App or a Power Automate flow that uses that connector.

All third-party connectors can be blocked, and all Microsoft owned premium connectors (except Dataverse) can be blocked. You can find a list of connectors that can't be blocked here. If a connector is grouped differently by multiple policies, the most restrictive policy is applied.

So, if one policy blocks a connector in an environment it is blocked regardless if other policies allow its use.

Email Exfiltration Controls

One of the ways that secured data can leave an environment is through the sending of email through the Outlook connector. Exchange admins can prevent email exfiltration by implementing exfiltration controls based on the email headers. Emails sent from Power Apps or Power Automate

place a x-ms-mail-application header and a x-ms-mail-operation-type header that defines if the mail was sent or forwarded. By using these controls, Exchange admins can ensure that data is not egressed to external properties through the Power Platform connectors. To learn more:

https://learn.microsoft.com/en-us/power-platform/admin/block-forwarded-email-from-power-automate

Threat Detection with Sentinel

One major governance challenge with the Power Platform is that through the simple to use, easy low-code and no-code development, makers can create new apps and flows who might not have a reasonable understanding of security awareness.

While DLP policies, a well-defined environmental strategy, and effective role governance offer essential control measures, they do not actively monitor day-to-day usage for potential threats and issues. With Sentinel integration for the Power Platform, you can monitor the platform from ongoing operational threats such as unauthorized geographies, suspicious data destruction, phishing attacks, flow activity by departing employees, and the change of DLP policies.

Sentinel collects all your logging, audits, and events into the logging workspace. From there Sentinel detects suspicious, malicious, and illegitimate activities on the platform and raises the proper notifications for admins to investigate the threats. This can help to prevent insider attacks, improve incident response time, comply with regulator and certification requirements, and augment your security infrastructure with the Power Platform.

Content Security Policy

A Content Security Policy (CSP) allows you to control what content header can be sent for model-driven and canvas apps at the environment level. This policy allows you to control what sorts of scripts, styles, fonts, and iframes can be included in your makers apps for an environment. Model-driven and canvas apps CSP policies are controlled and enforced separately. It is best practice to first enable and enforce the CSP on a developer or test environment first to ensure that no necessary includes are blocked by policy. Once you have verified the operation in a lower environment, it is suggested to first enable report-only mode in production, and then finally enforce the policy in production. To learn more about setting up a CSP to protect what content your apps can reference and include, visit Content security policy - Power Platform | Microsoft Learn.

Understanding Access Controls

Security roles play an essential role in defining and regulating access and permissions within the suite of tools, ensuring robust administration and governance. They are crucial as they enable organizations to

Persona	Details	Environment has Dataverse	Environment does not Dataverse
Environment admin	Can perform all administrative actions on an environment.	System admin (predefined) security role.	Environment admin role assignment.
Environment maker	Can create resources (e.g., apps and flows) in an environment but cannot make administrative actions on the environment itself. If Dataverse is provisioned, they can optionally be assigned maker access to the database.	Environment maker (predefined) security role for canvas apps and Power Automate. System Customizer (predefined) security role for model-driven apps/Dataverse customization.	Environment maker role assignment.
End user	Can access assets like apps and flow buttons that are shared with them but cannot create assets themselves. Note that end users are not given permission to the environment itself, they're only shared access to the applications and database that are located in an environment.	Customized security role that provides access to assets in the environment (such as Dataverse and model-driven apps). If using canvas apps, access is shared the same as non-Dataverse environments – at the app level. Custom security roles are created to support applications built in your organization. Custom security roles can also come with applications you install from AppSource or if your users sign up for Dynamics 365.	Users are shared access to the canvas app (no environment role assigned).

maintain control over who has access to what within the platform, thereby protecting sensitive data and intellectual property, as well as maintaining compliance with relevant laws and policies. Security roles in Power Platform allow administrators to assign varying levels of access to different users, ranging from full control to read-only, based on their job functions and responsibilities.

One of the highest levels of role control is the security group. Leveraging Entra ID's security groups, you can add users to different groups, and grant the necessary access to that group. All environments, when created, should be created with reference to a security group that has access to that environment. While environments can be created without a

security group and open to everyone, it is best practice to ensure that environments are targeted in their use and availability through the assignment of a security group. The exception to this is the default environment, which is open to everyone. This has security implications and is one of the reasons why the default environment should only be used for personal productivity and not production apps and data. Using security groups, you can group your users through their role, such as developers, and give them access to sandbox environments for testing. You can also create security groups for teams and give teams access to shared environments.

Securing your Environments

The distinction of the Power Platform from other low-code alternatives already employed within your organization (such as Excel or Access) or other Shadow IT point-solution SaaS providers, lies in the fact that all operations are regulated and authenticated via Azure Active Directory (AAD) – you need to sign in with your Work or School Azure AD account to use this service. This means that as an admin, you have full visibility of everything your makers and users do – it is governable, automatable, auditable and manageable by default.

In this section of the paper, we are going to look at how the Power Platform handles security from user authentication to authorization which allows users to perform actions with data and services.

Conceptually, security in the platform is there to ensure users can do the work they need to do with the least amount of friction, while still protecting the data and services.

The following is a high-level look at how the multiple layers of security make up the security model of the Power Platform:

- Users are authenticated by Entra ID, and use can be restricted using conditional access policies
- Ability to create applications and workflows is controlled by security roles in the context of environments.
- A user's ability to see and use Power Apps resources is controlled by sharing.
- The application with the user. Sharing of Power Apps canvas apps is done directly with the user or Entra ID groups. Sharing of Power Apps model-driven apps is done via assigning the user the appropriate Dataverse security role.
- Environments act as security boundaries allowing different security needs to be implemented in each environment.
- Power Automate flows and canvas apps use connectors. The specific connections credentials and associated service entitlements determine permissions when apps use the connectors.
- Environments with a Dataverse instance add support for more advanced security

models that are specific to controlling access to data and services in that Dataverse instance.

- Connector use can be further restricted with DLP policies. Cross-tenant inbound and outbound restrictions can also be applied to the connectors.

It is important to note, that when accessing data sources via connectors all the underlying security that the data source offers is in addition to the layers of security described above. Power Apps and Power Automate do not provide users with access to the connector data source they do not already have. Users should only have access to data that they really require access to.

Configuration of environment settings is key for controlling access, data policies, connectors, and permissions. Assigning appropriate roles – Environment Admin, Environment Maker, and Environment User – ensures that users have precise privileges within each environment.

Understanding Role Access in Dataverse

- Within the Dataverse, various security roles and controls are established to manage and safeguard data. Security roles in Dataverse are a combination of various sets of permissions that define the access level users or teams possess over records. These roles are crucial as they determine who can read, write, delete, append, assign, or share the data, and whether the access is organization-wide, user-owned, or confined to business units. These roles can be customized or used as predefined to create a security model that meets an organization's specific needs, ensuring that sensitive information is adequately protected and only accessible by authorized users.

Security role/control	Description
Security roles	Define the access level users or teams have over records within the Dataverse. Can be organization-wide, user-owned, or confined to business units. Can be predefined or customized.
Row-level security	Restricts access to specific rows in a table based on security roles.
Field-level security	Secures specific fields in a table, allowing administrators to restrict access to sensitive data fields.
Entity-level security	Allows administrators to restrict access to entire tables within the Dataverse.

Five steps to building a Layered Security Structure

Step 1: identify who or what groups of people (such as departments, sections, or teams) will have access to the app itself. This should be the same set of people you identified in the planning phase.

Step 2: among those users you identified in step 1, divide them into groups who will (or won't) have access to restricted types of information.

Step 3: identify the requirements for who can see the records.

Step 4: if you're using data sources other than Dataverse – or services that don't have Microsoft 365 or Azure Active Directory authentication – you should consider how you'll allow access to those systems. If you aren't in charge of those systems, seek advice from those service administrators.

Step 5: based on the above steps, you should consider how these different groups will be managed. We recommend that you use security groups.

Additionally, Dataverse implements a range of security controls such as row-level security, field-level security, and entity-level security to manage access to data tables, rows, and fields.

Row-level security allows administrators to restrict access to specific rows in a table based on security roles, ensuring that users only see the data they are permitted to. Field-level security is employed to secure sensitive fields in a table, and entity-level security restricts access to entire tables.

By utilizing these diversified controls and roles, organizations can create a robust security structure, allowing precise and secure access to data, which is crucial for maintaining the integrity and confidentiality of information within the Power Platform.

- Governing User Access

One of the first acts of governance with your platform is designing your policy and controls around user access. It is important when building an access policy to implement user access using a layered approach. You will need to design your layered approach specifically for applications that are released and shared as production environments.

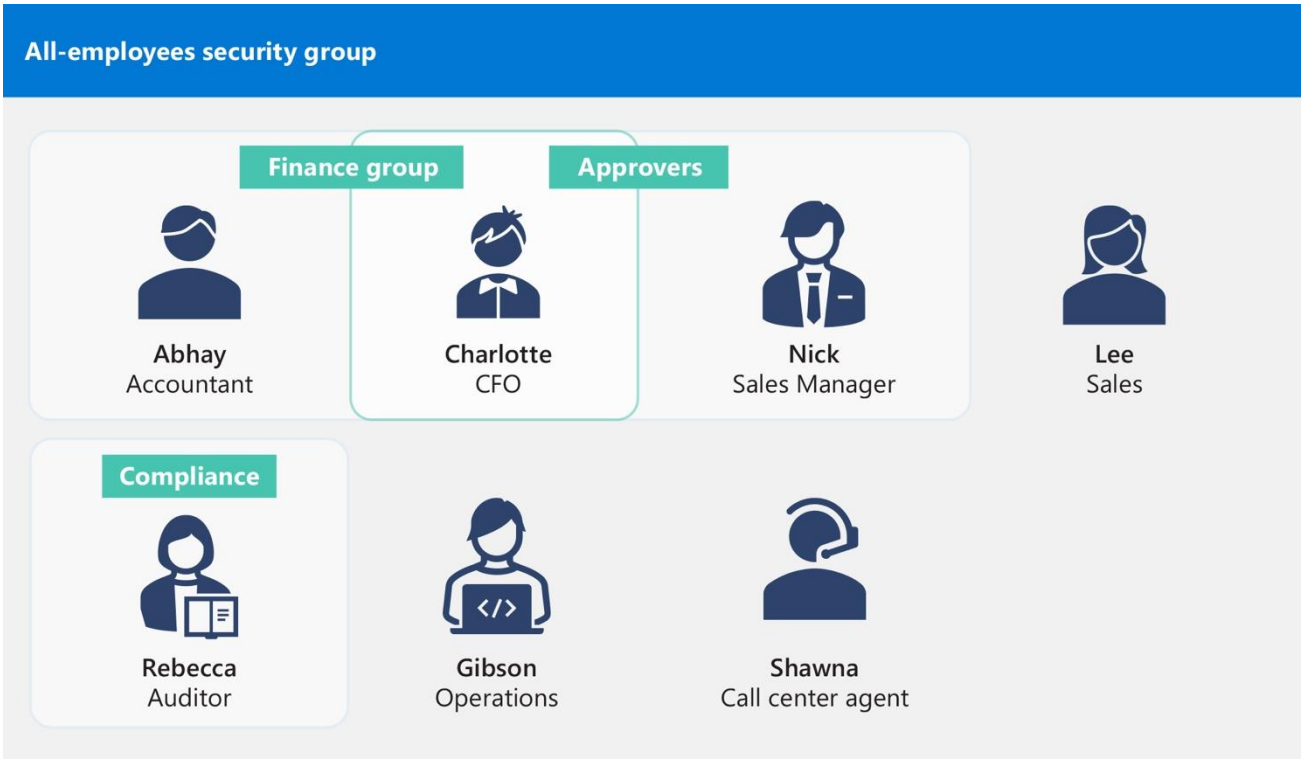
With layering, you evaluate the application on four tiers and develop groups for each tier. Finally, you design who belongs to each group. To design a layered security approach, you must evaluate and create groups with the following scopes:

- **Evaluate who has access to the app:** this is app level security. For production apps this could be entire departments, teams or even the entire organization.

- **For model-driven apps:** different forms within the application might have different security groups. For example, in an app that is for employees to submit a work request, the work request form will be open to all employees, while a back-end form to review and approve the request would only be accessible to the approval team.
- **Assess restricted data access for specific groups:** for example, members of the Legal team can only see records for the legal department – this becomes your record level security strategy.
- **Securing sensitive data fields in records:** determine if there are fields in your records that should be restricted such as Personal Identifiable Information (PII) data and restrict those via field level security.

Understanding Hierarchy Security

Organizations often have a need for managers and people leaders to be able to access and act on behalf of their direct reports. To accomplish this, the Power Platform takes advantage of hierarchy security. The hierarchy security model in Power Platform allows configuring granular data access based on organizational reporting structures. There are two choices available: one is a manager hierarchy that relies on direct manager-subordinate relationships, and the other is a position hierarchy that assigns users to specific roles within a hierarchical structure. With both, higher levels gain access to data of users below them in the hierarchy, with the depth setting controlling how many levels this propagates. For example, the CEO could get ready access three levels down, including direct reports, their reports, and teams.



Hierarchy security complements business units, security roles, and teams as part of a defense-in-depth approach. For complex needs, using fewer business units plus hierarchy security minimizes broad permissions while optimizing governance. For example, an organization could have five business units but 50 locations – adding location-based position hierarchies prevents excessive business unit proliferation. When thoughtfully combined with other tools, hierarchy security allows precision access aligned to the organization while reducing overhead of excessive business units and roles.

Organizations with rapid user growth, frequent restructuring, or highly complex teams and divisions can benefit from evaluating hierarchy security. As organizations scale and change, business units and security roles often cannot provide sufficiently granular yet flexible access management. Hierarchy models align to intuitive reporting structures, enabling access delegation and oversight based on shifting lines of authority. This reduces the proliferation of business units and roles otherwise needed to restrict data leakage across global divisions.

