



Clarity. Efficiency. Confidence.

eDiscovery and Information Governance in Office 365

Matthew F. Porter, Esq.
Solution Architect



Contact Information

Matthew F Porter, Esq.
Solution Architect

As a Solution Architect Matthew serves clients through the Western region, working with Epiq Sales, Client Services and Forensic professionals to bring together the right combination of technology, personnel and process to address each unique client project. Matthew has over 15 years of experience in the field of eDiscovery, as well as legal practice experience in fields including government contracts and biomedical industries. Matthew is a certified Relativity Expert, a Relativity Certified Sales Professional, and a Certified Brainspace Analyst.



Why a CLE on eDiscovery and Information Governance and in Office 365?

- **84%** growth in # of seats year-over-year
- **50k small businesses** adopt Office 365 every month
- **1 in every 4** Microsoft enterprise customers uses **Office 365**
- Office 365 is Microsoft's **fastest growing** commercial product ever
- Office 365 **eclipsed Salesforce.com** as the most widely used **cloud-based business application**
- Estimates are there are **155 million** Office 365 users



3

epiq

Why a CLE on eDiscovery and Information Governance and in Office 365?

The data being moved to Office 365 is:

- Among the most highly targeted and sought in discovery

It's an evidence repository



4

epiq

Why do organizations move to Office 365?



Cost

- Fixed predictable pricing of dollars per user for email, SharePoint, IM, collaboration, etc.
- Operational vs. Capital expense



Easier to deploy and manage

- Less infrastructure to integrate and manage

Allows IT to focus on more strategic engagement with business

- Email and file storage/sharing considered commodity services



Built to be deployed on multiple devices and available 24/7

- Mobile and cloud first! Microsoft's mantra

5

epiq

Dynamics introduced by moving to Office 365

New content types

- Planner
- Sway
- SharePoint specific content
- Voice mail preview

New storage locations

- OneDrive for Business
- Groups
- Teams
- Yammer

Change

- Persistent, continuous, and at high velocity
- **Lower bar to deployment**
- Heavy IT integration and configuration is handled by Microsoft
- Easier to deploy and consume features such as Instant Messaging, collaboration, Information Rights Management, etc.



6

epiq

OneDrive for Business

• What is it?

- Individual file storage tool that competes with DropBox, Box, GoogleDrive
- Potentially replace "My Documents" and home-share on file server
- Technically it's a SharePoint site
- Access via the web or local copy on user's device

• eDiscovery implications

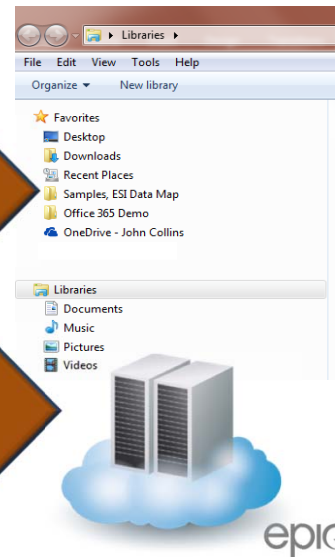
- ESI stored in OneDrive for Business is subject to eDiscovery tools
- ESI stored in OneDrive for Business is subject to Information Governance tools
- Centralized repository reduces need to collect from desktop, laptop, tablet

• FYI

- There is OneDrive for Business AND "OneDrive"
- OneDrive
 - Consumer oriented service
 - Provided with certain Office and Office 365 subscriptions

Work with files on local device...

...but your files are ALSO stored in the cloud

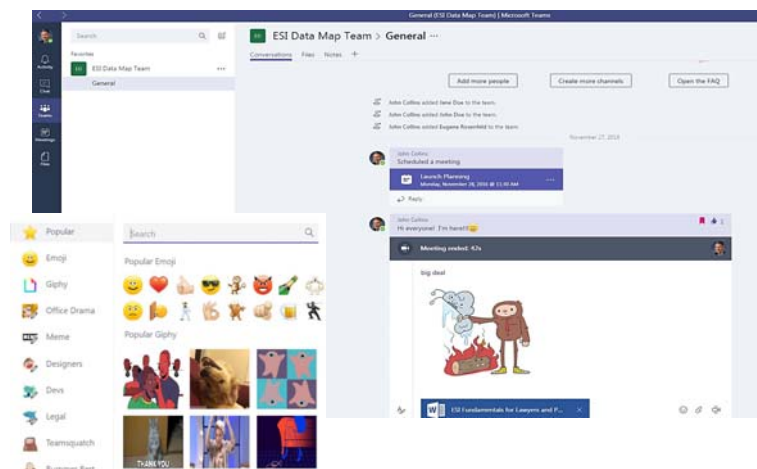


7

Teams

What is Teams?

