# IT Roadmap (Preview)

This report has been tailored to provide up-to-date technical recommendations based on your current IT service capabilities and the future state you want to achieve.

January 15, 2018

## What is the IT Roadmap?

Microsoft IT Roadmap helps you assess your IT environment, services and configurations to help you get the most value from your Microsoft cloud and physical IT infrastructure. The model uses a 4-level scale, based on industry best practices spanning IT service delivery, security, compliance, productivity and more, where level 4 represents the highest level.

|  |  |
| --- | --- |
| The overall level on the right indicates the highest assessed level common across all prioritized IT services. It will change when all assessed IT services attain a higher level.  The summary below shows a selection of prioritized IT services in your organization. It identifies the functional capability of your current implementation along with a future state – represented by the green dashed outline – determined by the capabilities you plan to implement. |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |

### Shared services: identity, security & compliance

|  |  |  |  |
| --- | --- | --- | --- |
| Level 1 | Level 2 | Level 3 | Level 4 |
| Apps and services are siloed by design, and employees are responsible for maintaining their own tools to communicate with one another. | Apps and services are integrated between inhouse and cloud services, improving visibility into business-critical data, and standardized channels for employee communication. | Enhanced protection for accessing corporate apps and services, for both users and devices. All services and processes meet organizational standards of compliance. | System proactively blocks unusual activity and provides recommendations to improve compliance. |

### PC deployment & management services

|  |  |  |  |
| --- | --- | --- | --- |
| Level 1 | Level 2 | Level 3 | Level 4 |
| Tools and processes we use may limit our ability to deploy and manage modern desktops; we have a set of simplified processes, these are mostly manual. | We provide some level of management on all end user devices, though may not be able to manage all aspects of modern devices and applications users want; we have standard processes and light automation. | We can manage users' desktop and mobile devices; management tools and the level of management possible depends on device; standard processes are well-documented, many are automated. | We have a unified management platform through which to can manage all devices, regardless of location or user; most standard processes are automated. |

### Communications services

|  |  |  |  |
| --- | --- | --- | --- |
| Level 1 | Level 2 | Level 3 | Level 4 |
| Basic telephone, conference bridge, and email services are provided. Users may leverage their preferred messaging, social networking, video, and screen-sharing services for work. | We provide discrete services for online meetings, instant messaging, video chat, screen-sharing, and social networking. | Communication tools are integrated providing a seamless, connected experience across all chat, telephony, and meeting services. | Real-time collaboration capabilities are infused within our productivity apps. Meeting and video content is auto-captioned and translated into other languages in real-time. AI (bots) can be used to automate everyday tasks. |

### Meetings services

|  |  |  |  |
| --- | --- | --- | --- |
| Level 1 | Level 2 | Level 3 | Level 4 |
| Audio conference bridge available for employees to set up and dial into meetings. Presenters may make use of publicly available video/screen-sharing services to share content in real-time, or distribute content in advance. Participants may set up 1:1 and group backchannel conversations using Instant Messaging. | Enterprise-quality online meetings for secure audio and video, desktop and file sharing. Attendee availability is visible while scheduling meetings. Can view and present content from desktop and mobile devices. | Meetings and webcasts can be recorded for later viewing; participants can join at any time. Meeting room availability is visible and can be scheduled. | Meeting content is auto-captioned and translated in real-time, also enabling search of presented content. Meeting room equipment integrates for quick joining. AI analytics monitors attendee activity to rate meeting effectiveness. |

### Group collaboration services

|  |  |  |  |
| --- | --- | --- | --- |
| Level 1 | Level 2 | Level 3 | Level 4 |
| Email may block employees from opening or saving specific file types, but employees are held largely responsible for what information they share and how they share it. | Encrypt sensitive emails before sending or storing. Employees are trusted to share files responsibly. We provide shared locations on our network to store and access files for employees. | System helps educate employees of our compliance policies, when writing emails, authoring or storing content that may be accessed by others. As we build teams, the infrastructure is automatically provided to share and collaborate on content. | System provides proactive recommendations to protect sensitive information based on document templates and patterns (Ex: patents, tax forms, etc.). System will block access to corporate data from risky locations or devices. We can revoke access from externally shared secured content even if it has left our network. |

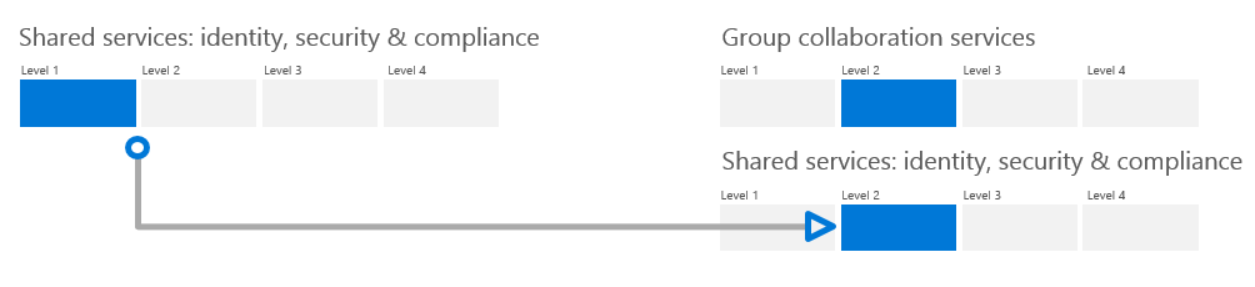
### IT change management services

|  |  |  |  |
| --- | --- | --- | --- |
| Level 1 | Level 2 | Level 3 | Level 4 |
| General resistance to technology change due to risk of business continuity. Most time is spent maintaining existing investments and responding to helpdesk requests. | IT can implement changes to meet business needs. There are standards and policies in place to maintain service levels and remain secure. | IT can respond to evolving business needs with robust change management process and tools. Budget and resources are planned in advance, ensuring business continuity. Users are informed and trained prior to changes that affect them. | IT is a strategic component for driving organizational direction via technology. IT service resourcing and costs vary dynamically based on business fluctuations. IT proactively seeks out better tools and processes for users. |

## Service dependencies

For some services, your IT implementation may already be at the level that most suits your current and future needs. For others, action needs to be taken to upgrade these services to meet your requirements. You can also designate capabilities as “Not applicable” when circumstances do not require the implementation of those capabilities.

The capabilities within “Shared services: identity, security and compliance” are prerequisite to most of the other IT services within the IT Roadmap. To advance levels within other services in the model, Shared services: identity, security and compliance must also be advanced.