Compliance demands, audits showing excessive permissions, or high costs to reconfigure static security also indicate hierarchy security's advantages. Its precise access scope and definitions can meet stringent controls, like in healthcare. Hierarchy security lessens the need to rebuild business units and roles after reorgs. Its lower maintenance overhead saves time and effort compared to constantly reconfiguring business units, teams, and security roles amidst organizational churn. For dynamic growth or regulated industries, hierarchy security is a crucial governance tool.

Power Automate Automation Security

Power Automate Desktop Flows used for robotic process automation (RPA) to automate legacy systems with prebuilt or custom user-interface actions have resources within the Azure and Power Platform environments which will require administrators to setup securely and with resilient mechanisms of controlling access.

Ideally, attended, or unattended automated flows should run on dedicated virtual machines (VMs). To ensure security, it is essential to implement specific controls, such as establishing secure communication for Azure resources through a virtual network, configuring network security group (NSG), and organizing Machine Groups.

Securing RPA automations is fundamental to ensuring the safe and compliant use of data and associated automation technologies by the appropriate end users. Administrators play a pivotal role in establishing a secure foundation that includes authentication, authorization, and encryption.

Establish secure communication for Azure resources (virtual network)

Establishing secure communication for Azure resources involves several key steps. Create a virtual network to serve as the foundation for connecting and isolating your Azure resources. To enhance security, assign a unique address space to each virtual network, ensuring that they operate independently and avoid potential conflicts.

Virtual network integration of Azure services for network isolation | Microsoft Learn

Configure Network Security group (NSG)

Set up Network Security Group (NSG) by defining both inbound and outbound rules for network traffic to the subnet. Make sure to assign unique priorities to each rule to ensure proper configuration and management of network security.

Virtual networks and virtual machines in Azure | Microsoft Learn

Organizing machine groups

Machine groups enable the grouping of multiple machines, aiding in the distribution of automation workloads and enhancing overall productivity. Power Automate Administrators should register dedicated machines for RPA processes and establish machine groups to facilitate the scaling of automations. Managing access to machines and machine groups can be assigned to individual users or user groups and should be restricted to makers within the context of the solution.

Manage machine groups - Power Automate | Microsoft Learn

Staying Compliant with Regulations

The Power Platform provides a variety of features that help ensure your organization's data is safe and meets a variety of compliance standards. The Power Platform is built on Microsoft's comprehensive approach to security, compliance, and privacy. There are a wide variety of compliance standards that the Power Platform meets that are national, regional, and industry specific. Some common standards are FedRamp, HIPAA, FACT, and FISC. The Power Platform is additionally GDPR compliant. You can learn more about your organization's regulatory compliance through the Microsoft Trust Centre.

It is important to note that environments are geographically linked and that data that resides within an environment's Dataverse remains in that geography. Your data is persisted in a highly durable way within that geography, but the data stays resident to the location the environment is provisioned in. Organizations that have multi-geography needs can take advantage of geographically separate environments to ensure data residency requirements.

Customer Managed Encryption Keys

By default, all of your data stored on Microsoft server's is encrypted using Microsoft managed keys. However, to further secure your data, you can opt into controlling the encryption keys that your data is encrypted with. You do this by generating your own RSA-HSM key and storing it in Azure Key Vault. You then create a Power Platform enterprise policy for your key and permission to access the key vault. You then create an enterprise policy to encrypt your individual environments with your new key. Choosing to use Customer Managed Keys (CMK) can give you added control over your data, but it does require you to safely manage your keys and ensure you have best practices managing the key vault in your Azure platform. It is important to note that data that already exists in an environment managed with a Microsoft managed key, will continue to be encrypted via the Microsoft managed key. Customer managed keys are only available to encrypt the data in managed environments.

Understanding the Customer Lockbox

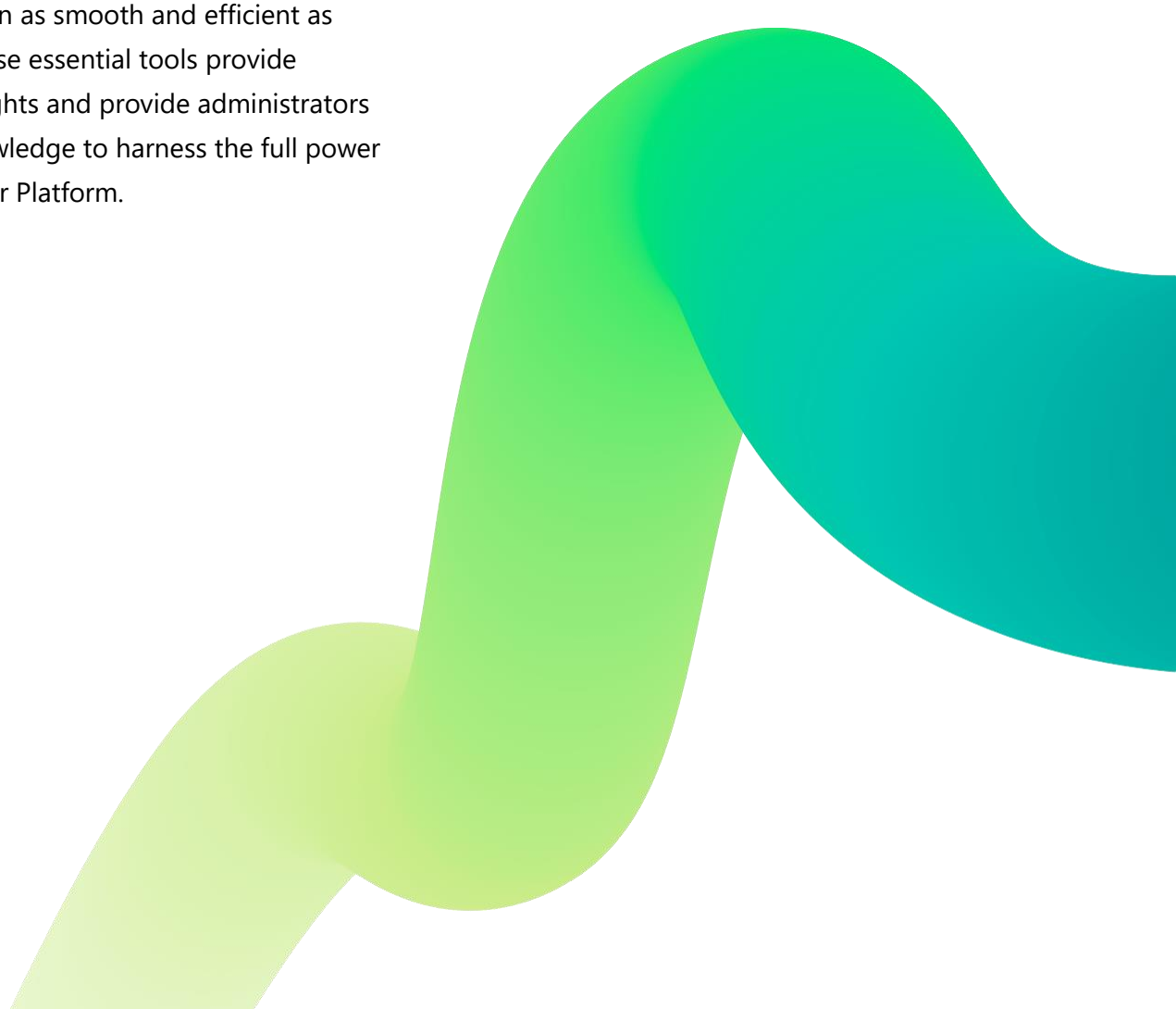
Another way to secure your data and ensure access compliance is using the Customer Lockbox. The Customer Lockbox feature, exclusively accessible in managed environments, ensures that in the event Microsoft personnel require access to your data to address a support request or issue, you will receive a prompt to either approve or reject this access via the lockbox. These requests and responses are recorded in the audit logs and show a complete story of Microsoft's access to your data during support tickets.

Monitoring your Platform

The transformative potential of the Power Platform allows businesses to optimize operations and improve productivity. However, to fully realize this potential, it is crucial to monitor and administer the platform effectively. Effective monitoring conveys numerous benefits including enhancing performance, ensuring security and compliance adherence, troubleshooting, resource and cost management, and proactive issue prevention.

There are a host of user-friendly tools available, all geared towards making Platform administration as smooth and efficient as possible. These essential tools provide valuable insights and provide administrators with the knowledge to harness the full power of their Power Platform.

To administer the Power Platform, an administrative user does not need to be allocated a Power Platform license. Click here to learn more.



Monitoring the Power Platform effectively involves focusing on four major areas: licensing, data, usage, and auditability. Each of these areas plays a critical role in ensuring the platform operates efficiently and within the boundaries of organizational and regulatory requirements.

Licensing is a fundamental aspect of Power Platform administration. Effective monitoring of licensing ensures that the organization is compliant with Microsoft's terms of service and avoids unnecessary expenses. By keeping track of the types and numbers of licenses in use, administrators can optimize their licensing strategy to match their actual needs. This not only prevents overspending on unused licenses but also ensures that all users have the appropriate level of access to the platform's capabilities. Regular reviews of licensing usage can highlight trends and inform future purchasing decisions, ensuring that the organization remains agile and cost-effective in its use of the Power Platform.

Data monitoring is another crucial area, focusing on how data is stored, accessed, and used within the Power Platform. This involves ensuring data integrity and security, as well as compliance with data protection regulations such as GDPR or HIPAA. Effective data monitoring helps in identifying and mitigating risks related to data breaches or misuse. It also involves overseeing data flows between different applications and services within the Power Platform, ensuring that data is accurate, up-to-date, and available to those who need it, while preventing unauthorized access.

Usage monitoring is about understanding how the organization utilizes the Power Platform. This includes tracking which apps and workflows are in use, how frequently they are accessed, and by whom. This information is vital for resource allocation, identifying popular or underused features, and understanding user behavior. By analyzing usage patterns, administrators can make informed decisions about training needs, potential enhancements, or the development of new applications. Additionally, usage monitoring can help in identifying any operational bottlenecks or areas where the user experience can be improved.

Lastly, auditability is essential for maintaining transparency and accountability within the Power Platform environment. It involves tracking changes made to the system, including who made these changes, when, and why. This is crucial for security, as it helps in quickly identifying and addressing unauthorized or suspicious activities. Audit trails also support compliance efforts by providing a clear record of actions taken within the platform, which is essential for adhering to various regulatory standards and for internal audits. Effective auditability practices ensure that the Power Platform remains a trusted and reliable tool for the organization.

Monitoring Licenses

License management is one of the core types of Power Platform monitoring that administrators will have to perform. Effective license management is a balance between ensuring that your organization is not only properly licensed for the features and solutions required, but also that you are licensing to enable and grow your organizations effective use of the Power Platform.

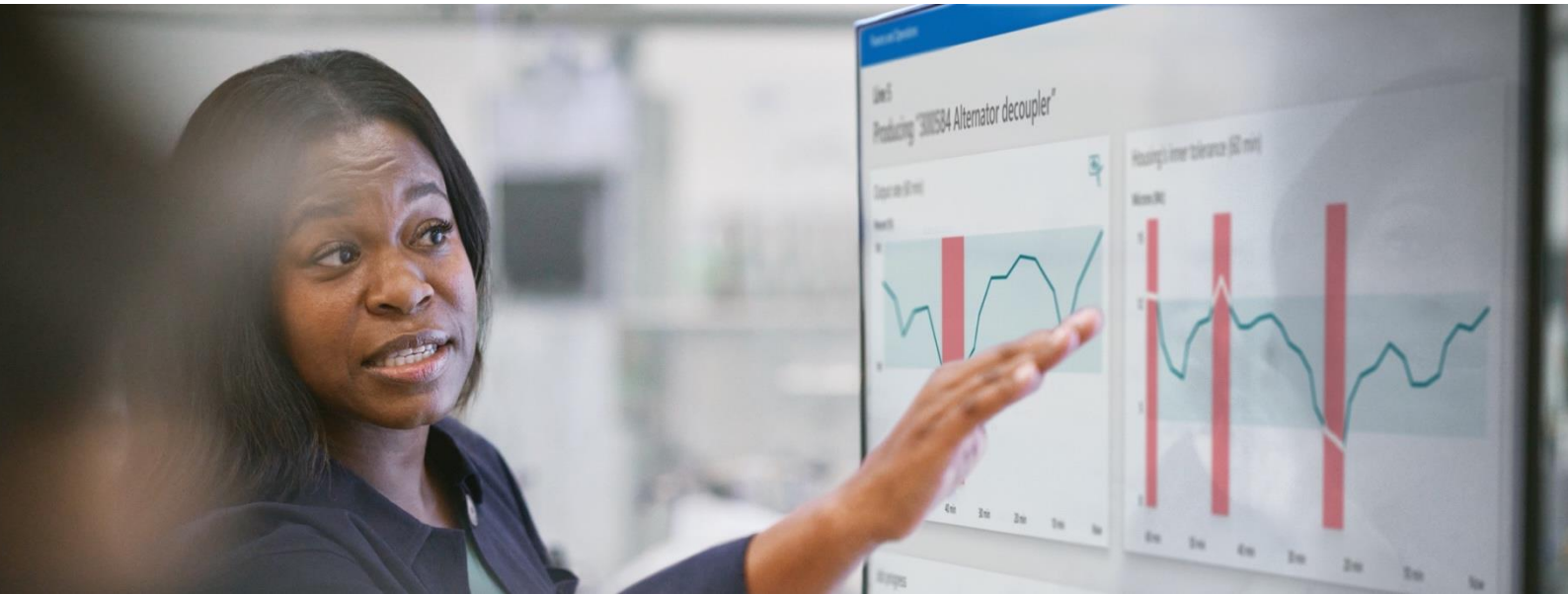
Licensing with the Power Platform is done on a per product basis. There are licensing options for a variety of implementation types. The Power Platform provides a variety of governance tooling to help with the management of these licenses.