- Microsoft's answer to Slack
- "Persistent" chat
- Meetings, files, notes
- Finally, the email killer?



8

epiq



What is Office 365?

What is Office 365?

- **Suite of Services/Products**

- E-mail, Instant Messaging, Collaboration, File Storage
- Office (Word, Excel, PowerPoint, Access, etc.), Exchange, SharePoint, Skype for Business



- **Cloud**

- Quintessential example of cloud computing
- Hardware, storage, backup and disaster recovery are handled by Microsoft



- **Software as a Service (SaaS)**

- Individuals, companies, organizations subscribe to the service for a fixed monthly or annual fee



Key elements of Office 365



11

epiq

epiq

How does Office 365 work?

How does Office 365 Work?

Office 365 Datacenters



Unlike many SaaS applications, Office 365 has a robust locally installed "client" software component: Office



14

What types of data may be found in Office 365?

What types of data may be found in Office 365?

- Exchange
 - Similar to “On Prem” Exchange
 - Additional considerations:
 - Site mailboxes (tied to SharePoint site)
 - Exchange Public Folders

Exchange Online

- Email
- Calendar
- Contacts
- Tasks
- Notes
- Journal
- Exchange Public Folders

15

epiq

What types of data may be found in Office 365?

- Teams
 - Calls and meetings
 - Calls and meetings can be recorded.
 - Voice and video
 - Replacing Skype for Business
 - Chat messages
 - File sharing and storage

Teams

- Instant Messaging
- Voice
- Online meetings
 - Video
 - Screen sharing
- Presence

16

epiq

What types of data may be found in Office 365?

- **SharePoint**

- **Collaboration**
 - Internal users
 - Internal users and external users
- **Custom Application Development**
 - Create a wide variety of applications to support business processes
- **Enterprise Content Management (ECM)**
 - Document and records management
 - Digital content management
- **File storage and sharing (OneDrive for Business)**
 - Replace file shares and “My Documents”

17

epiq

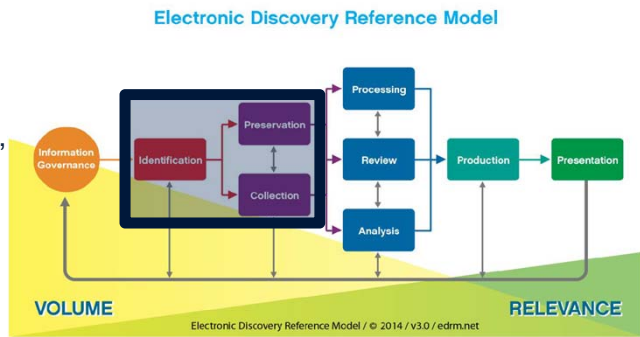
epiq

eDiscovery in Office 365

In a nutshell: eDiscovery Features in Office 365

“Standard” eDiscovery

1. Search across one or more mailboxes and SharePoint sites
2. Preserve Exchange/Outlook, SharePoint, and Skype for Business content
3. “Preview” preserved content
4. Collect and export Exchange/Outlook, SharePoint, and Skype for
5. Business content



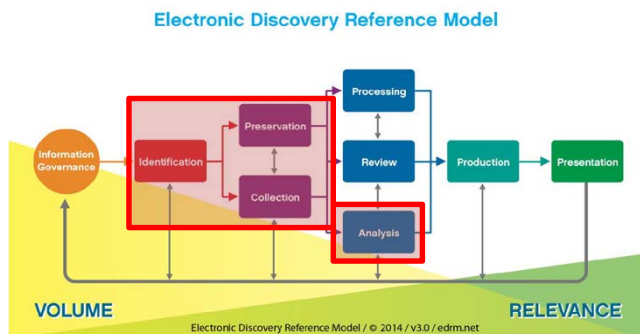
19

epiq

In a nutshell: eDiscovery Features in Office 365

“Advanced” eDiscovery

- Near-duplicate detection
- Thread analysis
- Predictive coding (“relevance”)
- Themes and Search