## Information for IT implementers

The main section of this report provides implementers with a view of the current and planned objectives to support business-level discussions and a list of action items to move the capabilities of each service to their target state. Where the target level is more than one level away from a service’s present state—for example, where your current state is Level 2 and your planned future state is Level 4—the action items will include enabling the capabilities of intermediate levels. *(Note: In some cases, the model may currently indicate an action to implement a capability at a lower level that may be superseded by a higher-level capability).*

While a specific level may not yet have been attained, each action will add capabilities to an IT service, allowing your organization to benefit from the investment as use IT Roadmap to guide you to your planned future state. You can return to the IT Roadmap later and add services or track your progress.

## IT Roadmap navigation by audience

[Business View of prioritized services](#BusinessViewOfPrioritizedServices)

[Action Plan for Implementers](#ActionPlanForImplementers)

[Security considerations](#SecurityConsiderations)

[Next steps](#NextSteps)

## Related Resources for Business Stakeholders

IT Roadmap is part of the Business Value Programs at Microsoft. Business Value Programs allows you to explore your business scenarios and see what value you can get from Microsoft 365. You can take a customized test drive with one of the Business Value Programs at <https://transform.microsoft.com> or connect with your Microsoft Partner for more details.

# Business view of prioritized services

The following tables summarize the benefit of enabling the services to specific levels and highlights the state of the IT services you selected to work for this project. Items marked green are capabilities you have implemented. These also indicate progress towards full implementation of your selected future level.

The tables show:

* Current state (blue): the level you have currently attained.
* Future state (red/green indicators): capabilities you have selected to implement
* Other levels (grey): capabilities you have chosen not to implement at this time

Items marked red, indicate a capability is not yet enabled. Guidance on actions to take to achieve the desired future level you have selected are provided under [Action Plan for Implementers](#ActionPlanForImplementers), below.

# Security Considerations

The tables below highlight important security implications (benefits and issues) associated with the capabilities you plan to implement or have implemented. We recommend you review these as you assess your IT Roadmap and prioritize your action plan.

## Shared services: identity, security & compliance

### Access management

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Access to services are secured by a managed directory service or using disconnected cloud identities. Users working may seek unapproved/unmanaged services to get work done; data may reside in unmanaged services. * No SSO for non-managed solutions. Users will have to manage multiple sets of credentials; we have no control over password policy or expiration; users may reuse login details, so multiple accounts may be compromised in a single attack. | * Multi-factor authentication required for all admin accounts. Eliminates most risk from compromised administrative accounts; users accounts may still be compromised. * Cloud access management services are synchronized with on-premises directory services (where used). Control over password and access policies, mastered on-premises; where single-factor authentication is used, this is still susceptible to credential theft and phishing attacks. | * Multi-factor authentication is the norm for user access to organization's data and services. Eliminates most risk from compromised users accounts but there are still no checks on device and application health, or users attempting to access resources from unusual locations or networks. * Single sign-on access to SaaS applications and services from multiple vendors leveraging a unified access management platform. Consistent access security model enforced across all cloud-based software apps and services. * We have implemented MDM and can configure access conditions to require that devices connecting to services to comply with our minimum requirements. The system can assess device compliance for platform, minimum versioning, and location at the time of log in to determine whether that device can access managed services. | * Conditional access to resources varies based on user, device and location. Our services are proactively scanning access requests from browsers, other applications, devices and network locations, rejecting access requests for attempts that do not meet pre-defined policies. * System can control file transfer activity policies with other cloud apps and services, beyond the organization's cloud environment. Users activity is monitored, and can be controlled and logged. * System can require additional identity validation from users when unexpected/unusual activity is detected. Constantly scanning access and authentication requests, making a proactive assessment of risk; can require additional factors of authentication, redirect the user to a password reset sequence, or block access, on a case-by-case basis. * System monitors for unusual user activity and resource usage and sends alerts to resource administrators. Policies and thresholds in place; able to identify and take action when suspicious behavior is detected. |

### Identity management

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * More than one directory may be in use; no single 'source of truth'. Use of multiple directories can lead to misalignment of user and resource records, permissions and access; common risk occurs as users leave the organization or change roles, access to previous systems is not always removed. * User and directory information is primarily accessed by email; includes contact details and organizational information. N/A | Integrated identity and access management service for people across apps and services used. An integrated identity and access management system across apps and services also means that rights can be centrally-revoked as required when users leave as organization or if user accounts have been compromised.  Cloud identity management services are synchronized with on-premises directory services (where used). Control over password and access policies, mastered on-premises; where single-factor authentication is used, this is still susceptible to credential theft and phishing attacks. | Directory can be federated with partner directories. Federating partner directories reduces risk unsanctioned information is shared between users & external partners (shadow IT) & allows differentiated access policies for external users; eliminates need to manage user accounts for partner users.  Meeting rooms and equipment are managed resources within the directory. N/A | Productivity apps display presence, recent conversations, content, events, group affiliations, and other people-related data; information is filtered based on permissions. Pervasiveness of people-information makes it easier for your users to find shared content and connect with each other, without compromising security controls or access limitations placed on files or sites. |

### Governance

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Very little procedure or processes pertaining to governance, mitigation, and documentation. Lack of controls and visibility into processes and procedures creates high risk to the organization. * Reactionary and rudimentary reporting and investigation. Reactive reporting may be insufficient and inconsistent to satisfy governance requirements. | Established processes and enforced policies with a focus on containment. Governance policies reduce risk after an incident has been reported by focusing on containment, but does not proactively work to prevent incidents from happening.  Reporting is limited to a recurring set of standard reports and monitoring activities are routine, if formulaic. Reporting and monitoring is limited and focuses mainly on activity and service availability.  Established process for data backup and restore. To help with business continuity risk, IT has processes in place to back up and restore data for critical systems and centrally-managed services. | Systems and processes in place to protect personally identifiable information. Privacy policies and controls in place minimize the risk of losing user or customer data.  Automated reports provide insights into current security threats and detected activity targeting our environment. We have an dashboard that allows us to explore current security-related threats, any traffic to our organization, and mitigation that has already taken place.  All modes of digital communication can be archived and discoverable through organizational search. We can search and discover all text-based data stored in our information archives.  Disaster recovery of all productivity data and services. Our IT team and chosen service providers have implemented disaster recovery plans to ensure minimal data loss if anything happens to our IT infrastructure or data centers operated by our service providers.  IT extends the reach of security policies by utilizing cloud access security brokers for policy enforcement, including security, credential mapping, encryption, tokenization, alerting, etc. Risk is minimized by using standard policies for security and data protection across our cloud-based primary apps and services. | Continuous process and policy improvement is enabled by quantitative feedback from the system. Security tools proactively help increase level of information protection by scanning for sensitive information and recommending suitable policies to apply. |

### Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * No guarantee of compliance. High compliance risk. Non-compliant services may not have required controls in place to meet legal requirements for your industry or location, such as auditability, data retention and privacy policies. | Some services are compliant. Medium-to-high compliance risk. Mix of compliant and non-compliant services can result in incomplete views of information for organizational search, audit and eDiscovery.  User responsible for using compliant services where necessary. Users may not be aware of compliance requirements for your industry or location and may not know which services meet these requirements. | Services have required control set for IT or compliance personnel responsible, to define and implement policies specific to their org and industry. Medium compliance risk. Software and services can meet compliance requirements, but IT is required to stay up-to-date with regulations and enable corresponding services or users are required to categorize their information and sites.  Services comply with local requirements in countries and regions where offered, including General Data Protection Regulation (GDPR). Low-to-medium compliance risk. The service providers we use meet compliance requirements for our market, but IT needs to enable industry- or organization-specific policies to be compliant.  eDiscovery, organizational search available across all IT managed services. Our legal team can perform search, eDiscovery and in-place hold against data stored in our information system. | System able to recommend configurations organizations may need to meet compliance requirements, which include control to grant service providers and third parties access. System proactively helps reduce compliance risk by identifying and flagging data that is insufficently protected.  System evolves to support net-new compliance requirements. Low compliance risk. Our service providers continuously monitor changing laws and regulations to ensure the services we use continue to meet evolving compliance requirements.  eDiscovery, organizational search and retention extends to third-party services. Data from systems outside of email, files and intranet can be ingested into our system, then retained, audited and searched to provide a comprehensive views of digital activities.  Advanced eDiscovery, leveraging intelligence to prioritize large search results for relevant information. Our tools enable us to sort through thousands of emails, documents and other formats quickly to find relevant items when performing organizational search. |

## Group collaboration services

### Messaging

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Ability to block receipt of harmful attachments by file type or file name extension. Transport rules limit obvious risks by blocking file extensions known to deliver malware, such as MSI, EXE, CMD, AppleScript or other script files. * Auto-block messages from block list senders, spam, and junk mail. Spam and junk filters reduce risk from phishing attacks or other potential email exploits. * Email access on mobile devices is limited to enrolled devices Mobile devices have basic policy management like enforced PIN, device encryption and ability to remotely wipe a lost device. | Message encryption service enabled for secure storage of sensitive messages. All email content 'at rest' is encrypted, reducing risk of data loss from storage media.  Rights management enabled for users to restrict dissemination of message & attachments. Rights management or other encryption methods (e.g. S/MIME or PGP) prevent unauthorized viewing, responding or forwarding of sensitive information. | Data Loss Prevention implemented for known sensitive information types. Policies for data loss prevention help educate users to avoid unnecessary sharing of sensitive information - e.g. personal IDs, credit card information, financial information, etc.  Message and URL tracing enabled. At an individual message level, message and URL tracing helps investigate who has been afflected or is susceptible to further attack.  End-to-end monitoring of email-based threats, including message and URL tracing. Reporting of users who have seen a message or followed a link can help investigate root causes or prevent further spreading of malware. We can use the message trace logs to contain email-based threats from spreading. | Document fingerprinting and auto-classification allows system to learn to identify org-specific identify information to enhance Data Loss Prevention. This reduces risk of data loss further by enabling the system to discover sensitive information using pre-determined templates for documents, for exampple: design specifications, contracts, or patent applications.  Ability to protect email with dynamic blocking of malicious attachments and protect emails and productivity documents from opening unsafe URLs. Reduces risk of data loss and attack by assessing attachments in a protected sandbox or preventing users from accessing known bad websites. |

### File sharing

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Mix of on-premises file servers and/or cloud-based file hosting services, with folder access permissions. The security risk of file servers tends to be that people seek more flexible options than VPN to access files away from the office; cloud-based services at level 1 tend to be consumer-grade without IT/security visibility. * Users expected to act responsibly sharing files. In this case there are no technology controls to monitor and limit information sharing; your data security is in the hands of each user's best judgement. | Directory-enabled folders for local file sharing. AFile server Access Control Lists may be too rigid for users, with locations locked to individuals or defined security groups; the risk is that users fall back to using locations where others can easily access information or find a third party option.  System warns users of external sharing risks. The system reduces risk by flagging a user if they are sending information to people outside the organization (e.g. sharing files via email).  Files maintain change log and can be discovered via organizational search. The security benefit of centrally hosting files is that they can be searched at any time when needed; this is a contrast to when users store files on their local disks, making search more difficult.  Rights management extends to file sharing. Rights management can ensure a file is encrypted and can only be decrypted and viewed by a trusted recipient. | Intranet or Cloud-based solutions include governance determining who can share documents and with whom (specific partners or orgs). To limit risk of data loss allow/block lists can limit which content users can share, and with whom.  Audit log search by item or person to trace who has accessed files. As needed, file history provides a forensic path to investigate who has touched a file and when.  Team or group collaboration tools auto-provision locations for shared content. Permissions are consistent with other group experiences to help discourage defaulting to "shared with everyone" experiences.  Users are informed proactively that information they're working on contains potentially risky or sensitive data. To prevent data loss, the system can be instructed to find sensitive information while being authored or shared, and inform the user proactively. | Advanced security tools monitor for and alert on anomalous and suspicious activity. Reduces risk of data loss by flagging IT or security personnel when anomalous activity is detected - such as copying large numbers of files locally or logging in from a suspicious IP address.  System able to track document access and revoke rights -- even to previously downloaded or synced files. Rights management systems can provide time, user and geographical views into who has accessed files and, as needed, reduce risk by providing proactive methods of revoking rights after sharing has occurred. |

### Teamwork

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Group authored files are edited individually and manually merged. This poses significantly more risk than authoring against a single document; mutliple versions of a document and unprotected email sharing are risks to data getting into the wrong hands. | Team members work on a common set of files; check out/in process in place or technology limitation to prevent write access by more than one user at a time. While this is an improvement to multiple files getting merged, the limitation of one person editing the file at a time often leads to several people downloading documents to work offline, then adding changes later. | Tools and processes allow multiple editors on the same file; co-authoring on shared files is an expected and mainstream experience across multiple device types; messaging and enterprise social tools are integrated into the collaboration experience. The security benefit is that files do not need to be stored on local devices; contributors can each securely access the central doc, and so links not the files themselves; permissions can be controlled per user and all activity is auditable.  External contributors supported with controls for limiting access to individual files and/or specific locations. Security upside is workers can share at a single file level, so external collaborators cannot see other content at the folder, library or site level unless explicitly given that access.  Control over which cloud apps and services integrate with the collaboration experience. Organization-wide control of which external cloud apps and services users may include as part of their collaboration experience allows us to restrict use of 3rd party platforms we do not trust to host our data.  Ability to set organization communication standards, controlling use of giphy, smilies, stickers and memes, and users' ability to delete conversations. Preventing users from deleting conversations and limiting use of inappropriate animated images in context of chat reduces risk of breach in organization policy.  Users can define the groups and teams they work in. N/A | Collaborators can easily identify the online presence of others and spin up chat, voice, video, and ad hoc meetings. Integration between other tools should be secure and use standard secure authentication and session initiation protocols.  Productivity tools provide intelligent recommendations to improve written communication. N/A  Administrative control of groups and teams with management of who can create groups; ability to manage team expiration automatically by policy. N/A |

