VANCOUVER ISLAND
UNIVERSITY

VANCOUVER ISLAND UNIVERSITY

PRELIMINARY PRIVACY IMPACT ASSESSMENTS

Microsoft Task & Project Management Apps:

- **Lists**
- **Planner**
- **Project**
- **To Do**

Version #:	**V0.1 - Draft**
Date:	**March 28, 2023**

INITIATIVE TITLE:	**Review of Microsoft Apps:** • **Lists** • **Planner** • **Project** • **To Do**
ORGANIZATION:	Vancouver Island University (VIU)
BRANCH OR UNIT:	IT
YOUR NAME AND TITLE:	Moira Connor, PrivacyWorks Consulting, Inc.
YOUR WORK PHONE:	778.388.2585
YOUR EMAIL:	moira@privacyworks.ca
INITIATIVE LEAD NAME AND TITLE:	Brad Moran, IT Business Architect, Vancouver Island University
INITIATIVE LEAD PHONE:	250.753.3245
INITIATIVE LEAD EMAIL:	Brad.Moran@viu.ca
PRIVACY OFFICER:	Bill Boyte
PRIVACY OFFICER PHONE:	250.740.6554
PRIVACY OFFICER EMAIL:	FIPPA@viu.ca

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
NO
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
NO
Related PIAs, if any:
• **Microsoft Office 365** • **Microsoft BI** • **Microsoft Bookings** • **Microsoft Content Creation Apps: Editor, Forms, OneNote, Publisher, Sway & Whiteboard**

VERSION CONTROL

Date	Version	Author(s)	Version Notes
March 28, 2023	Draft	Moira Connor Use of Province of BC, PIA template for non-ministry public bodies.[1]	Initial draft released for review by Brad Moran.

INPUT AND REVIEW TABLE

Privacy Impact Assessment				
Name	**Position Title**	**Author**	**Contribute**	**Review**
Bill Boyte	Privacy Officer, Vancouver Island University			✓
Brad Moran	IT Business Architect, Vancouver Island University			✓
Moira Connor	Sr. Privacy Analyst, PrivacyWorks	✓		

[1] Complete a Privacy Impact Assessment - Province of British Columbia (gov.bc.ca)

DEFINITIONS

Acronym or Term	Description
Contact Information	Definition from FIPPA: *means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.*
FIPPA	*Freedom of Information and Protection of Privacy Act* *https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00*
Personal Information	means recorded information about an identifiable individual other than contact information and includes, but is not limited to: • Name, age, sex, weight, height • Home address and phone number • Race, ethnic origin, sexual orientation • Medical information • Health care history, including physical or mental disability • Number or symbol assigned to the individual • Income, purchases and spending habits • Blood type, DNA code, fingerprints • Marital or family status • Religion • Education • Financial information • Criminal information • Employment information • Personal views or opinions, except if they are about someone else • Personal Information - Province of British Columbia (gov.bc.ca)
PI	Personal Information
PIA	Privacy Impact Assessment
SOC 2	System and Organization Controls, Type 2
VIU	Vancouver Island University

TABLE OF CONTNETS

PART 1: GENERAL INFORMATION

1 Initiative Overview

Vancouver Island University (VIU) is looking to integrate a variety of Microsoft products with their Microsoft 0365 subscription.

This privacy impact assessment (PIA) will focus on the following in-scope Microsoft products typically used for task and project management.

- Microsoft Lists,
- Microsoft Planner,
- Microsoft Project, and
- Microsoft To Do.

This assessment is to be considered a genera**l,** or foundational**,** review of the in-scope products. In order to conduct specific privacy assessments of each product, VIU will need to:

- determine/document how VIU intends to use the products;
- define what user/customer data they will be collecting, using and disclosing;
- define who will have access to the products, and how that access will be managed; and
- define what configurations will be put in place to maximize privacy safeguards (including a "consent" box where applicable).

For purposes of this preliminary assessment, it has been assumed that VIU does not intend to collect Personal Information. Note that, depending on context, VIU end-user data such as name, phone number and email address may be considered business contact information, and thereby not covered by the *Freedom of Information and Protection of Privacy Act* (FIPPA).

This assessment uses the Province of BC's Privacy Impact Assessment for Non-Ministry Public Bodies template (as of March 2023)[2]. Source information was derived from a diverse range of resources, including Microsoft documentation and publicly accessible web content.

[2] Complete a Privacy Impact Assessment - Province of British Columbia (gov.bc.ca)

1.1 Description of In-Scope Applications

1.1.1 Microsoft Lists

Microsoft Lists is a powerful and versatile information management tool that is part of the Microsoft 365 suite of applications. It enables users to create, share, and manage customizable lists to organize and track information, collaborate with team members, and streamline various work processes. With its intuitive interface and integration with other Microsoft applications, Lists offers a flexible solution for a wide range of use cases, from simple to-do lists to complex project management and data tracking.

For additional information please refer to the Appendices Microsoft Lists.

1.1.2 Microsoft Planner

Microsoft Planner is a collaborative task management tool that is part of the Microsoft 365 suite of applications. Designed to simplify teamwork and improve organization, Planner enables users to create, assign, and organize tasks within visual boards called plans. These plans help teams stay on track, manage their workloads, and collaborate more efficiently.

Planner allows users to create tasks, set deadlines, and assign them to team members. Tasks can be organized into customizable categories called "buckets," which help in grouping related tasks and visualizing the overall progress. Each task can have a detailed description, checklist, labels for categorization, priority level, and file attachments, making it easy to keep all necessary information in one place.

For additional information please refer to the Appendices Microsoft Planner.

1.1.3 Microsoft Project

Microsoft Project is a comprehensive project management tool that is part of the Microsoft 365 suite of applications. It is designed to help project managers and teams effectively plan, execute, and control projects of varying complexity. With robust scheduling, resource management, and reporting features, Microsoft Project enables organizations to efficiently manage projects, track progress, and make data-driven decisions.

One of the key features of Microsoft Project is its powerful scheduling engine, which allows users to create and manage tasks, dependencies, and milestones. Users can define work durations, set deadlines, and create task relationships, ensuring a clear and accurate project timeline. The built-in Gantt chart view provides a visual representation of the project schedule, making it easy to monitor progress and identify potential issues.

For additional information please refer to the Appendices Microsoft Project.

1.1.4 Microsoft To Do

Microsoft To Do is a personal task management application that is part of the Microsoft 365 suite of applications. Designed to help users stay organized and manage their daily tasks and responsibilities, To Do offers a simple, intuitive interface for creating and organizing tasks, setting reminders, and prioritizing work. The application can be used for both personal and work-related tasks, making it a versatile tool for individuals and teams alike.

With Microsoft To Do, users can create tasks and add detailed notes, due dates, and priority levels. Tasks can be organized into customizable lists, allowing users to group related tasks and manage multiple projects or responsibilities. To Do also supports subtasks through the use of checklists within individual tasks, enabling users to break down complex tasks into smaller, manageable steps.

For additional information please refer to the Appendices Microsoft To Do.

2 PIA Scope

2.1 In Scope

This preliminary privacy impact assessment (PIA) is specific to the following Microsoft Content Creation Apps:

- Microsoft Lists,
- Microsoft Planner,
- Microsoft Project, and
- Microsoft To Do.

2.2 Out of Scope

This PIA assesses the in-scope content creation apps but does not assess specific use cases of those apps. Specific use cases are required to better understand how Vancouver Island University will use the app and what data they intend to collect, use, store, or disclose.