Defensibly reduce
the volume of ESI
sent outside the
organization's four
walls

20

epiq

Enabling defensible legal hold: Recoverable Items Folder

- Users can only access one level, “Deleted Items”

- eDiscovery tool can access much more:

- **Deletions**

- Contains all items deleted from the Deleted Items folder.
 - This folder is “seen” by end users via “Recover Deleted Items”

- **Versions**

- If hold in effect, contains original and modified copies of the deleted items

- **Purges**

- If hold OR SIR in effect contains all items that are “purged”

- **Audits**

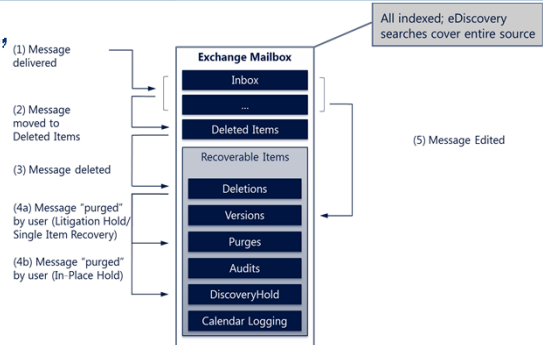
- If mailbox logging is enabled, contains mailbox audit entries

- **Discovery Holds**

- If “scoped” hold in effect this is where purged items go

- **Calendar Logging**

- Contains calendar changes that occur within a mailbox

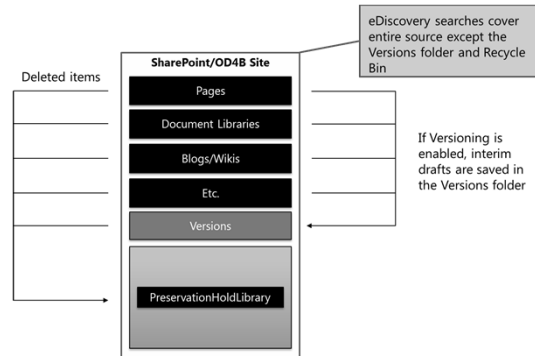


21



Enabling Defensible Legal Hold: Preservation Hold Library

- A “preservation hold library” is created the first time a SharePoint site is put under hold.
- Users can continue to work on content without disruption.
- Content on hold-including web pages, documents, lists, and other items are preserved as needed (if user edits an item it prompts preservation)
- Users don’t see the preservation hold library
- **To preserve all versions of content in a site, versioning must be enabled**



22



What DOESN'T Office 365 eDiscovery do “out-of-the-box?”

- **Legal hold notification and workflow**
 - Telling custodians they are on hold and tracking acknowledgements
 - Sending out questionnaires
 - Providing audit trail of when and who is on legal hold
- **Does not identify, preserve, or collect ESI located outside of Office 365- for example:**
 - Desktop, laptop, tablet computers
 - File (network) shares
 - Smartphones
- **“Full” eDiscovery processing***
- **Review**
- **Production**

25

epiq

epiq

Information Governance Features in Office 365

Information Governance features in Office 365

- **Retention & Disposition**

- In-Place Archive (Exchange)
- Document deletion policies (SharePoint)
- Information Management Policies (SharePoint)
- Messaging Records Management (MRM) (Exchange)
- Records Management (SharePoint Records Center) (SharePoint)
- Site Closure Policies (SharePoint)

- **Compliance**

- Preservation & Preservation Lock
- Supervisory Review

- **Information Security**

- Supervisory Review (Exchange)
- Data Loss Prevention (Exchange, SharePoint)
- Encryption (Exchange)
- Information Rights Management (IRM) (Exchange, SharePoint)



