Digital Workplace Maturity Model

The rapid evolution of Digital Workplace technologies has transformed the way organizations operate, collaborate, and deliver value to their employees, partners, and customers.

As businesses strive to remain competitive in an increasingly digital landscape, the adoption of these technologies becomes not just an option, but a strategic imperative. However, successful implementation requires more than just deploying tools—it demands a structured approach to ensure alignment with organizational goals, workforce readiness, and sustainable growth.

This maturity model roadmap provides a comprehensive framework to guide organizations through the stages of adopting Digital Workplace technologies, from initial exploration to full optimization.

By outlining key milestones, capabilities, and best practices, this roadmap empowers leaders to assess their current state, identify gaps, and chart a clear path toward a modern, efficient, and employee-centric digital work environment. Whether you're just beginning your journey or seeking to refine an established digital ecosystem, this model offers a phased, actionable strategy to drive transformation and unlock the full potential of the Digital Workplace.

Section 1: Maturity Model for Unified Communications Technologies

Unified Communications (UC) technologies, such as Microsoft Teams, are essential to the Digital Workplace, enabling seamless collaboration, streamlined workflows, and real-time connectivity across distributed teams. A maturity model for UC adoption offers organizations a structured framework to evaluate their current capabilities, set achievable goals, and progressively enhance their use of tools like Microsoft Teams.

This model defines five stages of maturity—Initial, Developing, Defined, Managed, and Optimized—each with distinct attributes, challenges, and opportunities. Below, we present these stages in a table format to guide organizations in assessing and advancing their UC maturity.

Stage	Description	Capabilities	Challenges	Goal
Initial (Ad Hoc Adoption)	Usage of Microsoft Teams is sporadic and unstructured, driven by individual employees or small teams experimenting with basic features. Little to no governance or training exists.	Basic messaging, ad hoc voice/video calls, minimal file collaboration.	Inconsistent usage, lack of awareness of full functionality, potential security risks due to unmanaged deployments.	Establish a foundation by identifying early adopters and use cases.

Developing (Emerging Structure)	The organization recognizes UC value and begins formalizing use. Teams is deployed more widely, with basic policies and training emerging, though integration remains limited.	Team channels for project collaboration, scheduled meetings, basic integration with email or calendars.	Siloed usage across teams, uneven adoption rates, reliance on legacy communication tools.	Build awareness, standardize basic usage, and encourage cross-departmental adoption.
Defined (Standardized Implementation)	Microsoft Teams becomes a core communication tool, standardized across the enterprise with clear policies, training, and integration with productivity tools (e.g., Microsoft 365).	Advanced features like persistent chat, breakout rooms, integration with third-party apps or telephony.	Scaling adoption to all employees, managing change resistance, ensuring consistent user experience.	Achieve enterprise-wide standardization and enhance collaboration efficiency.
Managed (Proactive Enhancement)	The organization optimizes its UC environment proactively, embedding Teams into	Real-time dashboards, automated workflows (e.g., Power Automate), robust telephony or	Balancing innovation with stability, addressing advanced security needs,	Leverage data and integrations to maximize ROI and workforce productivity.

	workflows with analytics driving improvements and advanced integrations enhancing functionality.	external collaboration features.	maintaining user engagement.	
Optimized (Strategic Leadership)	Teams is a strategic enabler of business outcomes, fully integrated into the Digital Workplace, supporting innovative practices and continuous improvement with a culture of digital fluency.	AI-driven features (e.g., meeting insights, Copilot), seamless cross-platform interoperability.	Sustaining momentum, adapting to emerging technologies, staying ahead of industry trends.	Drive competitive advantage through a future-ready, agile, and employee-centric UC environment.

This maturity model, structured as a table, provides a clear and concise progression path for adopting Unified Communications technologies like Microsoft Teams. Organizations can use it to transition from reactive, ad hoc usage to a strategic, optimized state. By identifying their current stage and targeting the next, leaders can prioritize investments, address gaps, and build a UC foundation that empowers their workforce and aligns with broader Digital Workplace objectives. In the next section, we will explore how to assess your organization's current maturity level and develop a tailored roadmap for advancement.