### Broad collaboration

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Groups find and use social tools of their choice; not known or not managed by IT. Security risk is that data is not managed by IT; BYO tools may lead to oversharing, or staff taking networks and sensitive information with them if they leave the organization. * Gathering ideas and feedback is ad hoc, collected via email and paper-based mechanisms. Risk factors include how information is collected, and secure disposal of paper-based media. * Collation and analysis manual. Risks can include how data is interpreted, entered and the consistency of how data is submitted. | Social solutions known to IT, deliver against defined SLAs. SLAs also include information protection and archiving as part of the service.  When gathering ideas and feedback, data collection is primarily digital. Risks for data loss is reduced, provided data is sent to a managed location or service; access and other governance controls need to be considered.  Inbound collection of data using visually personalized intranet and extranet surveys and feedback forms, with automated acknowledgement. Submission via forms and list interfaces ensure that data is captured in a consistent way; data access consistent with organizational policy.  Existing and new members can review past collaboration activity and conversations. Security considerations should be applied to access management. | Common backend file storage; full fidelity viewing/edit experience. Ensures files are in a managed location, searchable via organizational search and eDisocvery.  Controls for communication with external users and/or orgs. You can centrally manage access to social tools, including allowing or blocking users from defined domains.  Social solutions integrate with other collaboration software. Integration between other tools should be secure and use standard authentication protocols like OAuth.  Custom apps and workflows allow peer level review of inbound data and voting. Custom apps and workflow leverage modern authentication (usually Oauth); data access consistent with organizational policy.  Context sensitive automated responses. Service used to determine context and response must adhere to compliance standards.  Subscription-based real-time notifications for submissions. N/A | External contributors supported, with controls for limiting access to specific team or group conversations and shared content. External sharing and collaboration controls reduce the risk of oversharing information by authorizing only defined teams or groups to view or search information.  Data de-duplication and machine learning enables idea prioritization, sentiment evaluation and categorization. Service used to determine context, and response must adhere to compliance standards. |

## Communications services

### Messaging

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Basic email and/or messaging services provided. By of providing the email/messaging service you have visibility into message content stored on your servers or in your managed service. * Users / departments complement with unintegrated/semi-integrated BYO solutions. "Bring your own" solutions usually means that some portion of your data resides in a user-managed service without visibility to IT or security personnel. | Full complement of messaging services across user preferred modalities. In this case, your organization provides enough to discourage use of BYO solutions to help avoid data moving into unmanaged services.  User online status provided. This is helpful for security personnel when trying to quickly reach someone for issue management.  Most services are known to IT, deliver against defined SLAs and are auditable. N/A  Archiving of messages meets compliance requirements. Compliance and data governance requirements are enforced. | Services integrated, use common directories and single sign on. The common directory shared with social tools means you can leverage consistent identity and access management requirements across your all managed services.  Message and activity search available for each workload. This visibility is critical for eDiscovery and audit.  IM encryption. Often overlooked, encryption of instant messaging and related history helps protect information in transit and at rest. | Bots automate regularly used functions. Bots do need to be programmed in alignment with security and data access policies to avoid oversharing of sensitive content.  Relationship analytics provided to help best use time and maintain important relationship. N/A  Centralized eDiscovery across most data sources, incl. email, and document libraries, etc., including external resources (3rd party SaaS data ingestion). Allows you to search imported data from public social tools - like Twitter or Facebook - within your data governance systems to enable eDiscovery and organizational search. |

### Voice & video telephony

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * PSTN calling. Security risk is low, but information discovery and auditing is usually limited to inbound and outbound calls with call duration. * PBX functions for physical workspaces incl. call directories, holds, transfers, and voicemail. The primary security consideration is for protecting call logs and directory information. * Conference bridge capabilities. Security risk for simple call bridges is unintended meeting participants - these may be unannounced internal or external meeting participants. * Consumer-grade video & screen sharing services. Security risks include: sharing files and desktops too broadly; data displayed or shared not within managed services; and, lack of auditability of meeting participants for IT. | Commercial grade online meeting functionality. Online meetings have controls in place to monitor or limit to approved activities; all meetings are auditable, to see who has joined the meeting to prevent unauthorized access.  Secure voice & video calling, and desktop sharing. Access to meeting content is gated by attendee authentication, content is displayed over secure https channels and all attendee activity is logged.  Consumer-grade telephony software and services blocked or discouraged. The risks of not blocking or discouraging these services include data loss, lack of central management or auditing, and data oversharing. | Unified solution for PSTN, & PBX, conference calls, and online meetings from PCs/Macs, telephone and mobile devices. Unification improves consistency, auditability, and central discovery of meetings, calls and related instant messaging interactions.  Desk phones optional. N/A  Calls route to the users current device. N/A | Productivity and collaboration software integrates in-context calling with present/away/busy status. Security considerations are related primarily to indentity and access controls instrumented in apps, or the devices they run on.  Real time voice and caption translation available. Secuity considerations with broadcast meetings include logic for auto-publishing, access to live meetings, outputted videos or caption-based metadata, and content retirement processes. |

### Availability & presence

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Use of consumer-grade messaging tools may provide online user status. Use of consumer-grade messaging or social tools have several risks; chat is not centrally-managed or auditable, data resides in an unmanaged service and policies are not configurable. | On-premise or Cloud-based managed chat solution provides online status of users. Security benefits are that the service itself is known to IT, user identities and access can be managed, information can be archived. | Online presence tool indicates next available free time of people and resources (e.g. conference room). Security benefit here is limiting access to free busy information of people or resources only to authorized users.  Role Based Access Control (RBAC) permissions model to access calendars, meeting information, etc. Role-based access controls limit information access to intended personnel. | Meeting facilities (rooms/equipment) show free/busy availability locally, and offer 'meet now' function for ad hoc meetings. N/A |