30



IG features in Office 365: Retention & Disposition

Retention & Disposition: Messaging Records Management (MRM) (Exchange)

- **Email management framework**
- **Employs a “tagging” paradigm**
- **Tags get applied to:**
 - Entire mailbox OR a folder OR an individual message/item
- **Multiple tags can be created, for example:**
 - 1 year (delete all items after one year)
 - 5 year (retain item or items in folder for 5 years)
 - Archive (move Inbox items to archive mailbox after 6 months)
- **Policies:**
 - Can aggregate tags into distinct policies (Executive Policy, VP Policy, Legal Dept. Policy, etc.)
- **Legal hold suspends deletion**

new tag applied automatically to entire mailbox (default)

*Name: DPT - Delete 7 Years

Retention action:

- Delete and Allow Recovery
- Permanently Delete
- Move to Archive

Retention period:

- Never
- When the item reaches the following age (in days): 2555

Comment: Delete all items after 7 years (2555 days)

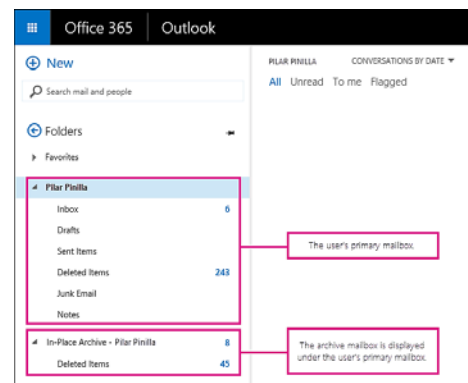
save cancel

29

epiq

Retention & Disposition: In-Place Archive (Exchange)

- **NOT the type of archiving associated with dedicated archiving tools such as Enterprise Vault, SourceOne, Legato, etc.**
- **Provides additional storage capacity for email**
- **Emails can be moved into the archive via several methods:**
 - Move or copy by user
 - Inbox rules
 - Retention policy
- **Key benefit is elimination of need for off-server storage (such as PST files)**

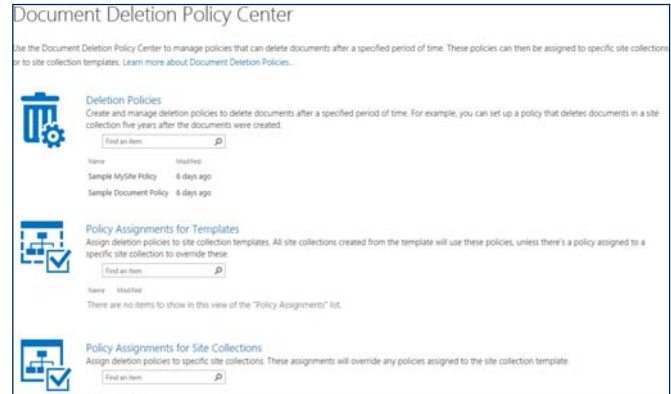


30

epiq

Retention & Disposition: Document Deletion Policies (SharePoint)

- **A policy framework for SharePoint**
 - Applies to site collections, sites, OneDrive for Business
- **Not a records management oriented approach**
 - Keep for X number of years then delete
- **Multiple policies depending on need:**
 - Policy for OneDrive for Business
 - Policy for internal team sites
 - Policy for extranets
- **Legal hold suspends deletion**

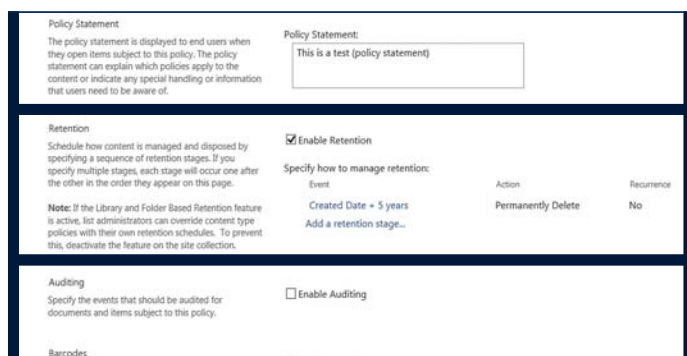


31

epiq

Retention & Disposition: Information Management Policies (SharePoint)