3 Data or Information Elements Included

3.1 Types of Information

A general summary of the types of information collected by each of the in-scope Microsoft applications is described in the table below.

Please note that the specific data collected and processed by these applications would vary depending on the user's settings and usage patterns. Additionally, Microsoft may update the data collection practices of these applications from time to time.

Application or Service	Types of Information Collected[3]	Link to Detail Table
Microsoft Lists	• List name and description • Columns with custom types, such as text, numbers, dates, or choices • List items with values for each column • Attachments or links associated with list items • Permissions and access control for the list • Comments or conversations related to list items • Rules and automation for list items	Microsoft Lists
Microsoft Planner	• Plan name and description • Plan members and their roles • Tasks with titles, descriptions, due dates, and priority levels • Task assignees • Task progress status (e.g., not started, in progress, completed) • Task labels and categories • Task attachments, such as documents, images, or links • Comments and conversations related to tasks • Task checklists	Microsoft Planner
Microsoft Project	• Project name and description • Start and end dates for the project • Tasks with names, durations, dependencies, and constraints • Task progress status and completion percentages • Resource names, types, and availability (e.g., people, equipment, materials) • Resource assignments to tasks • Resource costs and budgets	Microsoft Project

[3] In addition to customer and diagnostic data.

Application or Service	Types of Information Collected[3]	Link to Detail Table
	• Baseline and actual data for tasks, resources, and costs • Custom fields and formulas • Gantt charts, calendars, and other visual representations of project data	
Microsoft To Do	• Task lists with names and descriptions • Tasks with titles, descriptions, and due dates • Task priorities and reminders • Recurring tasks and frequency • Task categories, such as work or personal • Task attachments, such as files or links • Task notes and comments • Shared task lists with other users	Microsoft To Do

3.2 Personal Information

It is not intended that VIU collect Personal Information in the in-scope Microsoft applications. Depending on the context in which it is used, information that is specifically provided to contact a person at their place of business may not be considered Personal Information (e.g., name, phone number and email address).

Upon identifying the specific VIU use-cases for each in-scope Microsoft application (Lists, Planner, Project, and To Do), VIU should determine which use-cases intend to collect Personal Information or have a high likelihood of inadvertently collecting it. Those applications will require a further privacy review.

In general, the risk that the Microsoft apps included in this assessment would collect Personal Information (beyond business contact information), are defined as follows:

App	General Risk Level	Risk Rating Explanation
Microsoft Lists	High	The risk of collecting Personal Information in **Lists** is high due to its flexibility and customizability, which allows users to create lists for any purpose, including collection of personal data.

App	General Risk Level	Risk Rating Explanation
Microsoft Planner	Low to Moderate	Although **Planner** might collect some Personal Information like user-names and email addresses, the risk of collecting non-business Personal Information is relatively low. However, users could include Personal Information in task descriptions, attachments, or comments.
Microsoft Project	Low	**Project** typically collects and stores data related to projects and work schedules. The risk of collecting non-business Personal Information is low.
Microsoft To Do	High	**To Do** is a personal task management application, which means users might create tasks or notes that include Personal Information unrelated to business contact information. Since To Do can be used for both personal and work purposes, it presents a higher risk of collecting Personal Information compared to the other applications.

Microsoft Lists and Microsoft To Do have the highest risk of collecting Personal Information due to their customizable nature and usage for both personal and work-related tasks. The risk ultimately depends on how users set up and use these applications.

4 Reducing Risk of Unintentional PI Collection or Disclosure

4.1 General

The actual VIU use of each of the Microsoft applications (Lists, Planner, Project and To Do) would need to be assessed to determine the most appropriate means of reducing risk of unintentional PI collection or disclosure.

Across all applications, the VIU administrator should implement general best practices, such as:

- Enforcing strong password policies and enabling multi-factor authentication to protect user accounts and data.
- Training users on data protection and privacy principles, as well as VIU's data handling policies and relevant privacy regulations.
- Regularly monitoring and auditing user activity to detect and address any potential issues or privacy risks.

Specific actions to minimize the risk of unauthorized Personal Information collection or disclosure for the assessed applications is included below. Please reference the more detailed information included in the appendices for each application.

4.1.1 Microsoft Lists

- Set up strict access control and permissions for each list to ensure that only authorized users can view or modify the data.
- Create templates for lists with predefined columns to discourage users from adding columns that collect unnecessary Personal Information.
- Regularly review and audit the lists to ensure that they comply with company data policies and privacy regulations.
- Train users on how to create and manage lists responsibly, emphasizing the importance of not collecting Personal Information unless absolutely necessary.

4.1.2 Microsoft Planner

- Limit the number of users who can create or modify plans and tasks to reduce the likelihood of collecting Personal Information.
- Establish a clear naming convention and task description policy that discourages the inclusion of Personal Information.
- Train users on best practices for using Planner, emphasizing the need to avoid sharing Personal Information in tasks, comments, or attachments.
- Regularly monitor and audit plans to ensure they comply with company data policies and privacy regulations.

4.1.3 Microsoft Project

- Restrict access to project files by using strict access control and permissions, ensuring that only authorized users can view or modify project data.
- Establish guidelines for creating and managing project tasks, resources, and budgets that discourage the inclusion of Personal Information.
- Train users on best practices for using Project, emphasizing the need to avoid sharing Personal Information in tasks or resource assignments.
- Regularly review and audit project files to ensure they comply with company data policies and privacy regulations.

4.1.4 Microsoft To Do

- Enforce VIU policies that discourage users from creating tasks or notes with Personal Information unrelated to work.
- Train users on best practices for using To Do, emphasizing the importance of not mixing personal and work-related tasks within the organizational account.

- Regularly remind users to avoid sharing task lists containing Personal Information with colleagues or external parties.

PARTS: 2 – 8 – NOT APPLICABLE

For purposes of this foundational PIA, it has been assumed that VIU will not collect Personal Information, thereby completion of parts 2-8 of the PIA template are not required. Note that an addendum PIAs will be required if further VIU analysis determines use cases that may include Personal Information.

PART 9: SIGNATURES

5 PRIVACY OFFICE

Privacy Office Comments

Privacy Office Signatures

This PIA accurately documents in-scope Microsoft applications at the time of signing.

If there are any changes to the overall initiative, including if Personal Information will, or could, be collected, used, stored, or disclosed, the Vancouver Island University program area lead will engage with the privacy officer, and complete a PIA update.

Role	Name	Electronic signature	Date signed
Privacy Officer, Vancouver Island University	**Bill Boyte**		

6 PROGRAM AREA SIGNATURES

This PIA accurately documents in-scope Microsoft applications at the time of signing.

If there are any changes to the overall initiative, including if Personal Information will, our could, be collected, used, stored, or disclosed, the Vancouver Island University program area lead will engage with the privacy officer, and complete a PIA update.