Section 2: Maturity Model for Collaboration Software

Collaboration software, such as Microsoft SharePoint, serves as a cornerstone of the Digital Workplace by facilitating document management, team collaboration, and knowledge sharing across organizations. A maturity model for adopting collaboration tools like SharePoint provides a structured framework to evaluate current capabilities, set strategic goals, and progressively enhance their implementation. This model outlines five stages of maturity—Initial, Developing, Defined, Managed, and Optimized—each with unique attributes, challenges, and opportunities. Below, we present these stages in a table format to guide organizations in assessing and advancing their collaboration software maturity.

Stage	Description	Capabilities	Challenges	Goal
Initial (Ad Hoc Adoption)	SharePoint usage is limited and unstructured, often initiated by individual teams or employees for basic file storage or sharing, with no formal strategy or governance in place.	Basic document storage, simple file sharing, minimal site creation.	Inconsistent adoption, lack of user training, potential duplication of content or poor version control.	Establish a baseline by identifying early use cases and user needs.
Developing (Emerging Structure)	The organization begins to recognize SharePoint's potential, with broader deployment for team-based	Team sites for document collaboration, basic metadata tagging,	Fragmented usage across teams, reliance on legacy file systems,	Promote adoption, standardize basic site usage, and develop

	document management and basic collaboration, supported by initial guidelines.	limited workflow automation.	limited awareness of advanced features.	initial governance policies.
Defined (Standardized Implementation)	SharePoint becomes a central collaboration platform, standardized across the organization with defined site structures, permissions, and integration with tools like Microsoft 365.	Document libraries with version control, custom lists, integration with Teams or Outlook for seamless access.	Scaling to enterprise-wide use, ensuring user compliance with policies, managing site sprawl.	Achieve consistent usage and improve knowledge sharing across departments.
Managed (Proactive Enhancement)	The organization actively optimizes SharePoint, leveraging analytics and advanced features to enhance collaboration, streamline processes, and ensure governance and security.	Advanced workflows (e.g., Power Automate), search optimization, intranet portals, and robust permissions management.	Balancing customization with maintenance, addressing user adoption gaps, ensuring data security.	Maximize efficiency and collaboration through data-driven improvements and integrations.

Optimized (Strategic Leadership)	SharePoint is fully embedded as a strategic collaboration hub, enabling a digital workplace with personalized experiences, AI-driven insights, and a culture of continuous improvement.	AI-powered content recommendations (e.g., Delve), enterprise-wide knowledge management, seamless hybrid work support.	Sustaining innovation, adapting to evolving business needs, maintaining a clutter-free environment.	Drive business value through a scalable, innovative, and user-centric collaboration ecosystem.

This maturity model, presented in table format, offers a clear progression path for adopting collaboration software like Microsoft SharePoint. It enables organizations to move from unstructured, ad hoc usage to a strategic, optimized state that enhances productivity and knowledge sharing. By assessing their current stage and targeting the next, leaders can prioritize investments, address gaps, and build a robust collaboration foundation aligned with Digital Workplace goals. In the next section, we will explore how to assess your organization's current maturity level for SharePoint and develop a tailored roadmap for advancement.

Section 3: Maturity Model for End User Computing

End User Computing (EUC) encompasses the devices, applications, and services that empower employees to perform their roles effectively within the Digital Workplace. This includes desktops, laptops, mobile devices, virtual desktops, and supporting infrastructure. A maturity model for EUC adoption provides organizations with a structured framework to evaluate their current state, establish goals, and progressively enhance their end-user experience. This model defines five stages of maturity—Initial, Developing, Defined, Managed, and Optimized—each with distinct attributes, challenges, and opportunities. Below, we present these stages in a table format to guide organizations in assessing and advancing their EUC maturity.