At its core, Power Platform capabilities are included with Microsoft 365 and Office 365 licenses. For example, Microsoft Teams includes basic use of Power Automate and Power Apps. However, additional licensing may be required to unlock the full functionality of the platform. The Power Platform premium per user plans provides comprehensive use of Power BI, Power Apps, Power Automate, and Microsoft Copilot Studio. For more advanced workloads, add-on capacity licenses can be purchased for accessing additional resources.

Standalone licenses are also available if users do not require access to the broader platform. Evaluating workload requirements and user needs is crucial for determining the appropriate Power Platform licenses. The platform's flexibility supports everything from lightweight workflows to enterprise-grade application development.

Licensing Overview

The Power Platform offers different licensing options depending on usage scenarios. Core capabilities are included with Microsoft 365 and Office 365 licenses. Various premium per user plans unlocks capabilities across Power BI, Power Apps, Power Automate and Copilot. For more advanced workloads, add-on capacity licenses provide additional resources. Standalone app licenses allow access to specific apps without a full platform license.



Product	M365 and O365 licenses	Power Apps Premium	Per app per user / Per flow per user license	Other
Power Apps	Can build Power Apps and connect using standard connectors only (useful for M365 automation and applications). Limited Dataverse within the Teams environments.	License each user for unlimited use of the Power Apps. Includes managed environments. 250MB Dataverse Database Capacity.	License one app for one user. Includes managed environment for the environment the app is in. 50MB of Dataverse Database capacity.	Pay As you Go: Pay per app per active user of the app per month.
Power Automate	Can build Cloud Flows and connect using standard connectors only.	**Premium:** Allow licensed users unlimited cloud flows for both API and RPA based automation. **Standard:** Unlimited cloud flows for API based automation.	A minimum of 5 flows are licensed for unlimited use across an organization.	RPA Addons: RPA "bots" are licensed either as hosted or unattended and are licensed per bot.

Other Products

Power Pages	Included with Power Apps licenses as a Power App or Power Pages Website. Can be licensed via "capacity packs". Packs come in tiers of 100, 10000, and 100000 users. Licenses can be for anonymous or authenticated users per month. Can also be licensed as a pay as you go.	
AI Builder	AI Builder is licensed through capacity packs – each of which is for 1 million service credits. Service credits are used for various AI functionality at different rates. For example, training an image detection model will cost 20 credits per image for the first 500 images, and 10 credits per image for each thereafter. It will then cost 8 credits per image to inference in real time.	
Power Virtual Agents	Can be used within Teams only, has access to a Dataverse for Teams instance and can make use of cloud flows for the bots.	Can be licensed per agent for up to 2000 chat sessions per month. Allows for standard and premium connectors, as well as full Dataverse access and access to managed environments.
Dataverse	Dataverse capacity is shared across a tenant. By purchasing premium licenses Dataverse capacity will increase. Dataverse has three areas of capacity – Databases which are for structured data stored in tables, Files for binary objects stored as files, and Logs for text based log data. Capacity can be added to each separately in 1GB increments.	

Choosing the right license depends on assessing workload requirements and user needs. For example, light use by an individual may be covered under Office 365, while heavier workloads will require Power Platform or add-on capacity licenses. Evaluating these factors is crucial for determining the appropriate licensing. The platform's flexibility supports everything from lightweight workflows to enterprise-grade application development.

Licensing Monitoring

Monitoring license usage is an important aspect of ensuring not only that your licensing is adequate, but also ensuring that you are not over provisioned for licensing.
The primary method of monitoring your Power Platform license usage is through the Power Platform Admin Center's License consumption screens. This feature allows administrators to see the active licenses, as well as see which environments might be having license troubles.

Licenses can be allocated in a variety of ways, including through the Azure Poral, with an Azure Pay as you Go subscription, and through the Power Platform API. Your governance team should work closely with your Azure and Entra teams to determine how you will control and action the licensing of users within the other tools. In small organizations, your Power Platform administrators can often also serve this function, but in larger organizations this will likely be controlled through a service request to another team.

The summary tab allows you to see which environments might be having licensing troubles and allows you to quickly assign per user and per app/flow licenses to those environments, apps, flows, and or users. By default, this screen only shows managed environments but can also be used to show license issues in standard environments.

On the environments tab you can select the environment and the Power product and see the license consumption for that environment. You can see which license types are in use, the number of active users, and the specific user using an app or a flow. Additionally, the license consumption screen will show you recommended actions, including the conversion of the environment to a managed environment.

Managed Environment Monitoring

Managed environments have an additional interface to see the licensing details for the managed environment. This feature is only available for managed environments. Under the Billing->Licensing area of the Power Platform Administration Center you can see a summary of the license usage for Power

Apps and Power Automate within each environment. Power Platform usage analytics can provide valuable insights into license consumption to optimize governance. Administrators can identify what types of

licenses are launching apps and executing flows, how many users are actively using Power Apps and Power Automate in each environment, and which specific users are consuming licenses. This helps determine if any users need standalone licenses provisioned.

Usage analytics also enable assessing license compliance, such as identifying flows that may be out of compliance. By leveraging this data, organizations can right-size and allocate licenses efficiently and ensure compliance with licensing policies across environments. Robust usage analytics are crucial for optimizing Power Platform governance as adoption grows.

Licensing Connectors

With Microsoft 365 licenses, makers are automatically licensed to begin creating Power Apps and Flows within developer, trial, or their default environment with "standard connectors" only. The standard connectors are a series of connectors that facilitate connection to the data within the Microsoft 365 suite of products including OneDrive, Outlook, and SharePoint. These connectors are typically used to facilitate automation and extension around Microsoft 365 applications.

Many other connectors are Premium connectors and can only be used for with per app or per user licenses for Power Apps or Power Automate. They can also be used with Microsoft Copilot Studio licenses and Dynamics 365 licenses. Premium connectors are incredibly powerful and are commonly used to connect to third party APIs and core business critical systems.

Trial Plans

Users can self-service trial plans that allow use of Power Apps and Power Automate for 30 days. This allows users the ability to build for free for a limited time and will be prompted that they need to convert to a normal license once they are ready to move their app or flow to sharing with more users. This is an excellent time to evaluate the application and understand where in your environment strategy it will fit. You can then help to facilitate the packaging and movement of that app to the proper environment as well as fully license the user and/or app for it.

Developer Plans

Developer plans allow a user to self-sign up for an environment that can be used to build their apps and flows. The Power Apps Developer plan allows a user to self-sign up for a development environment to build and test with Power Apps, Power Automate, and Dataverse.

These environments have restricted capacity and can be shared with team members for development and testing purposes. These are excellent ways to

allow your makers the ability to get started experimenting and building with the Power

Platform, and its premium features, without incurring license costs. When a user is ready to move their solution into a shared environment, you can facilitate moving the app with Pipelines to a shared environment. At that point you can also evaluate how to license the app. To learn more:

https://powerapps.microsoft.com/en-us/developerplan/

Pay-as-you-Go

Pay-as-you-Go licensing allows you to pay for Power Platform usage using your Azure subscription. It allows you to use the power platform and pay just for your consumption without any commitment or upfront licensing. Makers can share apps and flows, and only pay for when they are used – always ensuring that you are licensed optimally for any given app or flow. Additionally, you can allocate these costs to a subscription, enabling enterprise features like cost-back where you bill business units for their usage of services. To view a case study:

https://customers.microsoft.com/doclink/1435340411391867976-t-mobile-telecommunications-power-platform

Request a license

Employees launching a premium app can seamlessly interact with an administrator to request a license through a process directly within the app.

Makers can also request a license on behalf of their users within the maker studio which will be sent to the administrator for approval.

Once the user has requested a license the request appears in a queue within the Power Platform Admin Center for administrators to approve.

Auto-claim for Power Apps Premium

Simplifies allocation of licenses from a pool of license when launching an app within a managed environment without needing an administrator to assign a license upfront. Automatic claiming for Power Apps is a feature of managed environments, accessible only when a user is accessing an app within a managed environment and a policy has been set up within the Microsoft 365 admin center.

Upon configuring a policy, any user within the organization in need of an individual Power Apps license is automatically assigned one under specific conditions. If user does not possess a standalone Power Apps license and accesses an app requiring a premium license, the system automatically user does not possess a standalone Power Apps license and accesses an app requiring a premium license, the system automatically allocates a Power Apps per user license to that user. If a user without a standalone Power Apps license launches an app within a Managed Environment, they are automatically provided with a Power Apps per user license.

This automated process ensures that users have the necessary licenses based on their app usage and environment requirements.

Manage auto-claim policies in the Microsoft 365 admin center | Microsoft Learn

Storage, Limits, Allocations

Licenses have a few limits and allocations as it pertains to usage of storage. Your Dataverse storage is shared across your entire tenant regardless of how many environments you have. Your Default environment starts with a small allocation, and you accrue additional storage to the tenant for each premium per app license, per user license for both Power Automate and Power Automate. You also accrue capacity for extra Power Page allotments.

Dataverse environments have 3 types of storage:

- **Database storage** is storage for tables, which comprise the structured data within your applications. Dataverse database storage starts with a 3GB allocation in the default environment.
- **File storage** is for the storage of files that are used within your applications and flows. This can include visual and UX assets, or files that are consumed in the course of the operation of your application. You start with 3GB of Dataverse file capacity in the default environment.
- **Log storage** is for the storage of logs of the platform. All auditable actions are logged to the logging area of the Dataverse. This uses the AuditBase and PluginTraceLogBase tables in Dataverse by default.

Another key licensing concept to be aware of is the request limits and allocation. On a daily per user basis, API usage is tracked across Power Apps, Power Automate workflows as well as direct developer API usage. The usage is expected to stay below the API request allocation that is provided based on the type of usage. The allocation as well as usage is tracked at the user level and not at the tenant level. The allocations have been designed so that most users will never exceed the limits.

You can monitor basic usage metrics in the admin portal and more detailed usage will be provided in the future. Administrators should work with app makers to help them design their solutions to stay within the limits. If usage for a user continuously exceeds the limit an add-on is available to increase an individual user's limit. For more details on request limits and allocations review here: http://aka.ms/platformlimits

Power Apps and Power Automate API request capacity add-on allows customers to purchase additional requests which can be assigned to

any user who has a Power Apps/Power Automate license as well as Dynamics 365 license.

These can be assigned to an application, and administrative and non-interactive users. Each capacity add-on provides an additional 10,000 requests/24 hours which can be assigned to any user.

Multiple capacity add-ons can also be assigned to the same user.

Monitoring Data

Data Classification with Microsoft Purview

Govern your business applications data with Microsoft Purview | Microsoft Power Apps

Monitor and protect data with Microsoft Purview | Microsoft Learn

Microsoft Purview Data Map supported data sources and file types | Microsoft Learn

Purview comprises a suite of data governance, risk management, and compliance solutions designed to empower your organization in governing, safeguarding, and effectively managing your complete data assets. As of October 2023, a private preview is available for 'Microsoft Purview Integration with Microsoft Dataverse.

The Purview integration with Dataverse offers the below key capabilities:

1. **Comprehensive Data Mapping and Discovery:** Businesses can create a comprehensive data map. This data mapping provides a unified overview of the data estate, encompassing integrations with many Microsoft and 3rd party data sources. By incorporating Dataverse insights with wider organizational data, businesses are empowered to make more informed data-driven decisions and adeptly manage their valuable data assets.

2. **Automatic Data Classification:** Business will be able to extend Purview classification system to be able to automatically detect and classify sensitive data stored in Dataverse. Security managers will be able to leverage pre-created classifiers or create their own. By automatically recognizing sensitive data, organizations can enhance their protective measures and mitigate the risks associated with data exposure.

3. **Data Security and Governance:** Security managers and data curators can harness Purview to oversee your entire organization's data estate effectively and centrally. Purview allows the creation of data policies that enables organizations to control access to data. By utilizing Purview with Dataverse, security managers can create or extend existing compliance policies and procedures, ensuring robust data security and governance.

Once integrating Dataverse with Purview and crawling your Dataverse content, the next step

is to analyze your data and create comprehensive classifiers. In Purview, classifiers are separated into “Classifications” and “Classifications Rules”.

Classifications serve as the identifier for your classifier, essentially a label that will be affixed to the corresponding data. On the other hand, Classification Rules are conditions that must be satisfied for the classification to be automatically applied. A single classification can encompass multiple rules. As of October 2023, there are two custom rule types at your disposal, ‘Regular Expressions’ and ‘Dictionary.’

Regular Expressions rules, as the name implies, permit the creation of regex expressions that are evaluated against your data. If a match is found, the respective classification is applied. Conversely, a Dictionary rule comprises a list of all potential values that a specific column may contain. When a match occurs, the classification is applied.

After auditing and confirming your classifications are being correctly applied. The next step depending on your organization will then be to create appropriate data policies to protect sensitive tables and to then incorporate your Dataverse insights into your organization’s wider data governance and compliance policies.

Monitoring Usage

Monitoring through the Admin Center

From the Power Platform admin portal, you can view tenant level analytics to help you manage capacity and troubleshoot problems. The analytics and capacity sections on the portal allow you to drill down into Dataverse, Power Automate, Power Apps, and Capacity analytics. Any service admin or environment admin has access to the analytics.

The Power Platform admin portal is best suited for ad hoc investigative monitoring of your Power Platform environment. The reports contained with the admin portal can be used to answer specific questions about the tenant. For example, the Overview reports in the Power Automate Analytics section can be used to determine the number of successful versus failed flow runs within the tenant. Ultimately, these reports are designed to give insight into the adoption, usage, and health of a Power Platform tenant.

Overview Reports

The Overview reports display data from Power Automate flows and Power Apps across all environments. Although filters can be used to home in on a particular environment or types of environments, these reports are set to display data across all environments by default. The primary benefit of these reports is that they provide a high-level view of the adoption, usage, and health of a Power Platform tenant. The Overview reports are organized under three headings: Usage, Maker Activity, and Inventory.