Program Area Comments

Role	Name	Electronic signature	Date signed
IT Business Architect, Vancouver Island University	Brad Moran	[redacted]	May 10, 2023

s. 22(1)

PART 10 – APPENDICES

7 APPENDIX A: SUMMARY INFORMATION OF APPS

7.1 Microsoft Lists

Category	Microsoft Lists
Description:	Microsoft Lists is a powerful and versatile tool for organizing, tracking, and sharing information across teams within an organization. It is integrated with other Microsoft applications such as SharePoint, Teams, and Power Platform. With Microsoft Lists, users can create customizable lists to manage tasks, track issues, inventory, events, or other structured data types. Lists can be created from scratch or by using a variety of pre-built templates to streamline the process. These templates can be further tailored to meet the specific needs of a team or project. Features of Microsoft Lists include: • Customizable views: Users can create different views for the same list, such as grid, calendar, or gallery views, allowing them to visualize and interact with data in a way that best suits their needs. • Conditional formatting: Lists can be configured with rules to automatically highlight, or format rows based on the data in specific columns, making it easier to identify trends, issues, or priorities. • Integration with Microsoft Teams: Lists can be embedded within a Teams channel, enabling seamless collaboration and communication around the data in the list. • Collaboration: Multiple users can work on the same list simultaneously, with real-time updates and version history available for tracking changes. • Access control: Permissions can be set to control who can view or edit a list, ensuring that sensitive data is only accessible to authorized users. • Automation: Integration with Power Automate allows users to create automated workflows to perform actions based on triggers, such as sending notifications or updating other lists when certain conditions are met.

Category	Microsoft Lists
Platforms:	Microsoft Lists runs on Windows, Mac, Android, iOS, and web platforms.
Key Data Inputs:	Users provide data values and configurations to Lists to create, customize and manage their lists. These can be categorized as: • List items: The individual rows of data in a list, each containing multiple fields (columns) with specific data types, such as text, numbers, dates, or choices. • Columns: The fields within a list that define the structure and data types of the list items. Users can create various column types, such as single line text, multiple lines of text, number, date and time, choice, person or group, and lookup, among others. • Views: Customized visual representations of the list data, defined by filters, sorting, grouping, and display options. Users can create multiple views for a single list to display the data in different formats, such as grid, calendar, or gallery views. • Formatting rules: Conditional formatting rules can be applied to rows or columns, allowing users to automatically highlight or format list items based on specific criteria, such as data values or date ranges. • Permissions: Access control settings that determine which users can view, edit, or manage a list, ensuring that sensitive data is accessible only to authorized individuals. • Templates: Pre-built list templates with predefined columns and settings, which can be used as a starting point for creating new lists. Users can choose from a variety of templates or create their own custom templates. • Automation: Integration with Power Automate enables users to create automated workflows with triggers and actions based on specific list events or conditions, streamlining list management and enhancing productivity.
Collection of Diagnostic Data:	Microsoft does not provide a specific breakdown of diagnostic data collected solely by Lists. General information on diagnostic

Category	Microsoft Lists
	data collected by Microsoft 365 services, which includes Lists, is as follows: • Required service data: This level of data includes information necessary for maintaining and troubleshooting the service. It may consist of data like error logs, performance metrics, and device information. This data is essential for Microsoft to identify and resolve issues that may arise during the use of the service. Note that this collection can't be disabled as it's necessary for the functionality and reliability of the service. • Optional diagnostic data: This level of data helps Microsoft improve its products and services, and includes additional details about the device, application usage, and performance. Optional diagnostic data might encompass information about feature usage, reliability, and responsiveness.
Collection of Customer Data:	Customer data collected in Lists typically includes: • List content: This includes the list items, columns, and metadata that users input while creating and managing lists. The data can encompass text, numbers, dates, choices, person or group, and other column types, depending on the user-defined structure of the list. • List configurations: This includes settings such as views, formatting rules, permissions, templates, and automation configurations that users define to customize and manage their lists. • Collaboration data: This encompasses data related to users' interactions with the list, such as sharing, comments, and version history, which helps track changes and facilitate collaboration within teams. • Attachments: Users can attach files, images, and other resources to list items, which are then stored within Microsoft Lists as part of the customer data.
Data Collected and/or Processed:	Lists collects and processes Customer data and Diagnostic data.

Category	Microsoft Lists
Personal Information Collected:	There is no inherent collection of Personal Information in Lists. Personal information collected in Lists is totally dependent on what Personal Information a user inputs when they create and manage lists. Personal information could include: • User and contact details: Users might create columns that store Personal Information such as names, email addresses, phone numbers, or job titles. • Person or group column: This column type allows users to reference other users within the organization, which may contain Personal Information like names, email addresses, or job titles. • Comments and collaboration: Users can add comments to list items or collaborate with others, which may include Personal Information if users choose to disclose it within the comments. • Attachments: Users can attach files, images, or other resources to list items, which may contain Personal Information if the attached files include such data.
Customer Data Storage Location:	In Canada, Microsoft has two data center regions: • Canada Central: Located in Toronto, Ontario • Canada East: Located in Quebec City, Quebec Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Learn
Built-In Integrations:	List has built-in integrations with: • SharePoint: Lists is built on top of SharePoint, which provides the underlying infrastructure for storing and managing list data. Users can create lists within SharePoint sites, and benefit from SharePoint's features such as document libraries, versioning, and access controls. • Microsoft Teams: Users can integrate Lists directly into Microsoft Teams channels, allowing team members to access, edit, and collaborate on lists without leaving the Teams environment. This seamless integration fosters better communication and collaboration around list data.

Category	Microsoft Lists
	• Power Platform: Lists can be integrated with Power Apps and Power Automate to create custom applications and automate workflows. a. Power Apps: Users can create custom forms and applications using list data as a data source, enabling more advanced data management and interaction scenarios. b. Power Automate: Users can automate tasks and processes by creating workflows that interact with Lists, such as sending notifications, updating other lists, or integrating with external services based on specific triggers and conditions. • Microsoft Graph API: Developers can use the Microsoft Graph API to interact with list data programmatically, enabling custom integrations with other applications and services within and outside the Microsoft 365 ecosystem. • OneDrive: Attachments added to list items can be stored in OneDrive, allowing users to leverage OneDrive's file management, sharing, and collaboration features. • Microsoft Planner: Users can create tasks in Microsoft Planner directly from list items, enabling better task management and tracking within the context of a project or team.
Optional Integrations/ Connections Requiring Configuration:	In addition to the built-in integrations, Microsoft Lists can also connect with other applications and services using optional integrations, add-ons, or connectors. • Power Automate Connectors: Power Automate offers hundreds of connectors that can be used to integrate Lists with external services and applications. Such as: Salesforce, ServiceNow, Google Sheets, and Trello. Users can create custom workflows that automate processes between Lists and these services based on specific triggers and actions. • Custom Applications: Developers can build custom applications using Microsoft Graph API or SharePoint REST API to interact with Lists data, allowing for tailored integrations with other software and services within and outside the Microsoft 365 ecosystem.

Category	Microsoft Lists
	• Third-party Add-ons and Extensions: Microsoft 365 supports various third-party add-ons and extensions that can be used to enhance the functionality of Lists or connect with other services. Examples include project management tools, visualization solutions, and reporting tools. Users should check the compatibility and availability of these add-ons for Lists specifically. • Power BI: While not a direct integration, users can export data from Lists to Power BI to create advanced visualizations, dashboards, and reports that provide insights into their data. • Office Scripts: Users can create custom Office Scripts to automate tasks and interact with Lists data in Excel. This enables users to manipulate and analyze list data within Excel while leveraging Excel's advanced features.
Activity Logging - End-user controls:	Activity logging is primarily managed at the organizational level by administrators. However, end-users can make use of certain features in Lists and the broader Microsoft 365 environment that may impact activity logging: • Version history: Lists maintains a version history for each list item, which records changes made to the item, along with the timestamp and the user who made the changes. End-users can view and restore previous versions of list items if they have the necessary permissions. • Item-level auditing: While end-users do not have direct control over activity logging, they can view the details of individual list items, which may include information about who created the item, when it was last modified, and who made the modifications. • Compliance and security settings: End-users with the necessary permissions can manage access controls and sharing settings for Lists. They can control who has access to the list and its data, which indirectly impacts the scope of activity logging by determining which users' actions will be logged.
User Activity Reports:	Using the Microsoft 365 audit log, VIU administrators can access and generate user activity reports for Lists, and other