Stage	Description	Capabilities	Challenges	Goal
Initial (Ad Hoc Adoption)	EUC is unmanaged and reactive, with employees using a mix of personal and corporate devices and applications with minimal oversight or standardization.	Basic device access (e.g., laptops or desktops), limited IT support, ad hoc software installations.	Security vulnerabilities, inconsistent user experiences, lack of centralized control or policies.	Establish a foundation by identifying core device and application needs.
Developing (Emerging Structure)	The organization begins formalizing EUC, providing standardized devices and basic policies, though	Corporate-issued devices, basic endpoint management (e.g., MDM), standardized OS and core apps.	Inconsistent deployment, limited remote work support, reliance on manual IT processes.	Standardize device provisioning and establish basic security and support frameworks.

	support and scalability remain limited.			
Defined (Standardized Implementation)	EUC becomes a structured component of the Digital Workplace, with standardized devices, applications, and policies supporting a consistent user experience across the organization.	Virtual desktops (e.g., VDI), single sign-on (SSO), standardized software catalogs, remote access capabilities.	Scaling to diverse workforces, managing legacy systems, ensuring compliance with security standards.	Achieve enterprise-wide consistency and enable flexible, secure work environments.
Managed (Proactive Enhancement)	The organization proactively manages EUC, leveraging automation, analytics, and advanced tools to optimize performance, security, and user satisfaction.	Self-service app portals, zero-trust security models, automated patching, real-time device monitoring.	Balancing cost with innovation, addressing diverse user needs, maintaining high availability.	Enhance productivity and security through automation and data-driven insights.
Optimized (Strategic Leadership)	EUC is a strategic enabler, delivering a seamless, personalized, and future-ready end-user	AI-driven support (e.g., predictive maintenance), device-as-a-service	Sustaining innovation, adapting to emerging technologies, ensuring	Drive competitive advantage with a cutting-edge, user-centric, and

	experience that supports hybrid work and drives business outcomes.	(DaaS), fully integrated hybrid work solutions.	scalability and resilience.	agile EUC ecosystem.

This maturity model, structured in table format, provides a clear progression path for adopting End User Computing solutions. It enables organizations to transition from chaotic, ad hoc setups to a strategic, optimized state that enhances workforce productivity and flexibility. By assessing their current stage and targeting the next, leaders can prioritize investments, address gaps, and build an EUC foundation that aligns with broader Digital Workplace objectives. In the next section, we will explore how to assess your organization's current EUC maturity level and develop a tailored roadmap for advancement.

Section 4: Maturity Model for Desktop Application Management

Desktop Application Management (DAM) involves the processes, tools, and strategies used to deploy, update, and maintain software applications on end-user devices within the Digital Workplace. Effective DAM ensures that employees have access to the right tools at the right time while maintaining security and operational efficiency. A maturity model for DAM adoption provides organizations with a structured framework to evaluate their current capabilities, set goals, and progressively enhance their application management practices. This model outlines five stages of maturity—Initial, Developing, Defined, Managed, and Optimized—each with distinct attributes, challenges, and opportunities. Below, we present these stages in a table format to guide organizations in assessing and advancing their DAM maturity.

Stage	Description	Capabilities	Challenges	Goal
Initial (Ad Hoc Adoption)	DAM is unstructured, with applications installed manually by users or IT on an as-needed basis, lacking centralized control or policies.	Basic app installation (e.g., manual setups), inconsistent versioning, minimal license tracking.	Security risks from unapproved apps, version mismatches, inefficient support and troubleshooting.	Establish a baseline by identifying critical applications and user needs.
Developing (Emerging Structure)	The organization begins formalizing DAM, introducing basic tools and processes for app deployment and updates,	Centralized app deployment (e.g., via SCCM), basic update management, initial license monitoring.	Inconsistent application delivery, reliance on manual processes, limited visibility into usage.	Standardize app deployment and establish foundational governance and tracking mechanisms.

