Office 365
GOVERNANCE
AGENDA

1. INTRODUCTIONS
2. GOVERNANCE APPROACH
3. SHAREPOINT RELATED SERVICES
4. QUESTIONS & ANSWERS
Presenter
Cory Williams
Business Productivity Practice Manager
SharePoint since 2003
Office 365 since 2010
cwilliams@cardinalsolutions.com
@corywilliams59

Charlotte Area SharePoint User Group Leader | @caspug
Cardinal provides creative technology solutions that transform client visions into compelling business and customer experiences.
GOVERNANCE APPROACH
Office 365 is updated frequently enough that clear understanding is required and each of the elements below could have a big impact on how your organization adopts and implements the various services.
Governance Committee

Guides the approach for what is and is not allowed.
- Should meet at least bi-monthly due to the frequent changes in Office 365.
- Include key representatives from multiple lines of business (HR, Legal, Compliance, IT, Regulated Business, Internal Communications)
Balancing Governance

Too much governance can stifle collaboration. Determining a good balance of policies and automation that still allow for active collaboration is the goal.
SHAREPOINT RELATED SERVICES
365 SERVICES LEVERAGING SHAREPOINT

SharePoint
Yammer
365 Video
Groups
PowerApps
Planner
OneDrive
Flow
Teams
Delve

All Services use SharePoint Storage Allocation

Data Loss Prevention (DLP)
Rights Management Services (RMS /IRM)
Azure Information Protection
Device Management (MDM)
SharePoint Online brings much of the same considerations you have for SharePoint On-premise except without the need to be concerned about hardware or your own server-side code.
SharePoint Hybrid enables an on-premise version of SharePoint 2016 to seamlessly integrate with SharePoint Online for some workloads.
OneDrive for Business is integrated with a lot of the Office 365 services including Exchange & Teams. While it is meant specifically for storing personal files, a lot of sharing still occurs from these locations which can bring its own challenges.

1. Boundaries & Limitations
2. User Management (Delegation/Secondary Admin)
3. External Sharing
4. Policies / Conditional Access
5. Sync & Quotas
Office 365 Video brings a YouTube style experience to an organization. Video does bring some of its own challenges but is great for many use cases from training to onboarding to events.

1. Boundaries & Limitations
2. Management Controls
3. Integration Points
4. Impact to SharePoint

SharePoint Site Collection
New Channel
Office 365 Groups is a mash-up of various Office 365 services and also supports Planner and Teams.
Planner is a tool designed for basic task management. Its great for teams that may have multiple projects in flight as it provides rollups for team members with an easy to use interface. It also has a couple of dependencies on other services.

1. **Boundaries & Limitations**

2. **Management Controls**

- New Plan
- Group Mailbox (Distribution List)
- SharePoint Site Collection
Teams is Microsoft’s persistent chat tool that combines multiple services to create an experience that brings teams together. The combination of services includes Groups, Skype, SharePoint, PowerBI, Office Online, & Planner.
Yammer is an Enterprise Social tool. Yammer allows consists of mostly public groups that are easily discoverable to enhance collaboration by opening up conversation to a wider audience.
Delve consists of two different components. The first is Delve Profiles which replaces a SharePoint My Site Profile. The second is that it surfaces up content via signals from SharePoint, Outlook, OneDrive, Office 365 Video, and Groups.

1. Management Controls
2. Integration Points
PowerApps is an application building tool for building both browser based apps and mobile based application. The tool reached GA a couple of months ago and is automatically included in Office 365 services.

1. Boundaries and Limitations
2. Management Controls
3. Environments
4. Connections
Microsoft Flow is a workflow based tool for building processes that can interact with multiple systems. The tool reached GA a couple of months ago and is automatically included in Office 365 services.
Security Capabilities

- Data Loss Prevention (DLP)
- Rights Management Services (RMS / IRM)
- Retention
- Azure Information Protection
- Device Management
- Auditing
- eDiscovery
- Secure Score

https://protection.office.com/
Data Loss Prevention provides the ability to leverage pre-built or custom policies to protect sensitive data.

**Examples of pre-built policies**
- U.S. Patriot Act
- U.S. Personally Identifiable Information (PII) Data
- U.S. State Breach Notification Laws
- U.S. State Social Security Number Confidentiality Laws
- PCI Data Security Standard (PCI DSS)
- U.S. Federal Trade Commission (FTC) Consumer Rules
- U.S. Financial Data
- U.S. Gramm-Leach-Bliley Act (GLBA)
- U.S. Health Insurance Act (HIPAA)

**Custom Actions**
- Choose where policy should apply (All or specific)
- Conditions
- Actions (Block content and/or Send notification)
- Notifications can include notifying the owner of a site or onedrive, notification to the person, additional people. Messages can be customized and policy tips will be used.
- Users have the ability to override
Rights Management provides for a certain level of control over what actions a user can take with documents.

### 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
  
  1/17/2017

- [ ] 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)

### Set group protection and credentials interval
Use the settings in this section to control the caching policy of the license the application that opens the document will use and to allow sharing the downloaded document with users that belong to a specified group.

- [ ] Users must verify their credentials using this interval (days)

- [ ] Allow group protection. Default group:

  Enter a name or email address...
Retention provides a set of policies to determine what content to delete or preserve.

**Deletion Policy**
- Can be applied to specific site collections or site collection template
- Based on amount of time from Created Date or Last Modified Date
- Delete to Recycle Bin or Permanently Delete
- Site Collection policies override any site collection template policies

**Preserve Policy**
- Can be applied to specific site collections
- Can be based on keywords or search all content
- Can be set between specific periods of time
- Preservation is based on modified date
- Time frames to preserve can be based on days/months/years
- If content is deleted it will be preserved in a secure location
Azure Information Protection utilizes the RMS service, but expands capabilities to document classification and labeling. This service is still in its early stages and SharePoint still utilizes the RMS capability already available. DLP can help to classify content today.

1. Manual Classification
2. Automatic Classification
3. On-premise via RMS Connector
4. Document Tracking and Revocation

Device Management comes in few different versions. Intune can be utilized but some features are available with Office 365 (note an Intune license is still required). There are also other solutions such as Cloud App Security that can take additional actions on files that are covered with Azure Information Protection.

1. **Allow access only from specific IP networks**

2. **Allow access from apps that don’t use modern authentication**

Deploy this policy:
- Block downloading files in the apps
- Block taking screenshots in the apps (Android only)
- Block copying files and content within files
- Block printing files in the apps
- Block backing up app data
- Require app passcode
- Block opening OneDrive and SharePoint files in other apps
- Encrypt app data when device is locked
- Require Office 365 sign-in each time the app is opened

**OneDrive & SharePoint Mobile Apps**
Almost every action taken in Office 365 can be audited over the last 90 days. Hybrid auditing with SharePoint 2016 On-premise is currently in preview as well.

1. **Scope to User**
2. **Scope to file name, folder name, or site URL**
3. **Add an alert**
4. **Export Results**
eDiscovery interface makes it easy to locate content to place on legal hold, to discover content, and to export content.

1. Easily assign permissions to a case
2. Create Legal Holds for sites and mailboxes
3. Easy to add conditions, do not need to know query language
4. Export Results
Secure Store is a security analytics tool that will help you understand what you have done to reduce the risk to your data in Office 365, and show you what you can do to further reduce that risk.

Based on 75+ configurations and behaviors

Like a credit score for security

Risk Assessment

Recommended Actions

https://securescore.office.com/
ROADMAP


QUESTIONS & ANSWERS

cwilliams@cardinalsolutions.com
@corywilliams59