Category	Microsoft Lists
	Microsoft 365 services, to monitor user actions such as creating, modifying, sharing, and deleting lists or list items.
Auditing:	Various user activities are logged and can be viewed in an audit report generated from the Microsoft 365 audit log. Some of the key activities logged in Lists include: • List creation and deletion: Creating or deleting a list. • List modification: Modifying list settings, such as changing views, applying formatting, or updating permissions. • List item creation, modification, and deletion: Adding, editing, or deleting list items. • Sharing and access control changes: Granting or revoking user access to a list or list item and modifying sharing settings. • Item version history actions: Restoring a previous version of a list item. • Column creation, modification, and deletion: Adding, editing, or removing columns in a list. • List item attachment actions: Adding, modifying, or deleting attachments in list items. • Integration actions: Creating or updating connections with Power Apps or Power Automate or integrating Lists with Microsoft Teams. • Commenting and collaboration: Adding, modifying, or deleting comments on list items. • List import and export actions: Importing data into Lists from Excel or exporting list data. When viewing the audit report, each logged activity will display relevant information, such as the timestamp, user details, and metadata associated with the activity.
Security Compliance:	Relevant Microsoft compliance: • ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS). • SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance,

Category	Microsoft Lists
	demonstrating strong internal controls and security practices. • ISO/IEC 27018: Microsoft Lists is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. • NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.
Privacy Safeguards:	Some of the privacy safeguards specific to Lists include: • **List sharing and permissions**: Microsoft Lists enables granular control over list sharing and permissions. You can control who has access to a list and what actions they can perform (view, edit, or manage). This allows organizations to limit access to sensitive data and ensure that only authorized users can view or modify list items. • **Column-level security:** In Microsoft Lists, you can apply column-level security to restrict access to specific columns within a list. This feature is particularly useful when dealing with sensitive data that should only be accessible to certain individuals within an organization. • **Item-level permissions**: Microsoft Lists allows you to set item-level permissions, enabling you to control access to individual list items. This provides an additional layer of privacy and security by ensuring that only specific users can view or edit particular list items. • **Versioning and auditing**: Lists support versioning, which helps maintain a history of changes made to list items. This feature allows you to track modifications and identify any unauthorized access or changes. Additionally, Microsoft Lists activities can be audited through the Microsoft 365 audit log, providing visibility and control over user actions.
Potential Privacy Risks:	Examples of potential privacy risks in Lists are as follows: • Inadequate access controls: If access controls and permissions are not set up properly, unauthorized users may gain access to sensitive data in Lists. This could lead to

Category	Microsoft Lists
	unintentional data exposure or misuse of Personal Information. • Data input by users: Lists allows users to create and manage structured data, which could include Personal Information. If users store sensitive data in Lists without proper access controls or data handling policies, this information may be at risk of unauthorized access or misuse. • Data sharing and collaboration: Lists facilitates collaboration by allowing users to share lists and list items with others, both inside and outside the organization. If sharing settings are not managed correctly, sensitive data may be exposed to unauthorized individuals. • Attachments: Users can attach files to list items, which may contain Personal Information. If attachments are not managed properly, they may pose a risk to the privacy of the individuals whose data is stored within the files. • Human error: Users may inadvertently disclose Personal Information through list item comments, collaboration features, or improper data handling. Human error can lead to unintentional data exposure.
Privacy Risk Mitigations:	Potential risk mitigations include the following: • Proper access controls and permissions: Set up access controls and permissions at the list level to ensure that sensitive data is accessible only to authorized individuals. • Data handling policies: Establish and enforce data handling policies that clearly define the types of data that can be stored in Lists and the appropriate methods for handling sensitive information. • Privacy-aware user training: Provide regular training to users on privacy best practices, focusing on the proper use of Lists and its features. • Secure sharing practices: Implement guidelines and best practices for sharing lists and list items both within and outside the organization. • Attachment management: Establish policies for handling attachments in Lists, including the types of files that can be attached and the appropriate access controls for those files.

Category	Microsoft Lists
	• Regular monitoring and auditing: Perform regular monitoring and auditing of user activities. Identify potential privacy risks and take corrective action as needed. Review and update access controls, sharing settings, and data handling practices based on audit findings.
Other Key Links:	• https://www.microsoft.com/en-us/microsoft-365/microsoft-lists • https://www.youtube.com/watch?v=plshQSoe_OY • https://adoption.microsoft.com/en-us/microsoft-lists/resources/ • https://support.microsoft.com/en-us/microsoft-lists • https://learn.microsoft.com/en-us/microsoftteams/manage-lists-app • https://techcommunity.microsoft.com/t5/microsoft-365-blog/configure-forms-and-rules-in-microsoft-lists/ba-p/2088300 • https://techcommunity.microsoft.com/t5/microsoft-365-blog/announcing-microsoft-lists-your-smart-information-tracking-app/ba-p/1372233

7.2 Microsoft Planner

Category	Microsoft Planner
Description:	Microsoft Planner is an intuitive, collaborative task management tool that enables people to plan, manage, and complete task-based initiatives. Users assign and manage tasks on a Kanban board using task cards, which they can populate with various important plan information, such as due dates, status, checklists, labels, and file attachments. Planner integrates with several Microsoft solutions, including Microsoft Teams. Depending on the Microsoft subscription plan, the following task planning features may be available: • Add assignments, start and due dates, bucket, progress, and priority to tasks • Add labels, checklist, attachments to tasks • Filter and group tasks • Copy plan • Export plan to Excel • View Planner tasks in Charts view • View Planner tasks in Schedule view • See Planner tasks in Outlook calendar • See Planner tasks in Microsoft To Do • Planner API in Microsoft Graph • Tasks app in Teams • SharePoint integration (Planner web part and full page app)
Platforms:	As a web-based tool, Planner is accessible from anywhere and available as a mobile app for both iOS and Android.
Key Data Inputs:	Microsoft Planner end-user input: • Tasks - title, description, due date, priority, labels, and assigned team members; • Buckets – groupings of tasks; • Plans – collections of tasks and buckets; • Members – team members responsible for completing tasks;

Category	Microsoft Planner
	• Progress status – such as Not Started, In Progress, or Completed; • Due Dates – assigned to tasks; • Labels – if required to categorize and filter tasks; and • Attachments – files, images or links.
Collection of Diagnostic Data:	Microsoft collects the following diagnostic data: • Usage Data • Device and Application Data • Performance Data • Error reports and crash related data • User and organization identifiers (e.g., typically anonymized)
Collection of Customer Data:	• **User and account data**: This includes information about the user's identity, such as name, email address, and user ID, as well as organization or tenant information. This data is required for authentication, authorization, and user management within Microsoft Planner. • **Customer content**: information users input into Microsoft Planner, such as task details, plan names, bucket names, task assignments, comments, labels, due dates, and attachments. Microsoft stores this data to provide the Planner service and ensure seamless access to users. • **Metadata:** information related to user activities in Planner, such as timestamps of task creation or modification, user identification (anonymized), and the relationship between tasks, buckets, and plans. • **Service-generated logs**: Microsoft collects log data generated during user interactions with Planner, such as IP addresses, device information, and browser types.
Data Collected and/or Processed:	• User and Account Data • Customer Content Data • Metadata • Service-generated Logs