### Enterprise social

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Users/departments use unintegrated BYO solutions. Security risk lies with information and access management lying outside of managed services; archive and audit capabilities may not exist. | Social solutions known to IT, deliver against defined SLAs, are auditable and managed. Security benefit in this case is that all memberships and conversations are typically archived by the provider and auditable, but related files and attachments may reside outside of typically managed locations.  Contents, docs and files shared by social tools may reside in disconnected locations, outside of standard content management systems. Yet another area for content storage, increases risk the data is not correctly managed (user deletion, backup policy, legal holds, etc.)  Tools to view/edit files may be tied to solution and insufficient/not full fidelity. Depending on how document previewers are implemented, the social service may leverage another service to render previews, thereby sharing data with that service provider. | Services integrated, use common directories and single sign on. The common directory shared with social tools means you can leverage consistent identity and access management requirements with your other services.  Integrates with other collaboration experiences. The integration with managed collaboration experiences helps ensure files are stored in managed locations.  Common backend file storage; full fidelity viewing/edit experience. The security benefit in this case is that all content - from conversations to uploaded files - is managed and auditable.  Controls for communication with external users and orgs. You can centrally manage access to social tools, including allowing or blocking users from defined domains. | Audit and eDiscovery tools are shared with email, related systems and external apps, including customer-facing social networks, etc. Allows you to search imported data from public social tools - like Twitter or Facebook - within your data governance systems to enable full eDiscovery and organizational search. |

## Meetings services

### Messaging

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Ad hoc IM. Instant messaging services are typically consumer grade; conversations cannot be audited by IT and may be open to public viewing. | Meeting software supports integrated, secure IM/chat. Meeting chat and IM channels are secure, with access limited to those invited to the meeting.  Backchannel messaging archived and auditable. Instant messaging during meeting can be archived and audited as needed, using organizational search. | Extensibility model in broadcast meetings allows synchronous enterprise social chat, online polling, attendee pulse, etc. Extensibility options leverage the same identity and access management controls of the meeting itself to limit data exposure risk; these optional services should be evaluated for how data collected during meetings is managed.  Communication controls can be used to place limits on files and links within IM and chat. Policy controls can prevent attaching files in instant messaging, or limit access and permissions to sensitive or restricted files.  Ability to control which custom cloud storage providers may be used to share files. Policy controls can prevent sharing of sensitive or restricted files via unapproved file sharing services. | Attendee messaging activity monitored and analyzed for attentiveness to rate meeting effectiveness. Meeting effectiveness is measured, in part, by evaluating multi-tasking happening during meetings; tools taking these measurements do so anonymously and are natively integrated with messaging systems. |

### File sharing

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Files shared prior to meeting or presentation/desktop sharing tools in parallel to voice conversation. If security controls are not in place to protect shared information in email or other file-sharing means, meetings can be a major vector for potential data leakage. | Ability to attach files for meetings. This method of attaching files can enable the meeting software to present uploaded files in context, eliminating the need for downloadable file attachments, with the potential even to prevent participants from downloading meeting content.  Participants can review and annotate presentation files at different rate to presenter. Files can be displayed with limited access and restricted download controls; as with sending files prior to a meeting, meeting participants can review slides ahead of them being presented.  Attendees and presenters can co-author files during online meetings. Central shared storage with per user permissions, helps eliminate the need to attach files via email or use anonymous file sharing services, where further distribution may be impossible to track.  Share desktop image and control with meeting participants. Desktop sharing helps protect data by reducing the need to send files to meeting participants; this is especially important when sharing sensitive content. | File uploads during meeting automatically go to org's common file sharing infrastructure. Collaborative sharing can integrate with content management systems, providing secure and auditable access to team members.  Attendee access to files persisted - unless access is revoked by file owners. Team collaboration software securely extends file permissions to team members in coversations and ad-hoc meetings, but not beyond those in the team. |

### Voice & video telephony

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * PSTN dial-up conference bridge capabilities. The risk with standing dial-in attendee and meeting codes is that unannounced participants can access audio meetings; this presents particular danger where ex-staff or guest speakers/attendees have credentials and timing of recurring meetings. * Consumer-grade video & screen sharing services. TThe risk with consumer grade video and screen sharing tools lies in greater potential for unwanted sharing or post-meeting discovery – through IT’s inability to search previous meetings or accidental publishing to consumer and open video platforms. | Commercial grade online meeting functionality. Standardized online meeting services add the ability to audit scheduled meetings, see who is participating via device or phone, and apply standard policy within the organization, and at group level, to control meeting access and activities.  One-click meeting join from any device without the need to input meeting IDs. Mobile meeting clients require a one-time persistent authentication, so subsequent meetings can be joined via single click; this should be paired with MDM or Mobile Application Management and multi-factor authentication.  Control for attendee and presenter roles; waiting area for admitting external attendees. Enterprise-grade online meeting tools allow meeting owners to view defined attendee types in a virtual lobby prior to granting them access; this ensures that content is not shared until those attendees are explicitly approved.  Secure voice & video calls, and desktop sharing. Channels for voice & video calls, and desktop sharing are kept secure by enforcing strict access controls; in-meeting chat is logged and encrypted at rest and policies can be used to control activities during a meeting.  Consumer-grade telephony software and services blocked or discouraged. Blocking via proxy, device policy, or communicated policy to users, ensures that controls for provided meeting tools are enforced and meetings can be audited in the future.  Ability to invoke ad hoc meetings via software. Integration between collaboration tools and productivity software helps reduce users' desire to "meet" using unsanctioned, self-sourced tools; this also helps ensure that meeting access, data protection and archiving requirements are met.  Can view desktop sharing from mobile devices, and present from mobile devices. While this is more a convenience to meeting participants and presenters, it helps to prevent users seek other ways to view or present content from mobile devices that may not meet security requirements. | Unified solution for PSTN, PBX, conference calls, and online meetings from PCs/Macs, telephone and mobile devices. A unified solution for PSTN and online meetings ensure that meetings are carried-out according to policies in place, and meeting activities and participants can be centrally logged and audited.  All broadcast meetings are recorded for later viewing; participants can join at any time; live rewind possible. Ensures staff have secure access to meetings content and directives when not able to join live, and to review/rewind as needed; allows direct access to critical, security-related, or other confidential information, ideally consumed from the source. | Video portal established; allows discovery of previous meetings users have permission to access. On-demand meeting availability for broadcast meetings helps ensure that the entire intended audience can securely view and take action on items presented during broadcast meetings.  Real time voice and caption translation available. Captioning ensures meeting content is accessible for hearing-impaired or multilingual audiences. |