	though scalability and automation remain limited.			
Defined (Standardized Implementation)	DAM becomes a standardized process, with consistent app deployment, updates, and policies across the organization, supported by integrated tools and documentation.	Automated app packaging, standardized update schedules, integration with endpoint management systems.	Scaling to diverse app portfolios, managing legacy apps, ensuring compliance with licensing rules.	Achieve consistent app availability and streamline management across all devices.
Managed (Proactive Enhancement)	The organization proactively manages DAM, using automation, analytics, and advanced tools to optimize app performance, licensing, and user experience.	Self-service app catalogs, real-time usage analytics, automated license optimization, patch management.	Balancing customization with efficiency, addressing app compatibility issues, maintaining security.	Enhance efficiency and user satisfaction through automation and data-driven improvements.
Optimized (Strategic Leadership)	DAM is a strategic asset, delivering a seamless, secure, and future-ready application ecosystem that	AI-driven app recommendations, zero-touch deployment, full lifecycle management,	Sustaining innovation, adapting to new app paradigms (e.g., SaaS), ensuring scalability and resilience.	Drive business value with an agile, user-centric, and forward-looking app management system.

	supports productivity and aligns with business goals.	cloud-native app support.		

This maturity model, presented in table format, offers a clear progression path for adopting Desktop Application Management practices. It enables organizations to move from reactive, manual processes to a strategic, optimized state that ensures application reliability, security, and user satisfaction. By assessing their current stage and targeting the next, leaders can prioritize investments, address gaps, and build a DAM foundation that aligns with broader Digital Workplace objectives. In the next section, we will explore how to assess your organization’s current DAM maturity level and develop a tailored roadmap for advancement.

Section 5: Maturity Model for Endpoint Device Management

Endpoint Device Management (EDM) involves the administration, security, and maintenance of devices—such as desktops, laptops, tablets, and smartphones—that employees use within the Digital Workplace. Effective EDM ensures device reliability, security, and alignment with organizational needs, particularly in an era of hybrid work and diverse device ecosystems. A maturity model for EDM adoption provides a structured framework to evaluate current capabilities, define objectives, and progressively enhance device management practices. This model outlines five stages of maturity—Initial, Developing, Defined, Managed, and Optimized—each with distinct attributes, challenges, and opportunities. Below, we present these stages in a table format to guide organizations in assessing and advancing their EDM maturity.

Stage	Description	Capabilities	Challenges	Goal
Initial (Ad Hoc Adoption)	EDM is reactive and unstructured, with devices managed individually or manually, lacking centralized oversight or policies.	Basic device provisioning, manual configuration, minimal security measures (e.g., passwords).	Security vulnerabilities, inconsistent configurations, limited visibility into device status.	Establish a foundation by identifying key devices and basic management needs.
Developing (Emerging Structure)	The organization begins formalizing EDM, deploying basic tools for device management and introducing	Centralized device enrollment (e.g., via MDM), basic patch management, standard OS configurations.	Inconsistent policy enforcement, limited scalability, reliance on manual interventions.	Standardize device enrollment and establish baseline security and

	initial security and compliance policies.			management processes.
Defined (Standardized Implementation)	EDM becomes a standardized process, with consistent device management, security policies, and tools deployed across the organization to support diverse work environments.	Unified endpoint management (UEM), remote wipe/lock, automated OS updates, basic compliance reporting.	Scaling to a growing device fleet, managing BYOD complexities, ensuring cross-platform consistency.	Achieve enterprise-wide device consistency and enable secure, flexible work scenarios.
Managed (Proactive Enhancement)	The organization proactively manages endpoints, leveraging automation, analytics, and advanced security to optimize device performance and user experience.	Real-time device monitoring, zero-trust security, automated compliance enforcement, self-healing tools.	Balancing security with usability, addressing diverse device types, maintaining high availability.	Enhance device reliability and security through automation and proactive insights.
Optimized (Strategic Leadership)	EDM is a strategic enabler, delivering a seamless, secure, and future-ready device ecosystem that supports	AI-driven device optimization, predictive maintenance, fully integrated hybrid work support,	Sustaining innovation, adapting to emerging threats, ensuring scalability and resilience.	Drive business agility with a cutting-edge, user-centric, and adaptive EDM framework.

	productivity and adapts to evolving workplace demands.	device-as-a-service (DaaS).		