- **Framework for**
 - How long to retain files and content
 - Audit actions taken on files and content
- **Provides various options for what happens to files and content**
 - Delete
 - Start a workflow
 - Etc.
- **Implementation requires planning, training, careful thought**
 - Can apply policies at the site collection, site, or library level



32

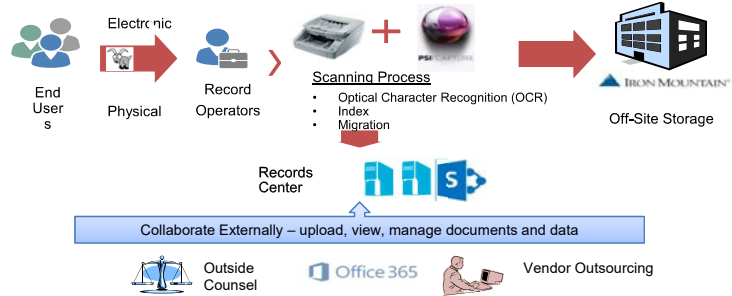
epiq

SharePoint Records Management

Out of the box, SharePoint provides a **framework** to implement records management

Three possible approaches:

- 1 "In-Place:" leave document in current location but declare it as a record
- 2 "Records Center:" documents are moved into a centralized repository within SharePoint and managed as records there
- 3 Hybrid



33

epiq

epiq

IG features in Office 365: Compliance

Compliance: Preservation & Preservation Lock

- **Preservation Policy**
 - Establish one or more policies
 - Based on date an item is created, sent/received
 - Policy can replicate journaling
 - Capture all messages regardless of end user actions
- **Preservation policy with preservation “lock”**
 - Can set the minimum length of time ESI retained
 - Cannot reduce the length of time
 - Can add MORE time

epiq

35

Supervisory Review (in “Preview”)

- **Email review for:**
 - SEC, FINRA, NASD email monitoring
 - Supports review and supervision of email correspondence with the public
- **Configuration options include:**
 - Select users to supervise
 - Create “lexicons”
 - Select % of communications to review
- **Supervisory Review client**
 - Mark items as compliant, non-compliant, further review
 - Add comments

36



IG features in Office 365: Information Security

IG features in Office 365: Data Loss Prevention (DLP)

- **DLP policies contain sets of conditions which filter messages and attachments**
- **DLP policies employ:**
 - Rules: for example, if a sequence of numbers such as 123-12-1234 appear
 - Actions: if 123-12-1234 appears, do not send the message
 - Exceptions: its ok to send the message if the sender is John Doe
- **Target PII, PHI, credit card numbers, social security numbers, drivers license numbers, etc.**
- **Use out of the box templates, create custom rules, or import rules created by 3rd parties**

PII Policy 12

general rules

Description:
Helps detect the presence of information commonly considered to be personally identifiable information (PII) in the United States, including information like social security numbers or driver's license numbers. Use of this policy does not ensure compliance with any regulation. After your testing is complete, make the necessary configuration changes in

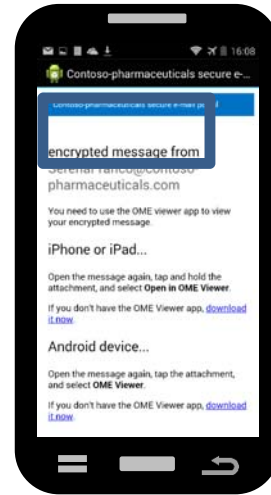
Choose the state of this DLP policy:
 Enabled
 Disabled

Choose a mode for the requirements in this DLP policy:
 Enforce
 Test DLP policy with Policy Tips
 Test DLP policy without Policy Tips



IG features in Office 365: Encryption

- **Multiple options available to implement a program to encrypt sensitive information in email**
- **Office Message Encryption (OME)**
 - Works with internal and external recipients
 - No special software required by recipients (don't have to be on Office 365)
- **Secure/Multipurpose Internet Mail Extensions (S/MIME)**
 - Uses certificates in a private-public key framework
 - Includes digital signature



epiq

39

IG features in Office 365: Information Rights Management (IRM)

- **Encrypts files and limits programs and users who are allowed to decrypt**
- **Limits what users can do:**
 - Email: who can access, forward, print, or copy sensitive data
 - SharePoint: limit actions users can take on files such as read-only (can't edit), copying and printing
- **Can be configured to be in effect for set period of time (expiration)**
- **Email rules:**
 - Can configure rules to apply IRM to certain messages (for example, messages containing word "confidential")

Information Rights Management (IRM)

IRM helps protect sensitive files from being misused or distributed without permission once they have been downloaded from this library.