Usage

The Usage reports provide a powerful tool in assessing the level of Power Automate and Power App adoption within an organization. The Usage analytics help you monitor the following:

Adoption	Usage	Health
Apps • Number of active users • Number of new users vs return users • Number of app sessions • Number of apps Flows • Number of flows • Number of runs	• Most used app environment • Most used flows • Top apps	• Successful flows • Failed flows

Maker Activity

The Maker Activity reports provide insight into the activities of Power Automate and Power App makers across an organizations Power Platform tenant. These reports can be used to identify the most active makers, the number of first-time makers and the total number of connections being used within an organization. The Maker Activity analytics help you monitor the following:

Adoption	Usage	Health
• Top makers • First-time makers • Total number of apps created/ published/modified/deleted by makers	• Total number of connections consumed in one or more environments	• N/A

Inventory

The Inventory reports provide a comprehensive overview of all the Power Automate flows within the tenant. The Inventory analytics help you monitor the following:

Adoption	Usage	Health
• App owners • Total # of cloud flows • Flow owners	• Number of model-drive vs canvas apps • Which apps depend on specific connectors • Which flows use certain connectors	• N/A

Power Automate Cloud Flow Analytics

The Power Automate Cloud Flow Analytics tab provides insights into various Power Automate metrics at the environment level. These reports provide more in-depth data than the Overview Reports as they are filtered to a specific environment. The table below highlights some of the key metrics available.

Adoption	Usage	Health
• Total runs trendlines • Types of cloud flows used/created; instant, automated, etc. • Cloud flows in use trend • Cloud flows creation trend • Flow share trend	• Total runs • Flow share rates; including by type. • Connectors used; by flow runs, by connector calls, total	• Successful, failed, canceled runs • Errors by type • Errors by flow

Canvas Power App Analytics

The Power App Analytics tab provides insights into various Power App metrics at the environment level. Once again, these reports provide more in-depth data than the Overview Reports as they are filtered to a specific environment. The table below highlights some of the key metrics available.

Adoption	Usage	Health
• Location: Regional adoption metrics; app launches by location • Connectors used; standard v custom	• Usage: Total app launches • Usage: App launches by device and by app player version • Usage: Daily active users	• Toast error trends, types and counts per app. • Best and least performed services • Service performance: API service response times • Service performance: Success rates for each service • Service performance: Number of HTTP 500 error codes = server not responding • Service performance: Successful connection request • Ability to filter by service or connector

Dataverse Analytics

Dataverse Analytics reports serve as a powerful tool that offers an in-depth understanding of user activity and platform performance over time. These reports enable the identification of your most active users, their activities, and the most used entities, workflows, and plugins. They also assist in storage and performance management, enhancing your system's efficiency and reliability. Furthermore, they provide the ability to effectively troubleshoot by offering detailed insights into the most common errors within workflows and API calls, thus enabling quick issue diagnosis and resolution.

The table below highlights some of the key metrics available.

Adoption	Usage	Health
• Home: Most active users • Active users: by business unit	• Home: Active users • Home: Total plug-in executions • Home: Executions by type • Home: API calls • Active users: Most active entities used • Active users: Most used custom/oob entities • Active users: By device type, browser, security role	• Home: API pass rate • Home: 10 most failing plug-ins • System Jobs: System job pass rate, throughput • System Jobs: Failure by workflows • Plug-ins: Success rate, execution, execution time, active plug-ins, top failures. • API Calls: Total, most used, failures, success.

Capacity Analytics

The Capacity section of the admin portal allows you to monitor storage capacity use and availability in your tenant. Reports can be viewed across all environments, or you can drill down into individual environments for additional data. There are five categories of reports available to Power Platform Administrators: Summary, Dataverse, Microsoft Teams, Add-ons, and Trial.

Summary

This tab provides a tenant-level view of an organization's storage capacity and usage.

The **Storage capacity usage** report shows the total storage capacity and usage across the three storage types: Database, file, and log. Additional information on how these types are defined can be found here. This report allows an admin to quickly assess how an organization is tracking towards their storage capacity.

The **Storage capacity, by source** breaks down total storage capacity by source. The **Org (tenant) default** source shows the total storage capacity given at the time of sign-up; the User licenses source shows the additional storage capacity added for every user license purchased; the **Additional storage** source calculates any additional storage capacity that has been purchased.

Self-service license amounts and storage capacity can be viewed by selecting the link on the **Storage capacity, by source** report. The **Capacity from self-service user licenses** table shows how much additional capacity has been allocated for each license type and purchaser. For example, the table will show how much database and file capacity has been added for all the Power Apps per user plans purchased by a particular user.

The Top storage usage, by environment details storage usage by environment across the three storage types. Administrators can use this report to quickly identify which environments are consuming the most storage capacity.

The **Add-ons** report shows summary information on add-on capacity. The following add-on metrics will appear in this report if purchased by an organization:

- App passes
- Flow per business process
- AI Builder credits
- Power Pages anonymous capacity
- Power Pages authenticated capacity
- Power Pages page views (legacy)
- Power Pages logins (legacy)
- App Passes for Microsoft Teams
- Power Automate Unattended RPA
- Power Automate hosted RPA
- Power Automate Process

Dataverse

This tab provides much of the same data as the **Summary** tab in a table format grouped by environment. Each environment is listed with columns for the environment type, database usage, file usage and log usage. The details column provides a link to additional environment storage capacity details, the following details are provided:

- Actual database usage
- Top database tables and their growth over time
- Actual file usage
- Top files tables and their growth over time
- Actual log usage
- Top tables and their growth over time

Microsoft Teams tab

This tab provides a view of the capacity storage used by your Microsoft Teams environments. Teams' environment capacity usage doesn't count towards your organization's Dataverse usage.

Add-ons

This tab can be used to view your organization's add-on usage details by environment and to assign add-ons to environments.

Trial tab

This page provides a view of the capacity storage used by your trial environments. Trial environment capacity usage doesn't count towards your organization's Dataverse usage.

Exceeding storage entitlements

In addition to the capacity reports, tenant, Power Platform, and Dynamics 365 admins will receive notifications when approaching or.

The Power Platform admin portal enables ad hoc monitoring. Reports answer specific tenant questions, providing insights into adoption, usage, and health.

exceeding the organization's storage capacity. A warning notification will be issued when any of the three storage capacities (database, file, or log) have less than 15% of space available. An additional warning notification that admin operation could be impacted will be sent when there is less than 5% capacity remaining.

A final notification will be sent when the tenant's storage exceeds the capacity entitlement. The following operation will be restricted while the tenant is 'in overage' of their capacity entitlements:

- Create a new environment (requires minimum 1GB capacity available)
- Copy an environment.
- Restore an environment.
- Convert a trial environment to paid (requires minimum 1GB capacity available)

- Recover an environment (requires minimum 1GB capacity available)
- Add Dataverse database to an environment.

In some instances, 'overflow usage' may be permitted. This is where the tenant has exceeded their capacity entitlement in one storage capacity but has surplus capacity in another type that can be used.

Please review the examples here for further details.

Analyze Telemetry with Application Insights

As a powerful diagnostic and monitoring tool, Application Insights yields invaluable insights into the performance and functionality of components within Dataverse, Power Apps (model-driven and canvas), Power Automate, and Power Pages. It is most used to monitor Dataverse and model-driven app telemetry as it provides a peak 'under the hood' into the intricate operations occurring within these workloads.

As an integral component of the broader Azure Monitor ecosystem, Application Insights is a trusted aid for reliable enterprise monitoring and diagnostic operations. It offers evidence-based answers to pressing questions, such as the sources of user interface slowness, or the evaluation of API performance over a period assessed against the volume of requests being made.

Integration of Power Platform telemetry into Application Insights facilitates enhanced monitoring, tailored troubleshooting, and effective optimization of a Power Platform tenancy.

Below is an overview of some of the key features of Application Insights as it relates to Power Platform monitoring:

- Detailed dashboards to provide an over of the health of your organization.
- Smart Detection features for proactive monitoring.
- Alerts for important scenarios based on your organizational needs.
- Ability to use custom queries to interrogate the telemetry logs.
- Ability to visualize and track navigation patters from a user perspective to assess how a user moves through an app to determine whether the app layout or navigation can be improved.

Auditing and Traceability

Setting Up Tenant Auditing

Auditing is set at an organizational level by setting properties on the Organization table in Dataverse. When you are beginning your platform, you can enable auditing to capture the history of how and who changes your data. There are four primary settings when enabling Dataverse auditing which are:

- Enable Auditing – Set this value to true to enable the auditing feature of the platform
- Audit Retention Period – This is the number of days audit data is kept. This value is by default 30 days but can be increased for more history.
- User Access Audit – This enables if audit logging is turned on for all user access
- User Access Auditing Interval – How often user access data is updated

After setting the organization wide audit settings, you can additionally set audit settings on individual tables, rows, or columns within Dataverse. It is advisable to set auditing on mission critical tables and columns. Some fields might change quite frequently, and the history of those fields is inconsequential to the history of the application (for example, saving the preferred color scheme for a power app for a user). For fields that have no audit value, it is advised that makers disable auditing on these fields to ensure that unnecessary data is not collected. To learn more about setting up auditing for Dataverse:

https://learn.microsoft.com/en-us/power-apps/developer/data-platform/auditing/overview

Auditing and Security Monitoring with Sentinel

Integrating with Azure Sentinel offers a robust solution for enhancing security and compliance. Azure Sentinel, Microsoft's cloud-native SIEM (Security Information and Event Management) system, extends the auditing capabilities of the Power Platform by providing advanced analytics, rich visualization, and AI-driven insights.

When Power Platform activities are monitored through Sentinel, it allows for the aggregation, analysis, and correlation of data across the entire enterprise, not just limited to Power Platform interactions. This integration enables administrators to detect, investigate, and respond to internal and external threats in a more timely and effective manner.

Sentinel's powerful tools can track user activities, identify anomalous behavior, and trigger alerts for potential security incidents. This level of auditing is invaluable for organizations aiming to uphold stringent compliance standards and maintain a high level of operational integrity. By leveraging Sentinel's capabilities, businesses can ensure a higher degree of traceability and accountability within their Power Platform environment, making it a key component in a comprehensive governance strategy.

To learn more, visit:
https://powerapps.microsoft.com/en-us/blog/integrating-microsoft-sentinel-and-power-platform-to-better-monitor-and-protect-your-low-code-solutions/

Activity Logging and Auditing with Microsoft Purview

One aspect of monitoring that is important for administrators, particularly in highly regulated environments, is the ability to review and audit all actions and activities that have taken place on the platform. The Power Platform allows administrators this ability so that organizations can effectively monitor, investigate, and alert on any activity that takes place in the Power Platform.

Purview provides auditing solutions that enable organizations to investigate and respond to security and compliance events. Purview captures and records user and admin operations performed across Microsoft 365 and the Power Platform.

Examples of activities captured include app or flow creation, DLP policy modification, and connection creation. Admins can surface these records using a simple audit search interface. Search can be filtered by a variety of properties including the activities, users, dates, record types and workloads.

Purview currently covers the following workload and activities:

- Power Apps
- Power Automate
- Power Platform connector activity
- Data loss prevention activity
- Dataverse and model-driven apps
- Power BI

The following scenario demonstrates how Purview can be used to investigate security or compliance issues.

Scenario: A user account has been compromised by a malicious actor. The account is used to create a canvas Power App and Power Automate flow to collect and write data to external API. A custom connector is created to write the data to the external API and the environment DLP policy is updated to permit the use of the connector. An administrator can use the Purview audit logs to investigate the following activity logs to better understand the breach:

- Power Apps – Created app.
- Power Apps – Edited app permissions
- Power Automate – Created flow.
- Power Platform DLP – Updated DLP policy
- Power Platform Connector – API created
- Power Platform Connector – Connection created

Dataverse Audit Logging

Dataverse auditing logs capture changes that are made to records in environments with a Dataverse database. Audit logs help administrators and other privileged users to answer questions like:

- Who created or updated a record and when?
- Which fields in a record were updated?
- What was the previous field value before the update?
- Who was accessing the system and when?
- Who deleted a record?

Please note that Dataverse audit logs are stored in Dataverse and consume log storage capacity. As such, you should be pragmatic when setting log retention periods for your environments.

There are three levels at which auditing can be enabled: Environment, entity, and column. These levels work in a cascading fashion such that auditing must be enabled on an environment before it can be enabled on an entity and auditing must be enabled on an entity before it can be enabled at the column level.

By enabling auditing, admins are placed in a better position to investigate and respond to security and compliance issues within the Power Platform.

Dataverse for Teams

Dataverse for Teams environments are automatically provisioned when a user builds or adds an app, bot, or flow to a Microsoft Team. Oftentimes a user will be unaware of the downstream effects of adding an app, bot, or flow to a Team and as such may not have given any thought to the suitability of a creating Dataverse for Teams environment. As such, it is imperative that an organization has robust monitoring in governance in place for these environments to avoid environment sprawl.

In addition to the monitoring capabilities in the Power Platform Admin Center, administrators may wish to implement more reactive measures to govern Dataverse for Teams environment creation, such as those outlined below.

Managed Environment Lifecycle with Automatic Deletion

Administrators can use the out-of-the-box automatic deletion feature to enforce life-cycle management of Dataverse for Teams environments. This feature will automatically disable environments after 90 days of inactivity and delete the environment if left disabled for 30 days. While an environment is disabled, apps cannot be launched, flows are suspended, and chatbots can't be interacted with.

Upon deletion, only the Dataverse environment is deleted, other Microsoft Teams assets such as the underlying Team and SharePoint site are not affected.

The automatic deletion process does not run in silence, a series of warning emails are sent to the Microsoft Team Owners, the user who created the environment and the tenant

admin if the environment admins are no longer in the tenant.