This maturity model, structured in table format, provides a clear progression path for adopting Endpoint Device Management practices. It enables organizations to transition from chaotic, manual device oversight to a strategic, optimized state that ensures security, scalability, and employee empowerment. By assessing their current stage and targeting the next, leaders can prioritize investments, address gaps, and build an EDM foundation that aligns with broader Digital Workplace objectives. In the next section, we will explore how to assess your organization's current EDM maturity level and develop a tailored roadmap for advancement.

Section 6: Maturity Model for Identity and Security in Digital Workplaces

Identity and Security form the backbone of a secure Digital Workplace, ensuring that users have appropriate access to resources while protecting sensitive data and systems from threats. This encompasses identity management, authentication, authorization, and security protocols. A maturity model for Identity and Security adoption provides organizations with a structured framework to evaluate their current practices, establish goals, and progressively strengthen their security posture. This model outlines five stages of maturity—Initial, Developing, Defined, Managed, and Optimized—each with distinct attributes, challenges, and opportunities. Below, we present these stages in a table format to guide organizations in assessing and advancing their Identity and Security maturity.

Stage	Description	Capabilities	Challenges	Goal
Initial (Ad Hoc Adoption)	Identity and Security practices are rudimentary and reactive, with basic passwords and minimal controls, often managed manually without a cohesive strategy.	Simple passwords, local user accounts, basic firewall or antivirus protection.	Weak authentication, inconsistent access controls, high vulnerability to breaches or insider threats.	Establish a baseline by identifying critical systems and basic security needs.

Developing (Emerging Structure)	The organization begins formalizing Identity and Security, introducing centralized identity tools and basic policies, though coverage and enforcement remain limited.	Single sign-on (SSO) for some apps, basic multi-factor authentication (MFA), centralized user directories (e.g., Active Directory).	Inconsistent MFA adoption, limited visibility into threats, reliance on legacy security tools.	Standardize identity management and implement foundational security controls.
Defined (Standardized Implementation)	Identity and Security become standardized, with consistent policies, advanced authentication, and integrated tools deployed to protect the Digital Workplace.	Enterprise-wide SSO, mandatory MFA, role-based access control (RBAC), basic threat detection (e.g., SIEM).	Scaling security to hybrid environments, managing complex user roles, ensuring regulatory compliance.	Achieve consistent access control and enhance threat detection across all systems.
Managed (Proactive Enhancement)	The organization proactively manages Identity and Security, leveraging automation, analytics, and advanced	Zero-trust architecture, real-time threat monitoring, automated provisioning/deprovisioning , advanced encryption.	Balancing security with user experience, addressing sophisticated attacks,	Strengthen resilience and compliance through proactive security and identity governance.

	frameworks like zero-trust to optimize protection and compliance.		maintaining audit readiness.	
Optimized (Strategic Leadership)	Identity and Security are strategic enablers, delivering a seamless, adaptive, and future-ready security ecosystem that supports business goals and mitigates emerging risks.	AI-driven threat prevention, passwordless authentication, continuous adaptive risk assessment, full integration with Digital Workplace tools.	Sustaining innovation, adapting to evolving threats, ensuring scalability across global operations.	Drive business trust and agility with a cutting-edge, user-centric, and resilient security framework.

This maturity model, presented in table format, offers a clear progression path for adopting Identity and Security practices in the Digital Workplace. It enables organizations to move from reactive, basic controls to a strategic, optimized state that ensures robust protection and seamless user access. By assessing their current stage and targeting the next, leaders can prioritize investments, address gaps, and build an Identity and Security foundation that aligns with broader Digital Workplace objectives. In the next section, we will explore how to assess your organization's current Identity and Security maturity level and develop a tailored roadmap for advancement.