Restrict permissions on this library on download

Create a permission policy title

Confidential Company Information

Add a permission policy description:

Documents and files classified as confidential (should not be shared outside company w/out NDA)

HIDE OPTIONS

Set additional IRM library settings

This section provides additional settings that control the library behavior.

Do not allow users to upload documents that do not support IRM

Stop restricting access to the library at

10/31/2015

Prevent opening documents in the browser for this Document Library

Configure document access rights

This section control the document access rights (for viewers) after the document is downloaded from the library; read only viewing right is the default. Granting the rights below is reducing the bar for accessing the content by unauthorized users.

Allow viewers to print

Allow viewers to run script and screen reader to function on downloaded documents

Allow viewers to write on a copy of the downloaded document

After download, document access rights will expire after these number of days (1-365) 90

epiq

40



Resources

Confidential—Not For Distribution

Resources for eDiscovery and IG in Office 365

**Moving
Target**

Office 365 admin

- Overview
- Setup and install
- Manage Office 365
- Users, passwords, and groups
- Troubleshoot
- Enterprise admin resources
 - Security & Compliance**
 - Overview
 - Security & Compliance Center
 - Alerts
 - Permissions
 - Security policies
 - Mobile devices
 - Data management
 - Search & investigation
 - Auditing
 - eDiscovery
 - Billing
 - Contact support

Security and Compliance in Office 365 for business - Admin Help

Applies To: Office 365 Admin

If your business has legal, regulatory, and technical standards to meet for content security and data use, you're in the right place. You can also use Office 365 security and compliance features if your business has specific security requirements for controlling sensitive information. In this section, you can also find out how Office 365 uses encryption and other security technologies to protect your data.

Top security and compliance tasks for Office 365 admins

- Import data to Office 365 to help address compliance requirements
- Read an Overview or Go to the Security & Compliance Center
- Search the Office 365 audit log
- Learn about Encryption in Office 365

- > Admin tasks for the Office 365 Security & Compliance Center
- > Import data to Office 365
- > Audit admin and user activities in Office 365
- > Manage mobile devices that access Office 365
- > Protect sensitive information using Data loss prevention
- > More security content for Admins
- > For Enterprises: Protect corporate assets



<https://support.office.com/en-us/article/Security-and-Compliance-in-Office-365-for-business-Admin-Help-7fe448f7-49bd-4d3e-919d-0a6d1cf675bb?ui=en-US&rs=en-US&ad=US>



Resources for eDiscovery and IG in Office 365

Moving Target

- Technet Library
- Office Products
- Office 365 for administrators
- Office 365 Security and Compliance**
- Office 365 Compliance Center
- Import PST files to Office 365
- Anti-spam and anti-malware protection
- Archiving
- Auditing
- eDiscovery
- Encryption
- Hold
- Information management policies
- Information Rights Management
- Legacy Exchange Hosted Services
- Exchange ActiveSync policies for managing devices
- Transport rules
- Use Office 365 tools for security investigations

Office 365 security and compliance

26 out of 44 rated this helpful - Rate this topic

Applies to: Office 365 Enterprise, Office 365 Midsize Business

Topic Last Modified: 2015-10-23

Microsoft Office 365 is designed to help meet your organization's needs for content security and data usage compliance with legal, regulatory, and technical standards. Setting up policies and enabling services that optimize these conditions is an important part of administering Office 365. To establish a secure and compliant Office 365 work environment that meets your organization's requirements, you may want to learn more about the staples of security and compliance described in this topic.

The following table describes the Office 365 features that are available to help you with fulfill your organization's security and compliance needs.