Govern with the Centre of Excellence Starter Kit

A more proactive approach to Dataverse for Teams environment management can be implemented via the CoE Starter Kit. The CoE Starter Kit is constantly collecting data about your Power Platform tenant, including the creation of new environments. This allows you to enforce environment compliance at the time of creation. The Starter Kit contains a collection of Power Automate flows that run daily to complete the following tasks:

- Check for new Microsoft Teams environments.
- Contact owners of new environments asking for compliance details such as a business justification.
- Generate a welcome email with pertinent information about their environment and a link to your organizations' Power Platform policy documentation.

The CoE Starter Kit also provides a flow to delete inactive environments, but this flow is no longer required given the out-of-the-box automatic deletion feature.

As with all CoE Starter Kit tools, they are built using Power Platform components and can be configured to meet your organizations particular needs. For example, you may wish to change the email content or request additional compliance information from makers.

Implementing the CoE Starter Kit components to manage environment creation will help to deliver a well governed Dataverse for Teams instance.

More Visibility with Managed Environments

When managed environment is enabled, Power Platform administrators will gain access to the new Usage Insights feature. When enabled, this feature generates a Weekly Admin Digest, providing an overview of platform usage over the past month. The weekly digest contains the following:

- Active Power Apps.
- Active Power Automate flows.
- Active Power App users.
- Inactive resources.
- Top Power Apps as determined by the number of user sessions.
- Top Power automate flows as determined by the number of runs.

Power Platform Administrators can select which managed environments appear in the Weekly Admin Digest. Default recipients of the digest are Power Platform and Dynamics 365 Service Administrators, with the ability to

add additional recipients as required. Please note that the recipients of the Weekly Admin Digest will also receive emails relating to the Managed Environments Solution Checker.

There are certain prerequisites that must be met to gain access to these features. Tenant-level analytics must be enabled, and Premium Power App licensing is required for all users interacting with apps or flows inside a managed environment.

The data contained in the weekly digest enables efficient management of Power Platform resources by highlighting top performing users, apps and flows to be nurtured and promoted. Conversely, the digest helps to identify inactive resources that can be decommissioned. This allows for optimal usage and productivity, while minimizing the risk of underutilized resources.

Monitoring through the Power Platform Centre of Excellence

The Power Platform CoE Starter Kit is a collection of components designed to assist with Power Platform governance. The components of the kit are powered by the Power Platform tools you are familiar with such as Power Apps, Power Automate and Dataverse. This means that they can be easily extended and customized by low-code developers to meet your specific organizational needs.

Installation of the CoE Starter Kit is a great first step for organizations looking to improve their Power Platform governance and adoption. However, it's important to note that the kit doesn't represent a complete Centre of Excellence, as a true CoE should incorporate an organizations people, processes, and strategy in addition to technical tooling.

The CoE Starter Kit is made up of three modules: Core, governance, and nurture.

This section will focus on the first two modules.

Core Module

The components within the Core module are the foundation of the CoE Starter Kit. The module contains a series of "sync" flows that crawl your tenant resources and populate the data in Dataverse tables. The data collected includes things like Power App creation date, Power App last launch date, flow creation date and environment capacity. A full breakdown of the various Dataverse tables can be found here. The data captured here is used to populate the other apps, flows and dashboards contained in the CoE Starter Kit.

Another component of the Core module is the DLP Impact tool Power App replacement of the DLP Editor. This app validates DLP change impacts and the ability to create draft policies that then generate tasks for makers who have impacted Cloud Flows or Power Apps to take action to remediate. This app extends this functionality of Managed Environments by illustrating the impacts of proposed policy changes.

The module provides two separate Power Apps for setting app and flow permissions. These apps allow administrators to identify apps and flows that have become orphaned when their owner has left the organization. Once identified, the starter kit apps can be used to re-assign ownership.

Admin capacity alerts can be configured to automatically alert administrators when environments exceed their approved capacity or are at 80% of their approved capacity. The approver capacity level is configurable within the CoE Starter Kit.

One of the most powerful components of the CoE Starter Kit is the Power BI dashboard. This dashboard provides a holistic view of Dataverse data with visualizations and insights for Environment, PowerApps App, Flow, Connector, Connection Reference, Maker, and Audit Log tables. Unlike the analytics contained in the Power Platform Admin Center, these reports are not limited to data captured within the last 28 days. The table below sets out some but not all the metrics available in the Power BI dashboard.

In summary, the Core module allows administrators to gain an in-depth understanding of their Power Platform tenant and how their resources are being used.

Monitor	Govern	Nurture	Compliance and Adoption
Includes a host of data around the following workloads: Dataverse, apps, flows, SPO form apps, custom connectors, desktop flows, PVA, AI Builder, Power Pages, Business Process Flows and Solutions.	Environment capacity, app deep dive (shows plan classification, connectors, view widely shared and orphaned apps), flow deep dive (suspended flows that conflict with policy, orphaned flows, top used connectors). App and flow archive; apps and flows given scores based on indications of inactivity, admins can use this to archive them. Grant or remove app access from the embedded app in the dashboard or add yourself as owner to flows. Connector deep dive; use of connectors, by connector, by licensing tier by maker.	See maker information. The Nurture section helps you find your "star" app and flow makers and see what connectors they're using, where they're based (department/ city/country), and how they're adopting Power Platform. Year over Year adoption trend graphs. PA adoption; users + standard v premium users over time. Desktop flow usage.	Apps and flows without an owner Apps and flows not in solutions Apps and flows with duplicate names Apps launched this month and quarter Unique users in the past month Total makers Apps and flows without an owner Apps currently not compliant with policies or billing policies Grandfathered apps Apps shared with everyone and with more than 100 users

Governance modue

The Governance module takes the foundational knowledge gained from the Core module and begins to put robust governance processes in place. The module consists of the four key processes outlined below among a host of other features which are discussed in greater detail here.

In summary, the CoE Starter Kit, as the name suggests, provides an excellent starter kit for organizations looking to improve their governance capabilities. One thing to note is that as the native governance capabilities of the Admin Center continue to improve you may notice some overlap between the CoE Starter Kit tools and native admin center capabilities. Where the two overlap it is suggested that you utilize the native capabilities. These capabilities are robust and fully supported. The CoE Starter Kit should be used to enhance the out of the box capabilities.

Compliance process	Govern	Nurture	Compliance and Adoption
This process sends an automated email alerting administrators of non-compliant apps, flows, and bots. Non-compliance is based on criteria such as the number of people the app is shared with, whether a business justification has been given and the business impact of the app. The criteria for non-compliance can be customized to meet your organization's requirements. Power Apps are provided for makers to provide compliance information.	Provides an automated approval process to request deletion of inactive apps and flows. Automated deletion request will be sent to makers who own apps or flows that have been unmodified or unlaunched in the last 6 months (this duration is customizable). Subsequent flows then manage the deletion of the resource. This Cleanup Old Objects App covers the scenario where a maker has ignored the automated archive approval requests. The app provides a way for the manager of a maker to view pending archive requests and either reject the deletion or send a reminder to the maker to respond.	This component finds orphaned resources and attempts to associate them with the maker's manager. Admins are notified if a manager cannot be found. The Flow bot is used to contact managers and present them with the following options to clean the apps or flows: • Receive an email of the list of resources. • Take ownership of all resources • Delete all resources. • Assign the resources to someone else. • View each resource individually and decide on each.	This process provides mechanisms for quarantining non-compliant Power Apps. Once quarantined an app can no longer be launched. Apps can be quarantined automatically by Power Automate flows based on specified criteria or manually by an administrator.

Monitor and Manage with PowerShell, Power Automate and Power Apps

One of the unique things about administering the Power Platform is you can use the same components to automate administration tasks and to alert the admin team when action is needed. Using the PowerShell cmdlets or the management connectors you can build flows and apps that help you do implement your governance policies.

Automation of tasks with PowerShell

The PowerShell cmdlets allow you to do similar tasks that you would do with the admin portals but do them in scripting where you can sequentially execute multiple commands or pipe output from one to automate common tasks. There are multiple PowerShell cmdlets that you can work with. The following is an overview of each that you would likely interact with.

It is not uncommon to build PowerShell scripts to do bulk operations on users, environments or their resources that use a combination of all the below cmdlets.

PowerShell cmdlet library	Common Tasks
Power Apps cmdlets https://docs.microsoft.com/powerapps/administrator/PowerApps-powershell	Designed for app makers and administrators to automate tasks with environments and associated apps, flows and connectors. Note: These cmdlets are currently in preview.
Microsoft 365 (formerly Office 365) 365 cmdlets https://docs.microsoft.com/office365/enterprise/powershell/getting-started-with-office-365-powershell	These are focused on Microsoft 365 (formerly Office 365) related tasks and can be used to automate user-related actions and tasks, for example, assignment of licenses.
Dynamics 365 cmdlets https://docs.microsoft.com/powershell/dynamics365/customer-engagement/overview	These are useful if you have any environments with CDS databases. Modules include support for using the CDS online admin API, as well as to automate solution
Microsoft Azure cmdlets https://docs.microsoft.com/powershell/azure/overview	The Azure cmdlets are useful if you are including any Azure components in your overall solution. This could also be used to script setup of the on-premises application gateway.

Automation of tasks with Power Automate

One of the unique things about Power Automate is you can use it to manage itself along with other parts of the Power Platform.

The following connectors can be helpful to automate administrator tasks with Power Automate.

Connector	Possible uses
Power Automate management connector https://docs.microsoft.com/connectors/flowmanagement/	Can be used to automate working with workflows including getting lists of new workflows or connectors in your environments.
Power Automate for Admins https://docs.microsoft.com/connectors/microsoftflowforadmins/	Allows you to perform typical admin actions, such as disabling a flow or deleting a flow.
Power Apps for Admins connector https://docs.microsoft.com/connectors/powerappsforadmins/	To set permissions on Power Apps or set permissions to a certain connector being used by this app.
Power Apps for App Makers connector https://docs.microsoft.com/connectors/powerappsforappmakers/	Can be used by the makers themselves, though some actions being an overlay to administration tasks, such as settings permissions to a Power Apps app – therefore administrators might be using this connector as well.
Power Platform for Admins connector https://docs.microsoft.com/connectors/powerplatformforadmins	One of the unique things about Power Automate is you can use it to manage itself along with other parts of the Power Platform. The following connectors can be helpful to automate administrator tasks with Power Automate.
Microsoft 365 Users connector https://docs.microsoft.com/connectors/office365users/	Useful for automating actions around users. For example, you could use the connector to get the manager of a user that owns an environment to be able to send them an email for approval.
Microsoft Forms https://docs.microsoft.com/connectors/microsoftforms/	Forms is an easy way to collect information to start an admin task. This can be combined with the approval connector to get manager approval.
Azure AD connector https://docs.microsoft.com/connectors/azuread/	Useful to perform tasks such as adding a user to a group or even creating the group.

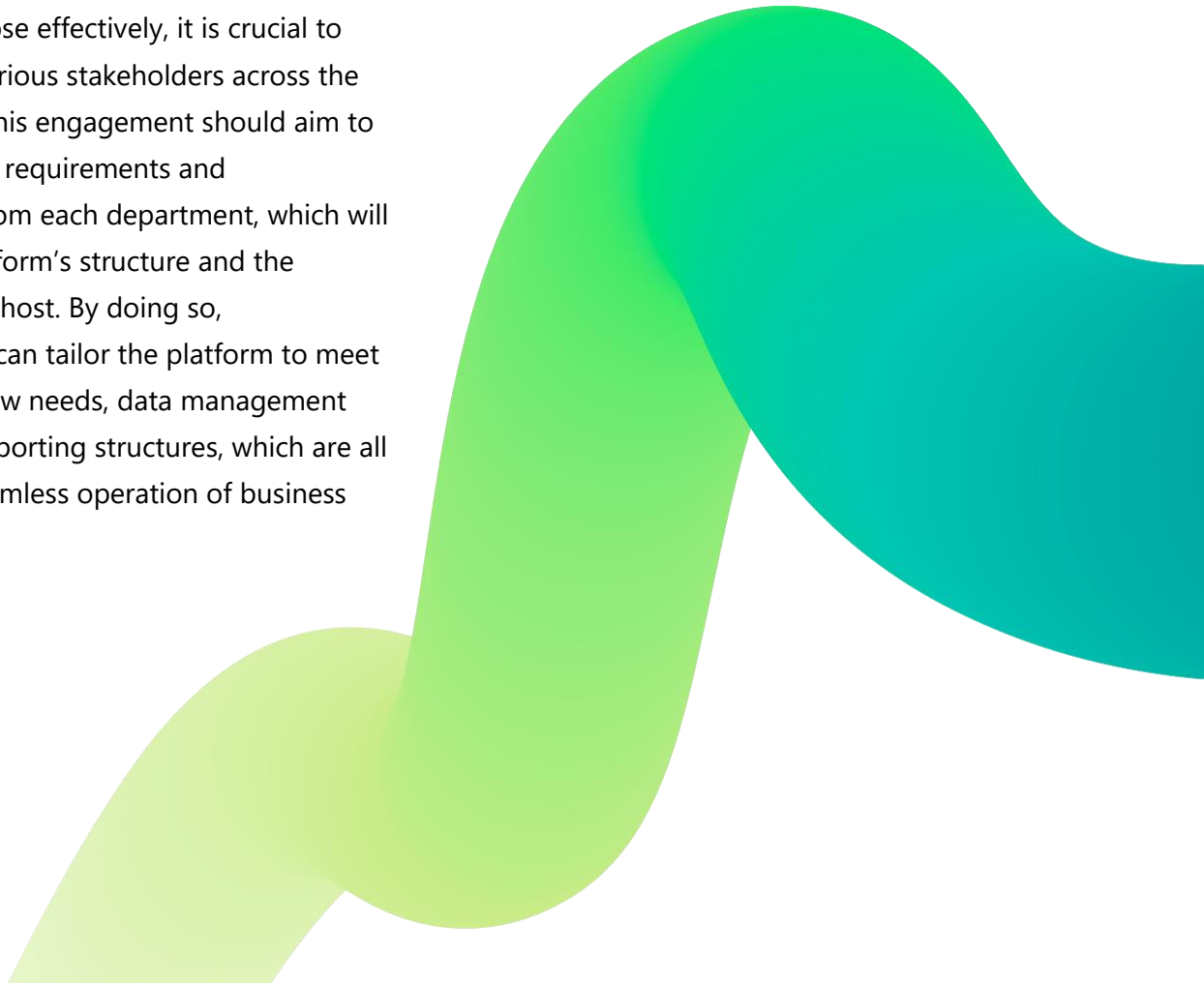
Setup Application Lifecycle Management

Building your Power Platform efficiently requires a bottom-up approach where considerations should be made early as to what departments, business needs and tools will be held within your platform.