### Availability & presence

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Personal calendaring using individual tools. Primary security risk from using personal calendaring is post-meeting audit and accountability of meeting owners and their activities; it may be impossible to track how many times employees have met external partners or customers. * Free/busy status may not be visible to others within the organization. Online status of employees is not only a convenience to users, it may impact the organizations' time to react to critical situations; if status is not visible, more time is needed to track people when issues require immediate attention. | Free/busy visible to colleagues. Free, busy, online and offline status can allow you to respond more quickly to security or related issues, by finding and communicating with available stakeholders.  Personal calendars can be shared and delegation rights can be assigned to others in the organization. Calendar sharing and delegation can reduce the amount of time spent arranging meeting times, which can lead to faster decision-making when required.  Team or group calendar overlays and ability to load multiple calendars. Similar to sharing calendars, calendar overlays for teams or groups helps drive greater collaboration and unified decision-making for planning or responding to situations.  External apps can make entries on users' calendars. While this is more of a convenience for users, the security implication to be aware of is how the extensibility protocols work, as some may give extended permissions to access email or contacts list content.  Access to meetings can be controlled and audited. Controls for policies around which groups or users in an organization can schedule external participants, which type of content can be shared, etc., can help enforce security and information protection policies. | Meetings rooms can be scheduled as resources. Resource accounts make it easier for users to assign space, but such accounts also allow you to treat an authenticated room differently to individuals, and reduce access to meeting content - for example: sharing content permissions to attendees.  Presence of attendees recorded. Attendee presence and RSVP status help in real-time when controlling who is in an online meeting, also after the meeting when auditing who participated; this may be helpful is determining the source of a data leak or other security breach. | Intelligent auto-detection within messaging systems suggest events and meetings to add to calendars. N/A  Meetings rooms' resources including conferencing and presentation facilities set up for immediate use. N/A |

### Broad Communication

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Unmanaged social tools may be in use in parallel to meetings. Sharing information in, what amount to, public forums carry obvious information protection concerns; often, even when consumer software offer invite-only areas, these can be discovered after-the-fact, or via accidental sharing. | Activity over managed social tools pre-post-and during meetings inform content and continue the conversation. Managed social platforms can enforce who has access to conversations that are occuring in parallel to a meetings, along with visibility into what is discussed. | Team collaboration solution allows colleagues to check free/busy status and create meetings from team or private chat. One of the best ways to follow or react in real-time to conversations happening around the meeting, is via secure social integration; this can allow for audience interaction for broadcast meetings ensuring that key messages are understood.  Enterprise social runs in context, alongside meetings. Real-time collaboration and ad-hoc meetings can be critical mechanisms to have in place when responding to security-related situations. |

## IT change management services

### Process

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Lack of resources limits proactive implementation of new capabilities and services. This has a significant impact on security, as systems often become outdated - either not patched or not designed for current and evolving threats. * Staff and skillset structured for maintaining current investments in assets and services; no formal workflows or repeatable processes for implementing change. The risk here is that IT doesn't have the time or resources to stay on top of evolving threats or the tools to detect and mitigate against them. | Processes in place to keep current investments in a vendor-supported state, including required security and quality updates. While it is critical that older systems continue to be supported for security updates, consider this a minimum requirement, as newer software and services are often fundamentally re-architected to address new threats to strengthen defenses.  Budget and headcount sufficient to respond to required changes. IT has the resources, time and skillset to make required security critical changes to existing systems; the risk is there they may not be the budget needed to migrate to more secure solutions.  Hands-off management of Cloud services, where possible. Leveraging cloud services will help ensure that security updates are applied, but responsibility to implement optional security controls may still rest with IT. | Repeatable processes in place, streamlined for efficient change management, allowing all systems to stay current. Benefit for security is that IT solutions have the most current security controls and architectural changes to address security challenges, and is able to respond quickly when needed.  Process in place to evaluate change in Cloud-services before change hits production users; adjustments may be made to configuration to suit requirements. This process would also be true as new security features and policies are rolled out to users, ensuring that the best balance of security and productivity can be met.  Able to plan ahead and allocate resources for future projects. IT planning is also assessing future projects to enhance security and protection levels in the organization.  IT has seat at the table for strategic planning of future business services or products. This extends to security, privacy and related considerations, as aspects to service and product roll-outs. | IT is a center of excellence for process and proactive change agent, looking for better ways to support the organization and its users. This discipline extends to security-related technologies and processes; the leadership position also helps ensure that future asks relevant to security are approved and implemented in a timely manner. |

### Automation

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Little to no automation. Without automation there is higher risk of human error, or delays in doing critical security and information protection work. * Users accounts, hardware, services and software are manually configured and deployed/retired; updates may be automatic if supported by the software. Manual IT is only as good as the process and accuracy of the teams performing the work; risks include delays in deploying software updates, deprovisioning accounts in a timely manner, etc. | For on-premises assets, automation supports discovery and authorization of software updates; changes to Cloud-services roll out automatically. For on-premise assets, IT the necessary tools, and needs the time and discipline to apply security critical updates; cloud services often apply these by default, evolving security capabilities in parallel, but IT may still need to configure them. | Segmentation of users by roles and responsibilities for pinpointed automation of available services and applications, maintaining configurations, and updating software and services. Role-based access controls in IT and beyond help limit the scope of what people can do, typically to the areas they understand most and are accountable for, thereby limiting the potential for automation-related mistakes.  Adding and removing user accounts fully automated, services enabled, devices assigned and configured. Identity lifecycle management and corresponding automation ensures that user permissions are granted and removed as people enter and leave the organization, or even teams within an organization.  Capacity requirements can be forecasted and services scaled accordingly. This level of automation helps mitigate risks by ensuring business continuity, and will translate to required security and compliance infrastructure, such as archiving services or backup. | Services scale up and scale down automatically to meet SLAs, based on real-time demand without allocating excess capacity in advance. Elastic scaling via automation helps business continuity; additional security impacts include planning for unexpected spikes due to outside attacks (e.g. DDoS) and the defined mitigation processes. |

### Training

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * User communications are reactive, via helpdesk; limited or no pro-active training. The risk here is that users are not aware of how to work and leverage software and services in a responsible way. | Communications and training limited to major changes; prioritized to reduce helpdesk activity. Risk remains that users are not aware of security and compliance nuances and risks to avoid when using IT services; training for major platform changes may require updated security training as it relates to new capabilities. | Planned communication and training developed to advise users of relevant new features and changes that impact current use. Training takes into consideration all new features rolling out, assesses training needs, and is inclusive of security and compliance considerations to be followed by the user. | Upcoming features and changes are evaluated and user training/communication tailored on a continual basis. Considerations around training and security impacts are proactive, and integrated as part of the feature evaluation and validation phases; adjustments to training effort and content are made during change evaluation.  Monitor usage reports post deployment to identify opportunities for further communication and training. Production rollouts are continuously monitored for usage and training opportunities; controls are also in place to detect and respond to anomalous activies with potential security impacts. |