DRAFT – FOR REVIEW ONLY

Category	Microsoft Planner
	• Diagnostic Data
Personal Information Collected:	There is no inherent collection of Personal Information in Planner. Personal information collected in Planner is totally dependent on what Personal Information a user inputs when they create and manage their tasks. Examples of the Personal information that Planner could collect include: • **User identification data**: This includes the user's name, email address, job title, and profile picture. This data is used for authentication, authorization, and to display user information within the Planner interface. • **User-generated content**: When users interact with Planner, they input data such as task titles, descriptions, comments, and attachments. While this content is generally related to tasks and projects, it could potentially include Personal Information if users choose to include it. • **Contact information**: If users choose to invite others to join a plan, they might input the email addresses or other contact details of those individuals. • **IP addresses and device information**: Microsoft Planner may collect IP addresses, device information (such as device type, operating system, and browser version), and other technical data when users access the service. While this data is typically used for maintaining and improving the service, it could potentially be used to identify an individual in certain cases.
Customer Data Storage Location:	In Canada, Microsoft has two data center regions: • Canada Central: Located in Toronto, Ontario • Canada East: Located in Quebec City, Quebec Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Learn

Category	Microsoft Planner
Built-In Integrations:	• **Microsoft Teams**: Planner can be added as a tab within a Microsoft Teams channel, allowing team members to collaborate on tasks and projects directly from Teams. Users can create, assign, and update tasks, as well as discuss them in the Teams channel. • **Microsoft Outlook**: Planner tasks can be synced with the user's Outlook calendar, displaying task due dates alongside other calendar events. Additionally, Planner can send email notifications about task assignments, due dates, and status updates. • **SharePoint:** Planner integrates with SharePoint, enabling users to create a plan directly from a SharePoint site. Additionally, users can link Planner tasks with SharePoint documents, providing easy access to relevant files and resources. • **OneNote:** Planner tasks can be linked to OneNote pages or sections, allowing users to create and manage detailed notes related to their tasks. • **Power Automate** (formerly Microsoft Flow): Users can create automated workflows between Planner and other Microsoft 365 apps or third-party services using Power Automate. Examples include automatically creating tasks based on flagged emails, sending notifications when tasks are completed, or updating a SharePoint list when a task's status changes. • **Power BI**: Users can create visual reports and dashboards in Power BI using data from Planner, enabling deeper analysis of task progress, team productivity, and project status. • **To-Do:** Tasks from Planner can be integrated with Microsoft To-Do, allowing users to manage their Planner tasks alongside their personal to-do lists.
Optional Integrations/ Connections Requiring Configuration:	Planner can be integrated with third-party applications and services through connectors and APIs. Some examples include: • Trello • Asana

Category	Microsoft Planner
	• Slack • GitHub • Jira • Salesforce • Google Workspace
Activity Logging - End-user controls:	Activity logging controls are primarily managed at the organizational level by administrators. However, users can **view** some activity logs related to their tasks and plans within Planner.
User Activity Reports:	Using the Microsoft 365 audit log, VIU administrators can access and generate user activity reports for Planner, and other Microsoft 365 services, to monitor user actions such as creating, modifying, sharing, and deleting plans or related plan items.
Auditing:	The following Planner activities are logged with relevant details, such as who performed the action, and the timestamp of the action: • Task creation: When a user creates a new task in Planner. • Task modification: When a user modifies a task's details, such as title, description, due date, priority, or labels. • Task assignment: When a user assigns or reassigns a task to another user or themselves. • Task completion: When a user marks a task as completed. • Task deletion: When a user deletes a task. • Task comments: When a user adds, modifies, or deletes a comment on a task. • Plan creation: When a user creates a new plan in Planner. • Plan modification: When a user modifies a plan's details or settings. • Plan deletion: When a user deletes a plan. • Bucket creation: When a user creates a new bucket within a plan. • Bucket modification: When a user modifies a bucket's details, such as the name or task order.

Category	Microsoft Planner
	• Bucket deletion: When a user deletes a bucket.
Security Compliance:	Relevant Microsoft compliance: • ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS). • SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance, demonstrating strong internal controls and security practices. • ISO/IEC 27018: Microsoft Planner is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. • NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.
Privacy Safeguards:	Microsoft privacy safeguards that are specific to Planner include (but are not limited to): • **Limited external sharing**: Planner does not support sharing plans or tasks with external users by default, reducing the risk of unauthorized access or data exposure. External sharing is possible only if the organization enables guest access through Azure Active Directory (AAD) and Microsoft 365 Groups, which still provides controlled access. • **Plan membership management**: Access to a plan in Planner is controlled through membership in the corresponding Microsoft 365 Group. Users can only view and interact with the plans they are members of, providing a level of access control specific to Planner. • **Clear separation of plans**: In Planner, each plan is separate and distinct, ensuring that users can only access the plans they are members of, and the data

Category	Microsoft Planner
	within one plan is not exposed to users in other plans. This structure creates a natural barrier to help safeguard privacy within the context of Planner. • **Task-level access control:** Planner allows users to control who can access a task by assigning it to specific individuals. While other team members can still view the task, only the assignees can interact with it or receive notifications related to it.
Potential Privacy Risks:	While Microsoft Planner incorporates privacy safeguards, there are still potential privacy risks associated with its use. Some of these risks include: • **Unauthorized access**: If access controls and permissions are not properly configured, unauthorized users may gain access to sensitive data within a plan or task. • **Inadvertent data sharing**: Users may inadvertently share sensitive information or personal data within tasks, comments, or attachments, making it accessible to other plan members. • **Data retention**: Data may not be retained and deleted in compliance with FIPPA and/or VIU policy. • **Third-party integrations**: Integrating Planner with third-party applications and services may introduce potential privacy risks if these integrations are not properly vetted or configured. • **Human error**: Users may accidentally delete, modify, or disclose sensitive data in Planner.
Privacy Risk Mitigations:	• **Access controls and permissions**: Ensure that proper access controls and permissions are configured for **each** plan in Planner, limiting access to authorized users only. • **User training and awareness**: Educate users to be mindful of the information they share in Planner and to report any suspected privacy incidents. • **Data retention policies**: Define and implement data retention policies that align with FIPPA and VIU policy.

Category	Microsoft Planner
	• **Third-party integrations**: Carefully evaluate the privacy policies and data handling practices of third-party applications and services before integrating them with Planner. • **Role-based access controls**: Implement role-based access controls to limit user actions to help prevent accidental or unauthorized access, modification, or deletion of sensitive data in Planner. • **Regular audits and monitoring**: Regularly audit user activity in Planner through the Microsoft 365 audit log to identify and address any potential privacy risks or violations.
Other Key Links:	• https://www.microsoft.com/en-ca/microsoft-365/business/task-management-software • https://learn.microsoft.com/en-us/office365/planner/ • https://learn.microsoft.com/en-us/office365/planner/planner-for-admins#how-do-i-turn-off-planner-for-my-organization • https://support.microsoft.com/en-us/planner • https://learn.microsoft.com/en-us/graph/planner-concept-overview