Having a thorough understanding of the business needs will help determine the ALM strategy and associated environment setup. This section highlights how to design these as well as some best practices for each.

To ensure that the Power Platform serves its intended purpose effectively, it is crucial to engage with various stakeholders across the organization. This engagement should aim to gather detailed requirements and expectations from each department, which will inform the platform's structure and the solutions it will host. By doing so, administrators can tailor the platform to meet specific workflow needs, data management policies, and reporting structures, which are all vital for the seamless operation of business processes. This stakeholder-centric approach not only guarantees that the platform is aligned with current business needs but also anticipates future demands, thereby future-proofing investments into the platform.

Once the business and development needs are clearly defined, the next step is to establish a robust governance framework. This framework should outline the processes for data handling, user access, and security, ensuring that they adhere to both internal standards and external regulatory requirements.



It is also within this governance structure that administrators should define the ALM processes. ALM is critical for the systematic planning, development, deployment, and maintenance of applications. By integrating ALM best practices into the governance framework, organizations can facilitate continuous improvement and innovation within their Power Platform environment, while maintaining control and compliance. This dual focus on governance and ALM ensures that the platform remains both dynamic and secure, capable of adapting to new challenges while safeguarding critical business operations.

For mission-critical or sensitive solutions, it is advisable to utilize dedicated pipelines, including development, testing, and production environments. Managed environments ensure consistent governance and security, and ALM pipelines can be employed to move solutions across these environments seamlessly with the required change control and approvals. It's crucial to define user roles and access levels within each environment, restricting certain actions based on organizational policies.

Shared dedicated environments and associated pipelines can be leveraged for alternative business scenarios, granting developers the ability to release applications into shared testing environments. Administrators can then release approved solutions from testing to a shared production environment, while still ensuring change management and controls are followed. This structured ALM approach allows makers to develop and test solutions in personal environments before promoting them to shared testing and production environments after necessary reviews and approvals.

By leveraging the ALM Accelerator, managed environments and pipelines features you can tightly govern which makers can release solutions to different environments, ensure source control is enforced, approvals at each release step and delegated deployments and release a sensible and agile deployment strategy that fits your organization's needs.

Solutions

To organize, package and deploy cohesive applications or workflows within the Power Platform, Solutions are key. Solutions serve as 'containers' for all the components that constitute a full Power Platform solution. Whether it's building complex apps, automating business processes, or creating data-driven visualizations, solutions help streamline the development life cycle by allowing developers, administrators, and solution architects to package, version, and migrate their work from development to testing to production environments while maintaining consistency and governance.

Solutions are instrumental in not only encapsulating the components – such as apps, workflows, connectors, and data models – but also in managing dependencies and

relationships between these components. This encapsulation is essential for maintaining the integrity of Power Platform solutions as they are promoted through different environments. By leveraging Solutions, organizations can ensure that all changes are version-controlled, and that any deployment can be rolled back, if necessary, thereby minimizing disruption to users. Furthermore, Solutions enable a modular approach to development; components can be reused across different applications, which accelerates development timelines and fosters a culture of efficiency and reuse within the organization's development practices. This modularity, combined with the governance afforded by Solutions, ensures that the Power Platform remains both a flexible and controlled environment, perfectly balancing the needs for innovation and stability.

Preferred Solution

By default, Power Platform components are stored in a solution named Common Data Services Default Solution, this is not a best practice model as there is no separation of maker components. Setting a preferred solution for a maker promotes healthy ALM practices by design. Administrators can ensure that any new canvas apps and cloud flows not created in a Solution are added by default solutions.

Administrators enable this functionality as an environment setting by turning on Preferred solution and Create new canvas apps and cloud flows in Dataverse solutions setting in the Power Platform Admin Centre.

Makers set their preferred solution in the maker portal Solutions tab. Setting a preferred solution and Create new canvas app and cloud flows in a Dataverse solutions is currently in preview.

Learn more about Set a preferred solution - Power Apps | Microsoft Learn

Structuring your Solution

Depending on the solution requirements, a solution contains a set structure of objects for the given business purpose. Solutions can contain all the following object types:

- Model-driven Power Apps
- Canvas Power Apps
- Power Automate flows
- Custom connectors
- Dataverse tables
- Dataverse option sets

It is common to structure your solutions with particular business opportunities or departments in mind. An example structure for a Human Resources solution could include:

Object Type	Use Case
Power Apps	• [HR Tools] Employee Onboarding • [HR Tools] Employee Training Register
Power Automate Cloud Flows	• [HR Tools] Employee Onboarding – Approval • [HR Tools] Employee Onboarding – Notifications • [APP Tools] Obtain Extra Active Directory Attributes • [HR Tools] Employee Training - Notifications
Connection references	• Cr_HR SharePoint Site • Cr_Office365Users
Environment Variables	• Env_var_HR-SharePoint-Site • Env_var_HR-SharePoint-List • Env_var_HR-GroupEmail

Environment variables can be excellent ways to store per-environment values at the solution level, that require updating when the solution is imported into a target environment such as UAT, or Production. Using Pipelines can add simplicity to this process whereby the Pipelines interface can prompt the deployment team to switch out any connection references and include the appropriate value for each environment variable for the given environment.

Unmanaged and Managed

There are typically 2 types of solutions in Power Platform:

- Unmanaged Solutions: These are used in your development environments while makers are creating and updating applications and flows within the solution. Unmanaged solutions should be used under source control.
- Managed Solutions: Managed solutions are used when deploying to any environment which isn't deemed as development. Unmanaged solutions should be converted to managed solutions during deployment as build artifacts. Managed solutions cannot be imported into an environment that also contains the originating unmanaged solution.

Creating Solutions

Creating solutions is very simple and takes only a few moments. You will need to consider the following properties:

- Display name: this is the name with which you will refer to your solution.
- Name: This is the internal name that Power Platform will reference in relation to the Display name.
- Publisher: The solution publisher is in the indication of who published the components within the solution. Publishers should be meaningful names along with a meaningful prefix. Publisher prefixes are concatenated with solution names to indicate the publisher for that solution. Without a unique publisher, the solution will opt to use the default publisher with the cr8a3 prefix.
- Version: This is the starting version point of your solution. Typically, these will be 1.0.0.0 – but you can start this from any point system.
- Configuration page: This allows you to set a known configuration page which can be used to display information about the solution as well as letting the user configure the app or flow after it has been deployed to another environment.
- Descriptions: The solution should be kept general, but should describe each component of a solution such as

Apps, Flows and environment variables or connectors.

- Package Type: This allows you to choose between unmanaged and managed package type for your solution.

Source Control

Source control refers to a system that maintains and stores development assets while tracking changes to those assets. A source control system provides a 'single source of truth' and gives developers the ability to roll back changes applied to development assets during the development lifecycle.

Setting Up Managed Environments

Setting up managed environments is essential for proficiently managing and overseeing the development and deployment lifecycle of Power Platform solutions. To initiate this process, administrators should access the Power Platform Admin Center and create distinct environments, each earmarked for specific. Stages of deployment, such as development, testing, and production. Environment creation should be aligned to your organizations Environment Strategy.

Environment	Environment Type and Use
Consoto DEV	Sandbox – Unmanaged- allows for multiple makers with components being immediately iterated on due to lack of version control. Solutions can be either managed or unmanaged.
Contoso SIT	Production – Managed – allows for system integration testing with a dedicated testing team. Solutions should be imported as managed.
Contoso UAT	Production – Managed – allows for further restrictions for user testing. Solutions should be imported as managed.
Contoso PROD	Production – Managed – full production environment with greatest security and DLP policies enabled. Solutions should be managed.

Environments can be created and managed from within the Power Platform Admin Center by an administrator. To use Pipelines for ALM, managed environments are required for all environments a solution will be released into. The development environment where the solution is initially created can remain unmanaged, but by using features – and during the import process in Pipelines, the subsequent environments should be managed, and solutions targeted to become managed alongside this.

A Base example configuration could be as in the table example above.

Managed environments ensure consistent security controls, governance facilitated through the process ensuring solution version control, understanding regarding the components contained within managed solutions. Administrators can associate environments with dedicated Dataverse databases for data management.

Deploying Applications with Pipelines

Power Platform Pipelines is an excellent tool for both makers, developers and admins looking to incorporate automation into ALM. Pipelines is a Managed Environment premium capability. Pipelines are very simple to setup and configure and each different set of users have a tailored experience:

- Admins can configure pipelines quickly.
- Makers can use the simplified pipelines UI to deploy solutions in only a few steps using the pre-configured pipelines.
- Developers can extend pipelines and run a pipeline using the CLI.

Setting up Power Pipelines

To setup Pipelines, there are a few pre-requisites which must be considered:

- Any environment in the pipeline must have a Dataverse database.
- Target environments (not including the initial development environment) must be enabled as managed environments.
- A host environment for pipelines which will host configurations, security and pipeline run history.

Once the Pipelines application has been installed in the host environment, pipelines can be created using the newly created Deployment Pipeline configuration app. Enter in a record for each environment you wish to be used in pipelines. Once this is record is created and verified within the app, you can then assign target environments for each new deployment stage [Set up pipelines in Power Platform - Power Platform | Microsoft Learn]

Using Power Pipelines Effectively

Using Pipelines effectively means ensuring your configuration is set with as much detail as possible. From the record of your environment to the descriptions in your deployment stage.

Pipelines offers the opportunity to ensure developers and makers are using data source variables and connection references as the UI will prompt users during the deployment stages to enter appropriate values for each.

An example of these prompts is if in your development environment you opt to connect to a development SharePoint site in one of your canvas apps – during deployment you will be prompted to enter a new value (or SharePoint list URL) provided your data source was setup as an environment variable. This applies to any variables that you have set within that environment. You will also need to consider potential layering – if you add values to your environment variables in your development environment, these will need to be removed to avoid layering. You will need to enter new values to each variable during the pipeline deployment.

Administering Pipelines Environments and Permissions

Pipelines allow fine grained control over which users can release solutions to which environments. When your organization is just getting started with Pipelines you will want to enable Developer environments to be able to release solutions into a shared testing environment.

This means that when a maker comes into the platform, your developer and the environment will need to be added to the pipeline configuration to release the code into the shared environment. While the developer can belong to a group that has permissions by default, the environment will not be added by default. As a result, you will need to design a process that adds the developer's environment to the list of environments the pipeline can release solutions from.

Adding environments to the pipeline's app will require an administrator to add either a target or source environment to the pipelines app. Organizations should create a dedicated environment for the pipeline app and assign a group of pipeline administrators to manage the environments, permissions, and pipelines that can be used by the organization.

As new developer environments come on board your team can decide to give permission as a source location for solutions to be released into shared target environments from. Once an environment is added, it must then be added to a pipeline.

Two security roles are created with pipelines which are the Deployment Pipeline User and the Deployment Pipeline Administrator. You will need to give your makers the role of deployment pipeline user, either directly or by group, if they are to be able to use the pipelines you deploy. Keep in mind that by granting this role, the user can use the pipeline, but they must also have roles that allow them to package the solution from the source environment, as well as deploy into the target environments.

The Deployment Pipeline Administrator is responsible for creating and modifying pipelines, adding and removing environments to the pipelines, as well as managing who has access to which pipelines. You should adopt a core pipeline management group that maintains the pipelines functionality.

Building a Pipeline Strategy

As you build your environment strategy, it's also important to build a pipeline strategy catered for all makers, professional developers and low-code developers. There are a few common types of pipelines organizations can build to minimize the management overhead of pipelines as well as enabling rapid iteration for your makers.

- Solution Specific Pipeline: organizations that build critical solutions in dedicated environments will typically build a specific pipeline to manage the release of that solution into the different environments. In this scenario, the environment that the solution is developed in is added as the development environment, and then the testing, staging, and production environments are added as the target. It is advised that administrators create pre-deployment authorization flows to the upstream environments to ensure that environment deployments are properly controlled and authorized.

- Generic Release Pipelines: organizations can also build generic pipelines that allow makers to release into shared environments. These pipelines are setup to allow solutions built in developers environments to release to shared test and production environments. Organizations will typically make use of pre-deployment steps to allow administrators of Production environments the ability to

approve the release of solutions into the shared environments. Alternatively, separate pipelines can be built that only administrators can use to release solutions from testing environments to production.

Extending Pipelines

Pipelines offer administrators customizable solutions tailored to an organization's specific requirements. This customization includes features like adding approvals, deploying via service principals, and integrating with various systems such as Azure DevOps and GitHub. Leveraging Microsoft Dataverse business events allows for the execution of business logic within Power Automate or other subscribers. Despite the potential complexity internally, the deployment experience for makers remains straightforward. Deployments progress through predefined steps, with gated extensions allowing the insertion of custom steps for executing business logic. This flexibility gives administrators control over the deployment process.

Delegated Pipeline Deployments

Delegated deployments can be executed either as a service principal or the owner of the pipeline stage. Implementing control over resources at different stages is essential for maintaining governance throughout the deployment process. Once activated, the pipeline stage carries out the deployment on behalf of the delegate (either the service principal or the owner of the pipeline stage) rather than the maker who made the request. It's important to note that this feature is currently in preview.