## PC deployment & management services

### Device acquisition

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Inventory maintained with limited computer models to ensure predictable experiences and driver support. OEM drivers, firmware or pre-installed software assessed for security (e.g. Superfish); limited hardware models provided from on-hand inventory to ensure low maintenance image support. | Hardware purchased from a limited pre-defined standards catalog. OEM trusted to fulfill hardware orders on demand; risk of unwanted software on these systems is low.  Hardware is purchased as-needed. N/A  Hardware supplier installs base OS with domain join support. OEM or system builder provides uncustomized Windows Pro image, or applies our IT team's provided volume license Windows image. | Either the hardware vendor or user can supply a device capable of Azure Active Directory Join and MDM auto-enrollment. Any current version of Windows can be set up to provide user with secure access to our resources, and can have our security and configuration policies applied.  Hardware vendors supply Windows computers with Signature Edition PC images preinstalled. New PCs come with a clean Windows install and we don’t need to reimage or uninstall unwanted apps that may not meet our security requirements. | Using Windows AutoPilot deployment service, we work with our hardware providers to help ensure that when the new device comes online during Windows setup from any internet connection, it can be custom-configured for that user. Working with our hardware partners, we can input device information in advance of the devices coming online and once they connect to the Internet, our specified security and related configurations are automically applied. |

### Provisioning

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Computers are wiped and reloaded using standard image inclusive of productivity software and pre-installed applications. The security risk in this approach is with how often images are updated to include latest security and feature updates for both the operating system and apps; if images are updated monthly or image process forces immediate updates, risk is minimized. * Hardware supplier may provide a current or previous OS version for new hardware. This practice of downgrading operating systems will mean that the latest security and protection technologies are not available. * New OS is rolled-out as part of a computer hardware refresh project, using manual data backup and restore. Security risk is primarily with handling of the data from previous system, temporary storage location or the individual performing the procedure. * Standard apps are installed before computers are delivered to users, or users have permissions and are expected to install their own software. Users with local administrator accounts pose a security risk and are often more susceptible to installing software, including various forms of malware. | Devices reimaged, with user-state migration, using task sequence automation and role-based customization for applications and configurations. Security risk is primarily with handling of the data from previous system, temporary storage location or the individual performing the procedure.  New apps are either installed by users or pushed via systems management software, or policy. Software delivered via systems management infrastructure tends to be more secure and does not require that users have local admin privilege; allowing users to perform software installs opens up additional risk. | In cases where Windows is upgraded on existing hardware, we use in-place upgrades; any additional configurations after the upgrade are automated. Because device OS upgrades are more predictable and can happen more frequently, we can take advantage of the latest security technology.  In cases where a computer is replaced, we can automate both user state migration between computers, and apply required apps & configurations for that user. We have a secure process that transfers users data, so they do not rely on unsecure methods such as removeable media or open network shares.  All data on PCs and devices is destroyed before disposal or transfer to a new user. We have processes in place to ensure no data can be recovered from devices we recycle.  App distribution and device configuration tools leverage our online managed store from the OS vendor. We have tested and authorized all the apps we use; the store itself requires that apps have been reviewed before they can be published and made available. | Any computer with a current version of the OS can be automatically tailored to corporate standards with productivity software, user-specific apps, security policies and user settings without reimaging. New tools can provide flexibility so that any device signed into company resources can be managed and provisioned using MDM and cloud-based technologies, ensuring security updates and policies are applied.  User data and settings typically resides in the cloud (public or private), reducing the need for user state migration when we replace a user's computer. Central storage, either in the cloud or in an on-premises location, means that IT has control of data access, archiving, protection and discovery; this should be paired with strong authentication policies, encryption and ongoing file activity. Monitoring. |

### LOB apps

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Windows applications are primarily packaged and installed as .EXEs or .MSIs This may offer vectors for malware exploits through LOB apps that were designed without modern security considerations. | Windows applications are converted to the Universal Windows Platform for deployment and management via our organization's Microsoft Store for Business. As long as our staff, vendors and partners can access our Microsoft Store for Business, they will be able to receive security updates as needed.  Remote desktop and application technologies may be used to access standard applications. Desktop and remote app virtualization can separate data from the end user's computer or device, as well as prevent copy/paste; the primary risk is with maintaining usability and performance, as users may seek other tools and methods to do their work. | New LOB apps are targeted as Web Apps, behind secure authentication and are mobile responsive. Browser-accessed LOB apps can be secured using identity & access controls that meet our requirements; all other aspects of the app are architected for security and compliance.  Our new LOB apps are created as native Universal Windows Platform apps. UWP apps leverage Windows-integrated authentication for secure connectivity to backend services; apps need to be designed to meet security requirements if data is stored locally or in a connected service.  All LOB apps that connect to organizational data and resources, enforce modern identity and access management controls, such as MFA. Information accessed by our LOB apps is secure and protected by our identity and access controls, regardless of where, which user or which device is connecting. |

### Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * Basic tools to authorize and publish software updates. Software updating is usually limited to security critical updates from major software vendors. * Limited settings and policies managed via directory service. Directory-managed policies can enforce security configurations, including software settings and software installation. | Agent-based systems management tools in place for application provisioning and updating; these systems management tools may be non-current versions or no longer supported by vendor. Even slightly out-of-date configuration management tools can add risk - they may not support the security features of newer systems, or new classes of device inventory.  Software updates typically limited to critical security updates. This policy for software update management ensures that security-related fixes are in place in a timely manner. | Software always on a vendor-supported build of the OS and productivity software; feature updates are continuously validated and implemented. Out-of-date software may increase risk; an always up-to-date strategy, in addition to delivering new end user features, can also deliver intelligent security solutions and new ways to protect users (e.g. hyperlink verification in productivity apps).  Computers managed with current systems management tools, which may be integrated with MDM solutions. Integration between computer and device management tools helps ensure that all connected devices can comply with required security configurations.  Policies and settings can be enforced whether or not the device is domain-joined. In BYOD (Bring Your Own Device) environments, users may not want IT to "own" their personal device using domain join or enrollment; policies can now be enforced within applications, which access sensitive information.  Software update requirements can be enforced with or without systems management infrastructure. Where users don't connect to the networks or VPNs required for our systems management tools to deliver updates, new methods keep users' computers up-to-date over standard internet connectivity, ensuring required security updates are installed. Quickly.  Computers are connected to inventory and telemetry services to provide information needed to validate current state and upgrade readiness. Monitoring each device for its operating system level, what firmware and applications are installed, including which versions, and what software updates are applied, provides insights into device state and which may be vulnerable to threats. | Productivity software deployed to new and existing systems integrates with cloud-based services for a fully connected experience (e.g. co-authoring, file sync, presence, IM, data protection, protection against malicious links/attachments, etc.). Applications connected to cloud-based services benefit from protections not possible with static configurations or proxy-based services, particularly where change is constant - e.g. hyperlink safety; attached/embedded code; evolving data protection policy.  OS version, settings, policies, apps and files follow users with their organizational IDs, so users can quickly get up and running on almost any current device. With cloud-based identities you can ensure that required security apps, settings and policies are applied to any modern device with which an organizational user signs in.  Device policy, app deployment and update management is performed using cloud-based management tools. Devices only have to connect to the internet to ensure that devices maintain our configuration standards and apply security policies; users do not need to connect to our organization's network. |