7.3 Microsoft Project

Category	Microsoft Project
Description:	Microsoft Project is a project management software developed by Microsoft. It is designed to help project managers and teams effectively plan, execute, and control projects by providing tools to manage tasks, resources, budgets, and schedules. Microsoft Project offers a range of features including: • **Task scheduling and management**: Microsoft Project allows users to create and assign tasks, set deadlines, allocate resources, and track progress. It also supports task dependencies, which helps project managers understand the order in which tasks need to be completed. • **Resource management**: Microsoft Project enables project managers to manage resources such as personnel, equipment, and materials effectively. Users can allocate resources to tasks, track resource utilization, and manage resource availability and conflicts. • **Gantt charts**: Microsoft Project supports Gantt charts, which are visual representations of a project's timeline. Gantt charts display tasks, their durations, and dependencies, making it easier to understand the project's overall progress and timeline. • **Timeline views**: The software offers various timeline views, allowing project managers to see a high-level overview of the project schedule or focus on specific tasks and milestones. • **Budgeting and cost management**: Microsoft Project includes features for managing project budgets, such as estimating costs, tracking expenses, and comparing planned vs. actual costs. • **Reporting and analytics**: The software provides a range of customizable reports and analytics tools to help project managers track progress, analyze performance, and identify potential issues. • **Collaboration and integration**: Microsoft Project can be integrated with other Microsoft products like Office

Category	Microsoft Project
	365, SharePoint, and Microsoft Teams, facilitating collaboration and communication among team members.
Platforms:	Microsoft Project is available on multiple platforms, including: 1. **Desktop:** Microsoft Project offers a standalone desktop application for Windows operating systems. 2. **Web-based**: Microsoft Project also offers a web-based version called "Project for the web," which is part of the Microsoft 365 suite. This cloud-based solution allows users to access and manage their projects from any device with an internet connection using a web browser. 3. **Mobile:** Microsoft Project does not have a dedicated mobile app; however, Project for the web can be accessed through mobile web browsers on smartphones and tablets, enabling users to view and manage their projects on the go. Additionally, Microsoft Project can be integrated with other Microsoft applications like Office 365, SharePoint, and Microsoft Teams to facilitate collaboration and communication among team members across different platforms.
Key Data Inputs:	Microsoft Project requires several key data inputs for end-users to effectively plan, execute, and control projects. These include: • Project information • Task information • Task dependency information • Resources available • Resource assignments • Project constraints • Project Milestones • Budget and cost information • Baseline data • Risks and potential issues • Any custom fields required by VIU

Category	Microsoft Project
Collection of Diagnostic Data:	Microsoft collects diagnostic data to improve the performance, reliability, and overall user experience of their products, including Microsoft Project. While the exact diagnostic data collected may vary depending on the version and platform (desktop or web-based), some common types of diagnostic data specific to Microsoft Project include: • **Usage data**: This includes information about how users interact with Microsoft Project, such as features used, frequency of use, and duration of usage sessions. • **Performance data**: Microsoft may collect data related to the performance of Microsoft Project, such as application startup time, responsiveness, and resource usage. • **Error reports**: If users encounter errors or crashes while using Microsoft Project, diagnostic data about these events may be collected. This data can include details about the error, the state of the application when the error occurred, and other relevant information to help Microsoft troubleshoot and fix the issue. • **Device and environment data**: This data may include information about the user's device, operating system, browser, and other applications installed on the device. • **Project-specific data**: While Microsoft does not collect the actual project data, such as task names, durations, or resource assignments, it may collect metadata or anonymized data related to the size, complexity, or structure of projects. This information can help Microsoft understand typical usage patterns and improve the product accordingly. Note that Microsoft has strict privacy policies in place to ensure that the diagnostic data collected is anonymized, aggregated, and securely stored. Users can also review and adjust their privacy settings within the Microsoft Project application or Microsoft 365 account settings to control the diagnostic data that is collected.

Category	Microsoft Project
Collection of Customer Data:	When using Microsoft Project, particularly the cloud-based "Project for the web" version, some customer data may be collected and stored on Microsoft servers. However, Microsoft has strict policies in place to ensure that the customer data collected is limited, secured, and used only for the purpose of providing and improving the service. Some customer data that may be collected specific to Project includes: • **Account information**: This includes user account details such as name, email address, organization, and user preferences. • **Project data**: When using Project for the web, project information such as tasks, resources, schedules, and other project details, is stored on Microsoft's servers. This data is used to provide the project management service and enable features such as collaboration, reporting, and integration with other Microsoft services. • **Usage data**: Microsoft may collect anonymized data about how users interact with Project for the web, such as the features used, the frequency of use, and duration of usage sessions. • **Support and feedback data**: If users contact Microsoft support or provide feedback about Microsoft Project, some customer data, such as contact information, may be collected to facilitate communication and address issues or concerns.
Data Collected and/or Processed:	Microsoft Project, particularly the cloud-based "Project for the web" version, may collect and process different types of data to provide and improve the service. The data collected can be broadly categorized into two groups: customer data and diagnostic data. • **Customer data**: This refers to the data that users input or generate while using Microsoft Project. It includes: a. Account information b. Project data

Category	Microsoft Project
	c. Support and feedback data: • **Diagnostic data**: This refers to the data collected by Microsoft to improve the performance, reliability, and overall user experience of their products, including Microsoft Project. The diagnostic data may include: a. Usage data b. Performance data c. Error reports d. Device and environment data
Personal Information Collected:	The Personal Information that may be collected specifically in Microsoft Project includes: • **Account information**: This includes user account details such as name, email address, organization, job title, and user preferences. • **Contact information**: If users contact Microsoft support or provide feedback about Microsoft Project, their contact information, such as name, email address, and phone number, may be collected to facilitate communication and address issues or concerns. • **User-generated content**: When users collaborate within a project or use communication features integrated with Microsoft Project, such as comments or notes, this user-generated content may be stored on Microsoft servers. • **User preferences and settings**: Microsoft Project may collect information about users' application preferences and settings, such as language, time zone, and other customization options.
Customer Data Storage Location:	In Canada, Microsoft has two data center regions: • Canada Central: Located in Toronto, Ontario • Canada East: Located in Quebec City, Quebec Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Learn
Built-In Integrations:	Microsoft Project can be integrated with other Microsoft products like Office 365, SharePoint, and Microsoft Teams,

Category	Microsoft Project
	facilitating collaboration and communication among team members.
Optional Integrations/ Connections Requiring Configuration:	However, some Project integrations may require additional configuration or setup. • **Power BI:** Integration with Power BI requires some configuration. You will need to connect your Microsoft Project data to Power BI using the appropriate connector (Project Online connector for "Project for the web" and OData connector for Microsoft Project desktop). • **Power Automate**: Integration with Power Automate requires configuration. You will need to create custom workflows and automation using Power Automate's connectors and templates for Microsoft Project. • **Azure DevOps**: Integration with Azure DevOps requires additional configuration. • **Third-party tools**: Integrating third-party tools like Smartsheet, Wrike, Trello, and others typically requires additional configuration or setup.
Activity Logging - End-user controls:	In Microsoft Project, particularly the cloud-based "Project for the web" version, end-users have limited control over activity logging. Most of the logging settings are managed at the organization level, and administrators have more control over data collection and privacy settings.
User Activity Reports:	Microsoft Project does not have a specific built-in feature for user activity reporting; however, administrators can create custom reports using available data from Microsoft Project or by integrating with other Microsoft tools and services. Some common elements included in user activity reports are: • **Task completion**: Information about the tasks assigned to users, their progress, and completion status. • **Time tracking**: Data on the time spent by users on different tasks. • **Project updates**: Details of changes made to the project plan, tasks, or resources by users.