Feature	Description
Office 365 Compliance Center	You can use the Office 365 Compliance Center to manage compliance across Office 365, Exchange Online, and SharePoint Online. You can manage archive mailboxes, eDiscovery cases, auditing reports, and retention and deletion policies in Exchange Online and SharePoint Online. You can also assign permissions to compliance managers in your organization so they can access some or all of compliance features in the Compliance Center.
Import PST files to Office 365	Use the Office 365 Import Service to import PST files to Exchange Online mailboxes or import data files to your SharePoint Online organization. For both types of files, you can upload the files over the network or copy them to a hard drive and then ship the drive to a Microsoft datacenter, where the data will be imported to Office 365.
Anti-spam and anti-malware protection in	Office 365 has built-in malware and spam filtering capabilities that help protect inbound and outbound email messages from malicious software and help protect you from spam. You don't need to set up or maintain the filtering technologies, which are



<https://technet.microsoft.com/en-us/library/dn532171.aspx>

43

epiq

Keeping up with Office 365

ANNOUNCEMENT: The Success Center has moved to fasttrack.microsoft.com. Success.office.com will be retired on November 1st, 2015. Visit fasttrack.microsoft.com to get started.

Office 365 Customer Success Center

Home Scenarios Deployment Adoption Roadmap Community Resources

Office 365 Roadmap

The Office 365 Roadmap lists updates that are currently planned for applicable subscribers. Updates are at various stages from being in development to rolling-out to customers to being generally available for applicable customers world-wide.

[Release Programs Guide](#)

[Service Updates FAQ](#)



Launched (1) Fully released updates that are now generally available for applicable customers

EXPAND ALL COLLAPSE ALL

- Public Folder eDiscovery & In-Place Hold

Rolling out (0) Updates that are beginning to roll-out and are not yet available to all applicable customers

In development (4) Updates that are currently in development and testing

EXPAND ALL COLLAPSE ALL

- eDiscovery Export De-duplication
- eDiscovery Export Reports
- eDiscovery Infix & Suffix Wildcards
- eDiscovery Multi-Query Export

Cancelled (0) Previously planned updates that are no longer being developed or are indefinitely delayed

Previously released (6) Generally available updates for all applicable customers

EXPAND ALL COLLAPSE ALL

- Analyze Office 365 data with Equivio Zoom

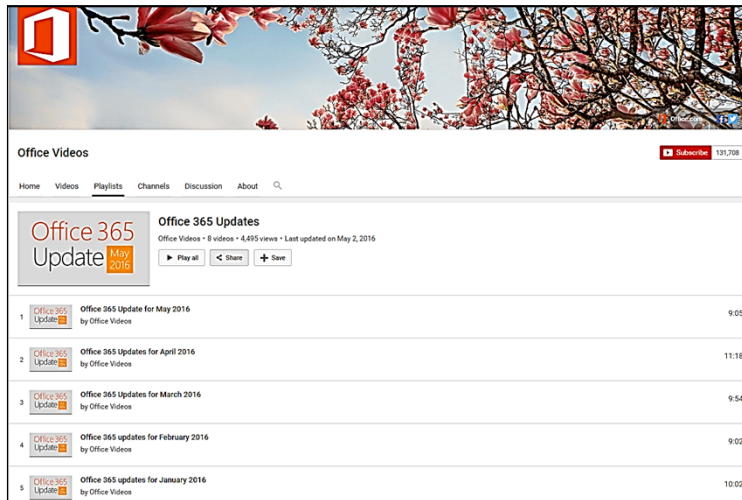


<http://fasttrack.microsoft.com/roadmap>

44

epiq

Keeping up with Office 365



<https://www.youtube.com/playlist?list=PLXPr7gfUMmKwn422HmCx7b7D5qh9T6frb>

45



Epiq O365 Services

- **Deep Dive** **FREE!**
 - Detailed review of eDiscovery and IG features
- **Workshop**
 - Review of current processes and procedures
 - Training/deep dive on native tools
 - Roadmap and strategy for O365 integration and adoption
- **Assessment**
- **Training**
- **Implementation**
- **Defensible Deletion of ESI before migration**
- **Email archive migration**



46