### Protection

|  |  |  |  |
| --- | --- | --- | --- |
| **Current** Level 1 | Level 2 | Level 3 | Level 4 |
| * All managed computers have auto-updating antivirus software installed. This ensures users' computers are always current, with antivirus signature files to prevent known threats. | Computer hard drives are typically encrypted. Hard drive encryption helps ensure that if a computer is lost, stolen, or the device is sent off to repair, no one can access information on the drive without knowing original user's log in credentials, and logging in.  Attached USB or similar storage devices may require encryption. Similar to hard drive encryption, attached storage encryption means that if a storage device is lost or stolen, the information stored on that device cannot be accessed. | Computers protected against credential theft and unauthorized operating systems using virtualization-based security technology. Virtualization-based security goes beyond sandboxing; it abstracts key information into an environment entirely separate from the underlying operating system.  Endpoint detection and response system in place to detect, investigate and respond to advanced attacks against computers after a breach. EDR systems assist with investigation, response and containment for attacks in the post-breach phase. | PC/device management system authorizes which apps may access the organization's data, restricting actions like copy/paste to unauthorized apps; provides a secure way to store and control org data on users' devices, separate from users' personal data. App management tools allow you to define groups of apps permitted to share information, ensuring your information remains within authorized apps and services; can selectively delete sensitive org information from users’ PCs and devices, if required. |

# IT Roadmap for Implementers

With all the options available to run IT services, IT Roadmap for Microsoft 365 provides a new way to visualize and plan a broad, long term strategy or our organization. IT Roadmap help you build a tangible plan, tailored both to your current set of IT investments and your future goal, based on your priorities.

Use the IT Roadmap as a tool to translate your plans in the language of your stakeholders. The following sections of this report provide a detailed review of your current systems and provide a practical, actionable plan to bring the IT capabilities in-line with the levels your organization’s needs.

You have selected the following services for this IT Roadmap. You may add to IT services to this list at any time.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Prioritized IT Services | | Current Level | | Future Level |
| Shared services: identity, security & compliance | | 1 | | 1 |
| PC deployment & management services | | 1 | | 1 |
| Communications services | | 1 | | 1 |
| Meetings services | | 1 | | 1 |
| Group collaboration services | | 1 | | 1 |
| IT change management services | | 1 | | 1 |
| Remaining IT Services |  | |  | |
| Intranet & search services | |  | |  |
| Data analysis & workflow services | |  | |  |
| Planning & project management services | |  | |  |

Selecting the levels that best match your current capabilities and future needs, the underlying model generates an Action Plan comprising capabilities not yet implemented. This Action Plan provides links to technical guidance and when possible the controls themselves in the Office 365, Intune and Azure portals on how to upgrade your present IT services using Microsoft 365 products and services. Some actions are straightforward, may take only minutes to implement and have minimal impact on the way end users use the system; others may require substantial planning, across multiple teams and require substantial user education.

The plan advises on the effort to implement, and the impact on end users.

# Action Plan

The Action Plan highlights all of the capabilities that you want to implement as part of your IT Roadmap. It exposes the estimates of IT Effort, User Impact, and whether FastTrack services are offered to assist your implementation.

Key:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IT Effort |  |  | User Impact |  |
| Low | Simple – click a button |  | Low | No training required |
| Medium | Straightforward, but planning/ implementation effort require |  | Medium | Intuitive, users may require instructions |
| Medium/High | Significant effort required - single team involved |  | Medium/High | Some user education/FAQ required |
| High | Significant effort required - across multiple teams, and/or scripted deployment (No GUI available) |  | High | Proactive education required |

### In total we have identified 0 actions across all services. These are as follows:

## Engage with FastTrack

Microsoft FastTrack is a customer success service designed to help customers realize business value faster with the Microsoft Cloud. FastTrack provides customers, partners, and field users with a set of best practices, tools, resources, and experts committed to making the experience with the Microsoft Cloud a success. Go to <https://fasttrack.microsoft.com> or connect with your Microsoft Partner for more details.

# IT Roadmap next steps

You are currently working on six prioritized IT services. Additional IT services to consider adding to your IT Roadmap in the future include:

* Intranet & search services
* Data analysis & workflow services
* Planning & project management services

To help in this future planning, the following table highlights the benefit of targeting each service to a specific Level. Like the services already on the IT Roadmap, when you add these to the IT Roadmap, the model will guide you through how to translate these targets into an action plan to enable your IT services infrastructure to support the functionality you are targeting for your organization.

### Intranet & search services

|  |  |  |  |
| --- | --- | --- | --- |
| Level 1 | Level 2 | Level 3 | Level 4 |
| Information is primarily distributed through email or print, and employees are responsible for knowing where it is stored. Video content can be downloaded from our network or streamed from public services. | Information is managed on our intranet where teams can search and share, and even stream video content. It can be difficult to locate content unless explicitly tagged by owners. | Our intranet supports managing workflows, video portals, and other interactive content. We offer secure connections to our intranet to our partners and suppliers to access a subset of resources. Search results are more relevant and files don't always require explicit tagging. | As project teams are created, publishing resources and workflows are automatically generated. Authors have visibility into how people access their content to gauge effectiveness. Content is delivered to you proactively without searching, based on what's trending and important. |

### Data analysis & workflow services

|  |  |  |  |
| --- | --- | --- | --- |
| Level 1 | Level 2 | Level 3 | Level 4 |
| Reporting is manual. Report distribution typically by email, file shares, or print. | Reporting is centrally created and distributed. Reports are static and not easily modified. Formalized conditions in place to create custom reports. | Reporting is optimized for 'self-service' with custom pivots, visualizations, and dashboarding. Reporting dashboards can be accessed securely from mobile devices. | Artificial intelligence helps create data insights and automatically detect and report anomalies. |

### Planning & project management services

|  |  |  |  |
| --- | --- | --- | --- |
| Level 1 | Level 2 | Level 3 | Level 4 |
| Basic milestone-focused planning tied to task lists, email, spreadsheets, or consumer-grade tracking tools. Information and reporting can be shared out, but isn't integrated across other existing solutions. | Expanded resource management and assigned task tracking tied to simple project management tools, that are used to inform time spent against defined tasks. | Robust set of project management tools with cost and budget tracking, broken down at the task level. Processes include automated workflows, critical path analysis, dependency chains, and real-time data visualizations. | Centralized project management office with standardized policies, processes, and practices. Tools inform proactively against project, budget, and resource risks across the organization. |