Learn more about Deploy pipelines as a service principal or pipeline owner - Power Platform | Microsoft Learn

Using the ALM Accelerator

The ALM Accelerator for Power Platform is a user-friendly canvas application designed to simplify the management of application life-cycles. It integrates seamlessly with Azure Pipelines and Git source control, offering a straightforward approach to ALM. This tool follows ALM pro-development code-first best practices, harnessing the inherent capabilities of the Power Platform to facilitate your ALM journey. Its development combines low-code canvas apps tailored for both makers and administrators with Azure Pipelines YAML and PowerShell templates.

With the ALM Accelerator for Power Platform app, creators can effortlessly manage source control by committing your solution code into a source repository, packaging it to an artifact for delivery, and delivering it to other environments, establishing version history, and deploy their solutions within the Power Platform. To make the most of this accelerator, it's essential to organize all your Power Platform elements – such as apps, flows, customizations, etc. – within a solution.

There are two target groups with which ALM Accelerator should be used by:

- Makers who're unfamiliar with core ALM concepts. These makers do, however, wish to save their work while maintaining the history of any changes.
- Makers who are comfortable with using systems such as Git with concepts such as pull requests, branching and merging and wish to use that method for source control or deployment configurations.

A system administrator familiar with Dataverse and Azure Active Directory can install the ALM Accelerator and should consider the license requirements for the following connectors:

- Dataverse
- Custom Connectors
- HTTP with Azure Active Directory connector
- Power Apps Per User (or Per App) license for users
- Azure DevOps Basic plan

Leveraging AI with your Platform

The Power Platform has worked extensively to integrate artificial intelligence at the heart of the maker experience. Leveraging Power Platform Copilots, makers are able to quickly and easily create apps, flows, agents, and Dataverse tables with simple prompting. The Copilot experience brings the power of Large Language Models and Generative AI to the platform, greatly accelerating the development workflow of most components on the platform.

What is AI Builder?

Power Platform AI Builder is a built-in tool for infusing AI into apps made with Power Apps and Power Automate. It provides customizable AI components like vision and language models that users can add through a no-code interface.

Key use cases are automating document processing, extracting information from forms and invoices, sentiment analysis on customer feedback, object detection in images, and speech recognition and synthesis. Users can leverage pre-built AI models or train custom models specific to their data.

Outcomes include faster app development cycles by reducing the need for data science expertise. AI Builder democratizes AI access so any maker can enhance their solutions with intelligence. It increases productivity through automated document digitization, speech transcription, and other manual tasks.

The low-code aspect allows non-expert users to experiment rapidly with AI. They get recommended AI model templates for common use cases. Power Platform manages cloud hosting, scaling, and model management, simplifying AI benefits by abstracting complexity.

	System Admins System Customizer	Environment Maker	Dataverse User	<None>
View AI Builder page	✓	✓	✓	✗
Create a model	✓	✓	✗	✗
View and use a created model	✓	Owned or shared model	Owned or shared model	✗
Create a flow to call a model	✓	✓	✗	✗
Create an app to call a model	✓	✓	✗	✗
Run a flow using a model	✓	Owned or shared flow using an owned or shared model	Owned or shared flow using an owned or shared model	✗
Run an app using a model	✓	Owned or shared app using an owned or shared model	Owned or shared app using an owned or shared model	✗

AI Builder Governance

Broadly speaking, AI Builder has governance controls using roles access. There are three major components to AI Builder solutions, which are the source data, the model, and the predictions. Makers will typically need access to the source data as well as AI Builder to train the model. Additionally, any other tools that leverage the model such as Power Apps and Power Automate Flows will need access to the model.

AI Models undergo various stages in their life cycle which aligns to some of the roles displayed above. A model is first created in a draft state where it undergoes an iterative process known as training. Here the model is learning the source data in order to make predictions. Once training is completed a

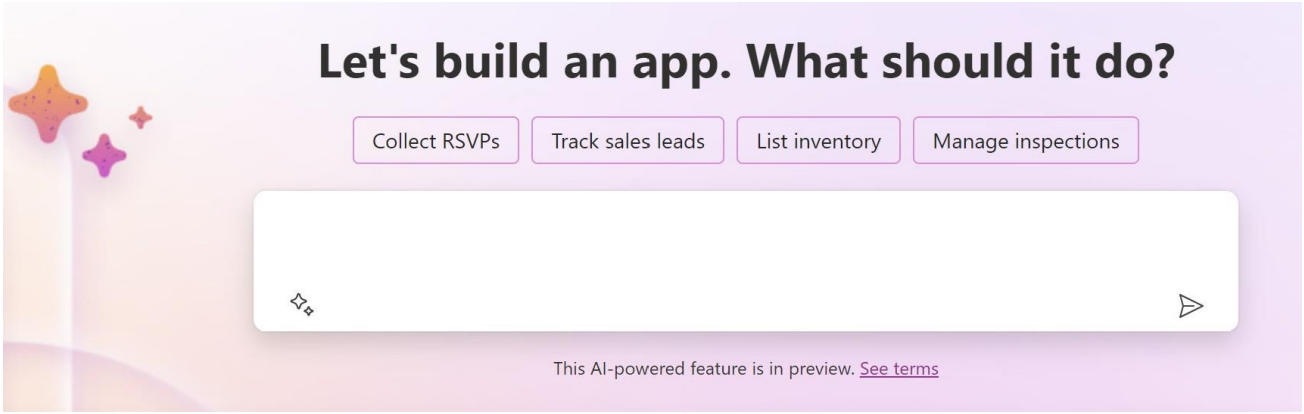
model is trained, but still cannot be used for real time inferencing and prediction.

Once the model is trained, accuracy will be scored, and a breakdown will be provided. Models can then be further trained to increase the accuracy score. From there the model must be published, at which point apps and flows can make real time predictions using the model. Those with the maker and administrator roles can create and train the model, but only users who have had an app or flow that uses the model shared with them, can actually operate the model.

AI Builder models are released once they are trained into other environments through solution packages, like other components of the Power Platform. AI Builder models can be released to Test and Production managed environments through the use of the Pipelines feature described above.

The final component of managing AI Builder is the allocation of credits to an environment. Each use case consumes differing amounts of credits, so it is important component of AI Builder credit planning to get an understanding on what type of model is being used, and the quantity of inferences done in each environment. Administrators will then allocate credits to those environments based on those estimations.

Your prompt data never leaves the Microsoft Cloud and is not shared with OpenAI.



What is Copilot?

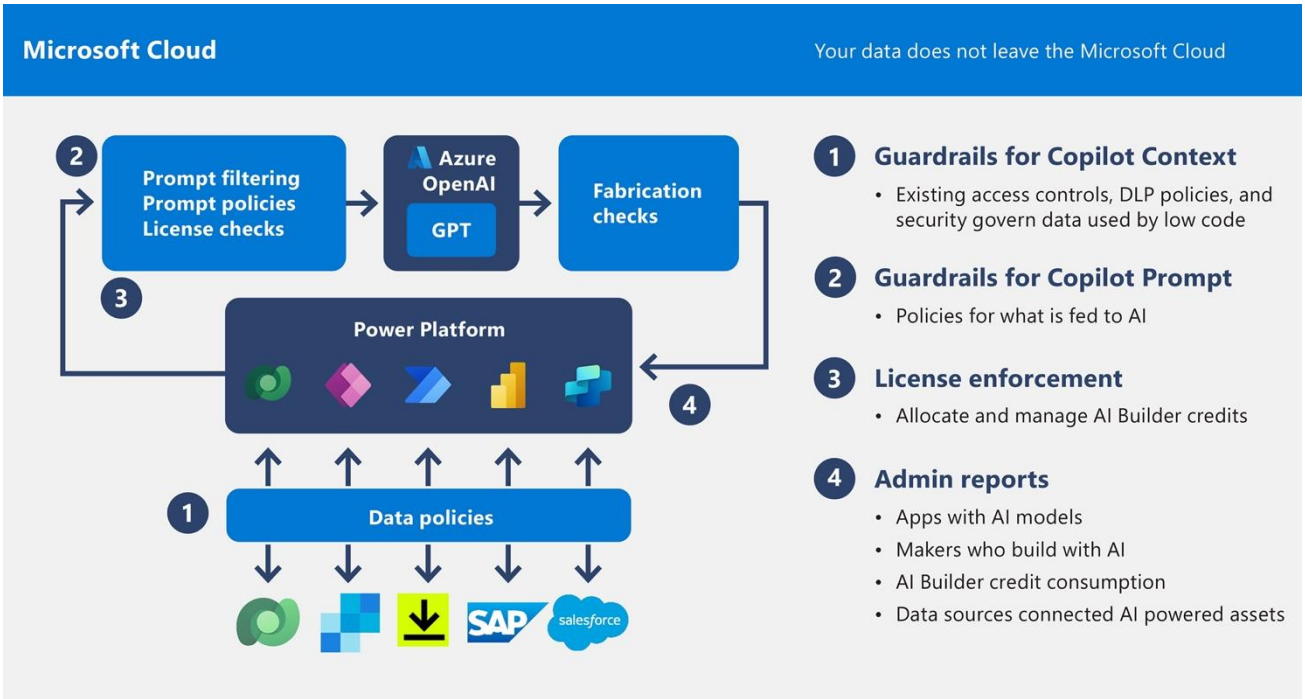
At a high level, makers interact with Copilot using a "prompt" where the maker describes what they are attempting to accomplish. For example, you might be trying to build an app that manages inventory, and you would simply prompt the solution "I would like to build an app that tracks inventory".

Copilot will then take you through the process of creating the Dataverse tables necessary, the Power App interface, and any flows required. It is important to note that using Copilot is not a fully complete process and serves to help makers "get started" with their development. While many of the Copilot generated solutions are sufficient, they often will require specific tweaks and customizations out-of-the-box.

There are capacity limits on the use of the solution as well that Microsoft might enforce if capacity is limited. Your makers can use Copilot to create Dataverse tables as well, simply describe what you want to store or do with a table and Copilot will generate the table for you.

Copilot is also available for Power Automate. Simply describe what you want your flow to do, and Copilot will generate the flow for you.

Additionally, Copilot features can be leveraged in Power Virtual Agents to build out the topic flows. You simply tell Copilot what the topic should do, and Copilot will generate the topic flow for you. With Virtual Agents, you can leverage Azure OpenAI Service to help the agent generate questions either based on a web page, a set of documents, or a customized OpenAI service. With Copilot + Azure OpenAI integration you can build robust intelligent agents.



What are the Governance Features of Copilot?

As Copilot rolls out, Microsoft has introduced a variety of governance features around the use of Copilot so that organizations can see how Copilot is being used and what apps are built using Copilot. These types of insights can help administrators identify apps that might need additional reviews for completeness, but also allow an organization to understand how the use of Copilot is taking place, so that you can dedicate more time to educating team members on how to leverage Copilot to greatly accelerate and improve their maker experience.

There are multiple areas where governance features are in place for Copilot. First and foremost is that Copilot can only create within your environment and the guard rails and policies that exist within that environment. That means that Copilot uses your existing policies, access controls, and security setup and cannot build solutions that violate them. Copilot understands what policies are in place and the solutions created are governed by those policies. Copilot cannot override them.

The second aspect of Copilot governance refers to the prompts generated by your makers when instructing Copilot to construct functionalities. These prompts use Azure OpenAI in the background and are automatically checked in multiple ways by Microsoft to ensure that Copilot is not used to perform or create anything that is against policy. Those checks include filtering out prompts that ask for improper or illegal output, prompts that violate policy, or prompts that violate licensing restrictions. Finally, the response from Azure OpenAI is

checked for fabrication to ensure that the output is valid and true.

All AI responses are governed by guiding principles which are fairness, reliability and safety, privacy and security, inclusiveness, transparency, and accountability. Responses that do not meet these guiding principles are filtered. Finally, Copilot is rigorously tested. Microsoft makes use of structured red teaming, where the organization intentionally attempts to get Copilot to function in an ungoverned way. By using structured and dedicated red-teaming and adversarial testing, Microsoft ensures that Copilot is safe for use.

How can I control the use of Copilot?

Copilot settings are enabled at the environment and tenant level. You can enable Copilot at a tenant level, and for environments where you feel it is useful. It is likely that you want to enable Copilot for your development environments, and you can build a policy to this effect. You can access the tenant level settings via the Power Platform Admin Center as an administrator and disable Copilot.

How is my Data Kept Safe with Copilot?

Prompt data leverages the Azure OpenAI service and is never used outside of your tenant. Your prompt data never leaves the Microsoft Cloud and is not shared with OpenAI. Only certain authorized Microsoft employees may review your data to investigate instances of potential abuse that is detected by automated systems. Your data is not used to train machine learning models of any sort.

It is also important to note that Copilot generate applications, flow and agents adhere the governance and rules of the environment, tenant, and connectors they use. Copilot has the same access that the maker using it has, so if a connector is unavailable to the maker, it is unavailable to Copilot. The permissions of Dataverse are respected regardless if the solution was made by Copilot or not.

Enabling and Supporting your Organization

A key component of your Power Platform governance is enabling and supporting your people in their journey to master its tools. To best enable your organization, it is recommended to have a healthy blend of organizational alignment, structured training and onboarding, and sustained evangelism of how the Power Platform is helping your people succeed with its use.

It is key that you have the organizational structures in place to ensure that the Power Platform is well maintained, supported, and governed.

Evangelism	Community development	Training and Support
Run internal App / Flow in a day workshop	Create an internal community on Yammer or Teams for your champions	Hold drop-in sessions in regular office hours for your makers to ask questions
Organize hackathons with real business scenarios	Use a Teams or SharePoint site to store resources, like your own best practices or brand guides	Provide internal learning resources and tracks for beginner, intermediate and advanced makers
Share success stories	Update your makers about new features in the platform with a monthly newsletter	
Hold Show and Tell sessions to learn what other makers are creating	Offer individual recognition and career paths	

Structuring your organization for the Power Platform

Depending on the size of your organization, it is key that you have the organizational structures in place to ensure that the Power Platform is well maintained, supported, and governed. As an initial start, the platform should be owned by a core group of administrators or team. As your use of the platform grows into the hundreds of flows, apps, and agents, you will want to allocate a dedicated team to handle the day-to-day monitoring, governance, and support.