Category	Microsoft Project
	- **Collaboration**: Information about user interactions, such as comments, notes, or file sharing. - **Logins and usage**: Data about user logins, active sessions, and application usage.
Auditing:	Various user activities are logged and can be viewed in an audit report generated from the Microsoft 365 audit log. Some of the Project activities that are logged and can support audit reporting include: - project creation, modification, and deletion activities; - task creation, updates, and completion activities; - resource allocation and update activities; - timesheet related activities; - project permissions and access activities; and - collaboration and communication activities.
Security Compliance:	Relevant Microsoft compliance: - ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS). - SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance, demonstrating strong internal controls and security practices. - ISO/IEC 27018: Microsoft Project is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. - NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.
Privacy Safeguards:	Most privacy safeguards are implemented across the entire Microsoft 365 suite, however, there are a few privacy-related features and practices that are more specific to Microsoft Project:

Category	Microsoft Project
	• **Granular permission settings**: Microsoft Project provides a range of permission settings for projects, tasks, and resources. Administrators can define and manage roles, access levels, and permissions for users within a project, ensuring that sensitive information is accessible only to authorized users. • **Project site isolation**: When integrated with SharePoint, Microsoft Project allows you to create dedicated project sites for each project. This isolation helps ensure that project information is segregated, and access to one project does not inadvertently grant access to another project's data. • **Project data sharing controls**: Microsoft Project allows users to control how and with whom project data is shared. Users can choose to share project plans, files, and other information with specific team members, groups, or the entire organization, depending on the desired level of privacy. • **Task confidentiality**: Microsoft Project allows users to mark certain tasks as confidential. When a task is marked as confidential, it will not be visible to users who do not have the appropriate permissions to view confidential tasks. This feature helps protect sensitive information within a project plan.
Potential Privacy Risks:	While Microsoft Project has privacy safeguards in place, there are still some inherent privacy risks specific to the nature of project management and collaboration. These include: • **Sharing sensitive information**: Project plans often contain sensitive information, such as confidential project details, personal data, or intellectual property. Users may inadvertently share sensitive information with unauthorized users or external parties, leading to privacy risks. • **Overly permissive access control**: If access control settings are not configured correctly, users may have broader access to project data than intended. This can result in unauthorized access to sensitive project information.

Category	Microsoft Project
	• **Insecure integrations**: Microsoft Project allows integration with third-party applications and services. If not properly secured, these integrations can introduce privacy risks and potential data breaches. • **Human error:** Users may accidentally modify, delete, or disclose sensitive project data, leading to privacy risks.
Privacy Risk Mitigations:	Potential Microsoft Project privacy risk mitigations include: 1. **Sharing sensitive information**: • Implement a data classification policy to categorize and label sensitive information. • Provide training to users on handling sensitive data and sharing best practices. • Use built-in collaboration features, such as sharing with specific users or groups, to control access to sensitive data. 2. **Overly permissive access control**: • Regularly review and update user access permissions, roles, and groups to ensure they align with the principle of least privilege. • Establish clear guidelines and processes for granting and revoking access to project data. • Monitor user access and activities to detect unauthorized access or suspicious activities. 3. **Insecure integrations:** • Assess the security and privacy policies of third-party applications and services before integrating them with Microsoft Project. • Limit access to necessary data and permissions when configuring integrations. • Regularly review and update integrations to ensure they adhere to security best practices and meet privacy requirements. 4. **Human error**: • Provide regular training to users on data protection, privacy, and Microsoft Project best practices. • Establish clear guidelines on handling sensitive data within Microsoft Project.

Category	Microsoft Project
	- **Implement a robust incident response plan to address potential data breaches or privacy incidents.**
Other Key Links:	- https://learn.microsoft.com/en-us/office365/servicedescriptions/project-online-service-description/microsoft-project-online-service-description?source=recommendations - https://learn.microsoft.com/en-us/project-for-the-web/project-architecture-overview - https://learn.microsoft.com/en-us/project-for-the-web/turn-project-for-the-web-off - https://learn.microsoft.com/en-us/projectonline/change-permission-management-in-project-online - https://learn.microsoft.com/en-us/projectonline/project-online - https://support.microsoft.com/en-us/project - https://www.microsoft.com/en-us/microsoft-365/project/project-management-software

7.4 Microsoft To Do

Category	Microsoft To Do
Description:	Microsoft To Do is a task management application that helps users to organize and prioritize their daily tasks, to-dos, and lists. To use Microsoft To Do, users need to create an account using their Microsoft account or work/school account. Once logged in, users can create a new list or add tasks to an existing list. Each task can have a due date, a reminder, a priority level, and a note. Users can also add subtasks to a task, which can be checked off individually as they are completed. The interface of Microsoft To Do is simple and user-friendly, with a clean and customizable design. Users can customize the app's theme and rearrange their lists by dragging and dropping them in any order they want. The app also allows users to add images and files to their tasks, making it easy to keep all the relevant information in one place. One of the unique features of Microsoft To Do is the "My Day" feature. Each day, users are presented with a fresh list of tasks that they can choose to complete for that day. This feature helps users focus on their most important tasks and avoid feeling overwhelmed by a long list of to-dos.
Platforms:	It is available on multiple platforms, including Windows, iOS, Android, and the web.
Key Data Inputs:	Microsoft To Do collects certain types of data to provide its services to users including: • **Account Information**: Microsoft To Do collects information about a user's account, such as their name, email address, and password, to enable them to log in and use the app. • **Task and List Information**: The app collects data about the tasks and lists that users create and manage within the app, including the name of the task, the due date, notes, reminders, and priority levels.

Category	Microsoft To Do
	• **Usage and Performance Data**: Microsoft To Do collects data on how users interact with the app, including how often they use the app, how long they use it, and the features they use most frequently. The app also collects data on app crashes and errors to improve performance. • **Device and Network Information**: Microsoft To Do collects data about a user's device and network, such as the device type, operating system, IP address, and browser type. This data is used to diagnose technical issues and improve the app's performance. • **Location Data**: The app collects location data if a user chooses to enable location-based reminders for tasks. • **Feedback:** Microsoft To Do may also collect user feedback and surveys to improve the app's functionality and user experience.
Collection of Diagnostic Data:	Microsoft To Do collects diagnostic data to help diagnose and troubleshoot problems that may occur in the app., including: • **App usage and performance data:** This includes data on how users interact with the app, such as the frequency and duration of app usage, and data on the app's performance, such as app crashes and errors. • **Device and network data**: This includes data on the device type, operating system, IP address, and browser type, as well as network connectivity data. • **Error reporting data**: This includes data on errors that occur in the app, such as the error message, stack trace, and related app logs. • **App configuration data**: This includes data on the app's configuration settings, such as the app version, language settings, and feature settings. • **Feedback data**: This includes data on user feedback and error reports submitted through the app's feedback feature.
Collection of Customer Data:	Microsoft To Do collects customer data to provide its services to users, including: • **Account Information**: This includes the user's name, email address, and password, which are used to create and authenticate the user's account.

Category	Microsoft To Do
	• **Task and List Information**: This includes the tasks and lists that the user creates within the app, including the name of the task, the due date, notes, reminders, and priority levels. • **Usage and Performance Data**: This includes data on how users interact with the app, such as the frequency and duration of app usage, and data on the app's performance, such as app crashes and errors. • **Device and Network Information**: This includes data on the user's device and network, such as the device type, operating system, IP address, and browser type. • **Location Data:** This includes location data if a user chooses to enable location-based reminders for tasks. • **Feedback:** This includes user feedback and surveys submitted through the app's feedback feature.
Data Collected and/or Processed:	• **Customer data**: This refers to the data that users input or generate while using Microsoft To Do. It includes: a. Account data b. Task and To Do data c. Usage and performance data d. Device and network data e. Location data f. Support and feedback data • **Diagnostic data**: This refers to the data collected by Microsoft to improve the performance, reliability, and overall user experience of their products, including Microsoft To Do. The diagnostic data may include: a. App usage and performance data b. Device and network data c. Error reporting data d. App configuration data
Personal Information Collected:	Personal information that may be collected specifically by Microsoft To Do: • **Account information:** This includes the user's name, email address, and password, which are used to create and authenticate the user's account. • **Task and to-do information**: This includes the tasks and to-dos that the user creates within the app, including

Category	Microsoft To Do
	the name of the task, the due date, notes, reminders, and priority levels. This information could reveal personal or sensitive information about the suer's activities, preferences, and priorities. • **Usage and performance data**: This includes data on how users interact with the app, such as the frequency and duration of app usage, and data on the app's performance, such as app crashes and errors. • **Device and network information**: This includes data on the user's device and network, such as the device type, operating system, IP address, and browser type. • **Location data:** This includes location data if a user chooses to enable location-based reminders for tasks. • **Feedback:** This includes user feedback and surveys submitted through the app's feedback feature.
Customer Data Storage Location:	In Canada, Microsoft has two data center regions: • Canada Central: Located in Toronto, Ontario • Canada East: Located in Quebec City, Quebec Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Learn
Built-In Integrations:	Microsoft To Do is integrated with: • **Outlook:** Microsoft To Do is fully integrated with Outlook, which allows users to access their Outlook tasks directly from the app. Users can also create new tasks and to-dos in Microsoft To Do that will appear in their Outlook task list. • **SharePoint:** Microsoft To Do is integrated with SharePoint, which allows users to create and manage tasks related to SharePoint lists and documents. • **Microsoft Planner:** Microsoft To Do is integrated with Microsoft Planner, which allows users to create and manage Planner tasks within the To Do app. • **Microsoft Teams:** Microsoft To Do is integrated with Microsoft Teams, which allows users to access their tasks and to-dos from within the Teams app. Users can also create new tasks and to-dos directly from Teams.

Category	Microsoft To Do
	• **OneNote:** Microsoft To Do is integrated with OneNote, which allows users to create new tasks and to-dos directly from OneNote notes. • **Microsoft Forms**: Microsoft To Do is integrated with Microsoft Forms, which allows users to create tasks related to Forms surveys and quizzes.
Optional Integrations/ Connections Requiring Configuration:	Microsoft To Do can be integrated with Power Automate (formerly known as Microsoft Flow), which allows users to automate tasks and workflows between different apps and services.
Activity Logging - End-user controls:	Users can access their privacy settings in Microsoft To Do and adjust their preferences for diagnostic data and usage data sharing. Specifically, users can choose to turn off diagnostic data sharing, which will prevent the app from sending usage and performance data to Microsoft for analysis and improvement purposes.
User Activity Reports:	Microsoft To Do provides user activity reports can include the following elements: 1. **Task creation and completion**: The user activity report includes information on when tasks were created and completed, as well as who created and completed them. 2. **Task lists:** The report includes information on the task lists that were created, modified, or deleted by users. 3. **Task assignments**: The report includes information on who assigned tasks to other users and who received assignments. 4. **App usage**: The report includes information on when and how frequently users are accessing the app. 5. **User management**: The report includes information on when users are added or removed from the app and when their permissions are modified.
Auditing:	The type of To Do activities that are logged and can be used to populate To Do audit reports are the same as the activities that are included in user activity reports:

Category	Microsoft To Do
	- Task creation and completion: This includes information such as the task name, due date, notes, and priority levels. - Task lists: This includes information such as the name of the task list, who created it, and when it was last modified. - Task assignments: This includes information such as the name of the task, who assigned it, and who accepted or declined the assignment. - App usage: This includes information such as the date and time of app usage and the device used to access the app. - User management: This includes information such as the name of the user, who added or removed them, and when the change was made.
Security Compliance:	Relevant Microsoft compliance: - ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS). - SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance, demonstrating strong internal controls and security practices. - ISO/IEC 27018: Microsoft To Do is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. - NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.
Privacy Safeguards:	Microsoft has robust privacy safeguards that apply to all their Microsoft products and services. Privacy safeguards that are specific to Microsoft To Do include: - **User authentication:** Microsoft To Do requires users to sign in with a Microsoft account in order to access the

Category	Microsoft To Do
	app. This helps to ensure that only authorized users can access their to-do lists and tasks. • **Task privacy settings**: Microsoft To Do allows users to set privacy settings for individual tasks and lists. This means that users can choose to keep certain tasks or lists private and not share them with others. • **Limited data sharing**: Microsoft To Do limits the data it shares with third-party services and only shares data that is necessary to provide the service. For example, when users connect their Microsoft To Do account to Microsoft Planner or Microsoft Teams, only the necessary data is shared to allow the integration to function. • **User controls**: Microsoft To Do provides users with controls to manage their data and privacy preferences. Users can access their privacy settings within the app and choose whether or not to share diagnostic data and usage data with Microsoft.
Potential Privacy Risks:	Microsoft To Do is designed with privacy in mind and includes privacy safeguards, however, there are still potential privacy risks associated with the app, including: • **Task and list data**: While this risk is not specific to Microsoft To Do, the app's focus on task and list management means that the type of data being collected and stored is highly specific and personal. For example, users may create to-do lists for personal tasks or work-related projects that they may not want others to have access to. • **Personalization features**: Microsoft To Do includes features such as suggested tasks and smart lists that use user data to provide a personalized experience. While these features can be helpful, there is a risk that user data could be used for purposes other than personalization or could be shared with third-party services. • **User controls:** While Microsoft To Do provides users with controls to manage their data and privacy preferences, there is a risk that users may not fully understand these controls or may not be aware of the privacy risks associated with using the app.

Category	Microsoft To Do
Privacy Risk Mitigations:	Risk mitigations that can help to address the potential privacy risks associated with Microsoft To Do include: • **Task and list data**: To mitigate the risk of unauthorized access to task and list data, users can take steps such as using strong passwords and two-factor authentication to secure their account. Users can also consider keeping sensitive tasks and lists private, and only sharing them with trusted individuals. Additionally, users can regularly review their tasks and lists to ensure that they are still relevant and necessary and delete any that are no longer needed. • **Personalization features**: To mitigate the risk of personal data being used for purposes other than personalization or being shared with third-party services, users can review the privacy settings in the app and choose which features to enable or disable. For example, users can choose to turn off suggested tasks or smart lists if they are uncomfortable with the app using their data. Users can also review the third-party integrations that they have enabled and choose which data to share with these services. • **User controls:** To mitigate the risk of users inadvertently sharing more data than they intended, Microsoft To Do provides users with controls to manage their data and privacy preferences. Users can review the app's privacy settings and choose which data to share with Microsoft, as well as which features to enable or disable.
Other Key Links:	• https://learn.microsoft.com/en-us/connectors/todo/ • https://learn.microsoft.com/en-us/graph/api/resources/todo-overview?view=graph-rest-1.0&preserve-view=true • https://learn.microsoft.com/en-us/graph/todo-concept-overview • https://learn.microsoft.com/en-us/graph/todo-concept-overview#why-integrate-with-to-do • https://support.microsoft.com/en-us/todo • https://www.microsoft.com/en-us/microsoft-365/microsoft-to-do-list-app

Category	Microsoft To Do