When your organization's use is just beginning – and you are less than 100 flows or apps – it is recommended that you appoint at least three team members to be the custodians and administrators.

Whether you have a dedicated team or a small group managing platform governance and ownership, it is essential to structure your organization effectively for overseeing platform feature usage. This requires a core governance structure – either by an empowered individual like a CTO or CIO, or a steering committee – a team must evaluate when new features are introduced to the platform, and when they are enabled for your organization. Often, the administrative group will meet with a larger steering committee to discuss and authorize the introduction of new preview features such as Copilot.

Your core administrative team will need to be able to action requests for the platform including:

- New environments
- New users and license allocations
- New pipelines
- Changes in policy
- Enabling connectors

You can offload some of this activity by introducing team environments that are largely governed by administrators in that team. By creating a best practice overarching policy, team environment leads can largely manage the day-to-day operation of their use of the platform.

Build Power Platform Onboarding and Training

Training and framing your people's use of the Power Platform is essential for continued success with the platform. As an initial effort on building an effective onboarding experience, investigate the roles of the typical users of the Power Platform. Most organizations will have some mixture of business users, makers, and administrators. You might consider different training content for professional developers from low-code developers as well. Once you can translate your onboarding and training experience into a digital experience, you can leverage managed environments welcome links to welcome new users to their new environment and the platform.

A role-based curriculum is important – builders need technical training on Power Apps and Power Automate, while business users need end-user training on using solutions. Separate programs for governance roles like administrators allow customization for their needs.

Training delivery should leverage different modes – hands-on labs, live workshops, online courses, documentation, and office hours. This caters to different learning styles, while gamification through points and certifications encourages learning. Additionally, your organization can take advantage of a multitude of content available on Microsoft Learn.

Metrics such as usage, help tickets, and user feedback pinpoint areas of improvement. Training should evolve based on these metrics, aiming for business users to independently create secure, scalable solutions, reducing reliance on central IT.

Successful training is key to change management when rolling out low-code solutions across large enterprises.

Power Platform in a Day Workshop

Engaging your team in training and onboarding workshops is effectively achieved through the Power Platform in a Day series of workshops. These workshops are offered

virtually through various partners in different languages and time zones across the world. There are four different workshops offered for different aspects of using the Power Platform.

The App in a Day workshop helps your people understand how to build Power Apps that make work processes become more paperless. In this session, team members will learn how to right custom business applications leveraging Dataverse, Power Apps, and Power Automate. They will learn how to properly use connectors and share apps within the organization.

The Automation in a Day workshop is specially geared towards creating Power Automate flows for both cloud flows and Power Automate desktop flows. This training, targeted at the beginner level, will help team members automate and orchestrate their business process. Additionally, this module will go over form processing features of AI Builder.

Finally, the Copilot in a Day workshop will help your team members to design and build intelligent conversational chatbots. This module will help your team understand how to create chatbots, take action and integrate with connectors, and build rich personalized conversations.

You can learn more about the Power Platform in a Day workshops here: https://powerplatform.microsoft.com/en-us/training-workshops/

Leverage the Power Platform Community

One of the best resources are the Power Apps and Power Automate community sites:

Power Apps community resources:

- https://powerusers.microsoft.com/t5/Power-Apps-Community/ct-p/PowerApps1

Power Automate community resources:

- https://powerusers.microsoft.com/t5/tag/Power%20Automate/tg-p/category-id/PowerApps1

These are forums where you can post your question and both the community and Microsoft can respond. Often your issue or question has already been discussed and you can simply look at the prior answers.

The Power Apps and Power Automate teams blog frequently on both new updates as well as ongoing examples of using the features of the products. The Power Automate blog for example has an ongoing series of beginner workflows and intermediate workflows. These are great ways to get ideas even if you don't need that exact solution, it can give your ideas on how to handle similar scenarios. The Power Apps blog has a category for: Admin Features

The blog post on Power Apps Learning Resources: https://aka.ms/ PowerApps resources, is updated frequently, and contains links to learning resources as well as real world customer stories.

Microsoft Learn offers short courses that can be consumed by both makers and administrators. The Power Apps courses can be found here: https://aka.ms/powerup

Administrators will likely find the managing application courses a good fit. For Power Automate you can find the courses here: https://docs.microsoft.com/flow/guided-learning/

There are also a couple courses on administering workflows would be good for administrators.

Leverage Power Platform Partners

If you find that you or your teams are looking for some outside assistance, you can use the Partner Finder to locate a partner that specializes in Power Apps and Power Automate. You can find the list of partners here: https://PowerApps.microsoft.com/partners/

The Partner Showcase is also a good place for inspiration as well as to take a look at some of the amazing things partners have built on the platform.

You can find the showcase here: https://PowerApps.microsoft.com/partner-showcase/

Next Steps

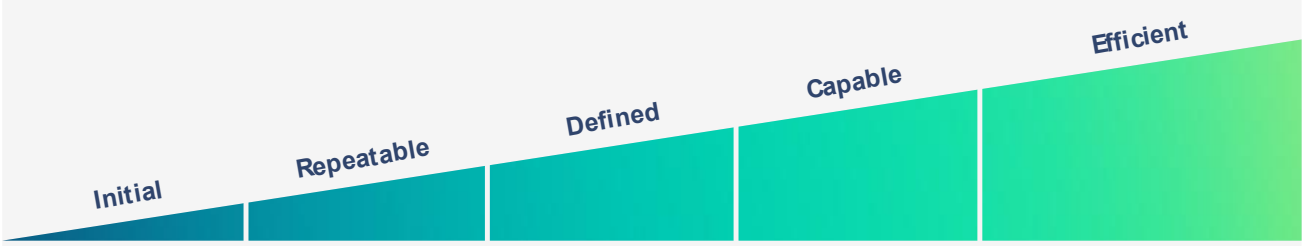
Undertake the Power Platform Adoption Assessment

If you are an organization just beginning your use of the Power Platform, or already have a substantial footprint of Power Platform usage, it is a worthwhile activity to undertake the Power Platform Adoption Maturity Assessment.

The goal of this model is to help organizations to align both their capabilities, but also their strategic transformation to better use the platform to drive organizational outcomes. The assessment is available here: https://learn.microsoft.com/en-us/assessments/3c62fd23-9d36-491c-8941-26d5553365f8/

Establishing a robust Power Platform governance structure is crucial for effective administration and usage, tailoring responsibilities to your organization's size and needs.

The model will rank organizations on a scale of 100 to 500.



Level 100	Level 200	Level 300	Level 400	Level 500
No overall strategy or governance, pockets of experimentation, apps limited to teams, focus is getting started.	Implementing central controls and policies, gaining tenant-wide visibility, managing environments and DLP, but still ad-hoc.	Standardizing practices, automating governance, makers sharing components, measurable success transforming business.	Mature managed processes, transforming critical apps, community for best practices and training, quantifying business value.	Power Platform key to digital strategy, rapid transformation of mission-critical capabilities, advanced integration, community influencing best practices.

The maturity assessment can function as a guide for your organization as you transform and bolster your organizations use of the Power Platform. Organizations will start at level 100 when they have no strategic guidance or plan for using the Power Platform. They will typically have some apps mostly using simple Excel and SharePoint connectors as well as some components from various SharePoint deployments. There will likely be very little use of the governance features described in this document. Organizations at this stage can begin the change management process through the organization of training events, hackathons, and lunch and learn session. They can nurture early adopters and recognize early success with the platform. At this stage, it is time to get serious about the adoption by appointing key custodians of the platform and a structure to manage governance of the platform.

Organizations at level 200 have begun to branch out with their use of environments. They have inconsistent and non-uniform strategy for managing governance and policy across the platform. They will likely have the CoE deployed and will make tactical use of some of the features of the CoE. They will not have a coherent environment strategy, governance strategy, or use of ALM or managed environments. Organizations at this stage will begin to enact on their governance and operational structure. They will undertake a DLP Impact Analysis to establish their starting policies.

At level 300 organizations are standardizing and automating governance processes, enabling makers to share components and achieve measurable success transforming business. The CoE defines environment strategies, application support tiers, and celebrates maker impact stories. At this

maturity level, organizations can develop environment strategies to balance governance and productivity, define tiers for app support based on criticality, and celebrate maker success stories. This stage is about standardizing practices, so opportunities include automating governance requests, sharing components between makers, and quantifying Power Platform's business impact.

At Level 400, Organizations have mature, automated processes for Power Platform management. They transform critical business capabilities and quantify impacts. Platform champions share best practices and make branded templates and components available. Organizations have mature processes and can create app catalogs for discoverability, use approvals and Teams to automatically communicate, and clarify responsibilities between admins, makers, and the CoE. Additional opportunities are establishing community channels for best practices sharing, offering branded templates and components, and conducting business value assessments.

At Level 500, Power Platform is key to the digital strategy, rapidly transforming mission-critical apps. Standardized processes and an expert community enable quick delivery of high-impact solutions. Advanced integration unlocks data, and execs sponsor Power Platform as a strategic asset. When Power Platform is strategic, opportunities include simplifying solution life-cycle management, enabling idea submission through apps, and influencing best practices community-wide. Organizations can rapidly transform business capabilities by integrating advanced features like AI, unlocking legacy system data, and gaining executive sponsorship.

The Maturity Adoption assessment serves as your organization's road map to Power Platform adoption, strategy, management, governance, and ultimately transformation into a nimble, highly agile organization of creators that can leverage highly advanced technology platforms to rapidly respond and evolve their business.

Develop your Environment Strategy

One of the initial activities your team should undertake is the building of an Environment Strategy. Key here is for you to understand.

- Which environments will be shared amongst many apps and developers
- How will you create Developer Environments and onboard developers. Enable environment routing.
- Restrict the creation of Production Environments
- How will you group environments?
- Defining how you will use managed environments for developers.

- Defining how you will use managed environments for test and production environments.
- What standard policies will you use for each group of environments?
- What standard pipelines will you create to release into your shared environments?
- How will people request new environments?
- How will people request to release new solutions into shared environments?

Develop an App Roadmap

Once you have developed a core governance strategy, it is essential that you begin to build a backlog of potential applications you can modernize and/or build. This backlog will function in multiple ways:

- As new makers onboard, an app backlog can give them a set of target apps that would be helpful to build. You can leverage new makers to help action this backlog and get strategic movement in directions that help your business.
- This backlog will help your organization understand the value proposition for the Power Platform, particularly where an app can provide a strategic outcome that turns the Power Platform center into a revenue generating center.

Your app backlog will help you plan how you will execute on building core functionality and agility using the power platform. It will also help to spur ideas about how other parts of your organization can leverage the platform to bolster their processes, business, and agility.

Assign Responsibility

Perhaps most importantly in your next steps journey is to setup a structure of responsibility for the Power Platform administration, operation, and governance. This motion will vary depending on the size and scale of your organization. While administration, operation, and governance can be handled by a small team for small organization, large organizations will likely need to split the operational components from the governance part to some degree.

You should choose a core set of Power Platform administrators. You can either assign them the Power Platform Administrator role and they can action the setup and administration of your Power Platform Tenant, or you can use PIMS as discussed above and allow these people to elevate to the Power Platform Administrator role as needed. The latter is useful in highly regulated environments that are typically seen in large enterprises, whereas the former is common in smaller operations.

You should also establish a governance function whose responsibility is twofold – Power Platform configuration and Power Platform usage. For small organization, you can setup a small set of empowered custodians who evaluate new features and products and decide when and how to roll them out to the organization. Their responsibility is to provide direction and oversight on how to build the organization around the use of the Power Platform. For larger organizations, however, the configuration of the Power Platform is likely something that will require a more robust governance structure such as a small advisory board or steering committee. Often, Power Platform governance sits on IT Governance Boards, Cloud Advisory Boards, and Cloud Business Offices within larger enterprises. From a Governance standpoint, the decision to use Power Platform and how risk is managed with it, is part of a broader, strategic governance discussion within the enterprise.

The second responsibility of the governance structure is to guide how the Power Platform is used within an organization. This includes decision making around many of the topics that are discussed in this document. Ultimately, the governance function needs to be able to steer the organization to use the Platform in effective and efficient ways. This includes everything from evaluating and designing an environment strategy, to dictating which DLP policies should apply to each environment, all the way to building and evangelizing apps, flows, agents, portals, and AI models on the platform.

Regardless of if you are part of a large enterprise, or a small organization having a group responsible for the day-to-day operation of the platform is key. For small organizations, this group will want to begin to build the beginnings of a very simple service catalog of common actions they can perform on the Power Platform including building new environments, adding, and removing people from roles, building new ALM pipelines, evaluating connectors and adding them to environment DLPs, and ultimately releasing apps to more secure production environments. This service catalog is the first step to building a Power Platform administrative team. In large organizations, these service items will be candidates for automation and can be delivered through custom built Power Apps and ITSM tooling. You can additionally take advantage of some of the features of the CoE toolkit to help accelerate your administrative team on their service management automation journey.

Execute

Perhaps the most important component of any strategy with any platform is how you execute on that strategy. By holding regular governance meetings that evaluate initiatives and progress on those initiatives, you can ensure that your team's strategy is being executed according to plan. The Power Platform is an incredibly useful and powerful tool that brings immense agility to organizations that leverage it. But behind every organization that leverages the Power Platform effectively is a team of champions that not only provide guidance and stewardship over its use but ensure that it is being used in a way that executes according to the organization's broader strategy. By leveraging the Power Platform community along with building champions within your organization, you can bolster your execution and realize the immense power that the platform provides.