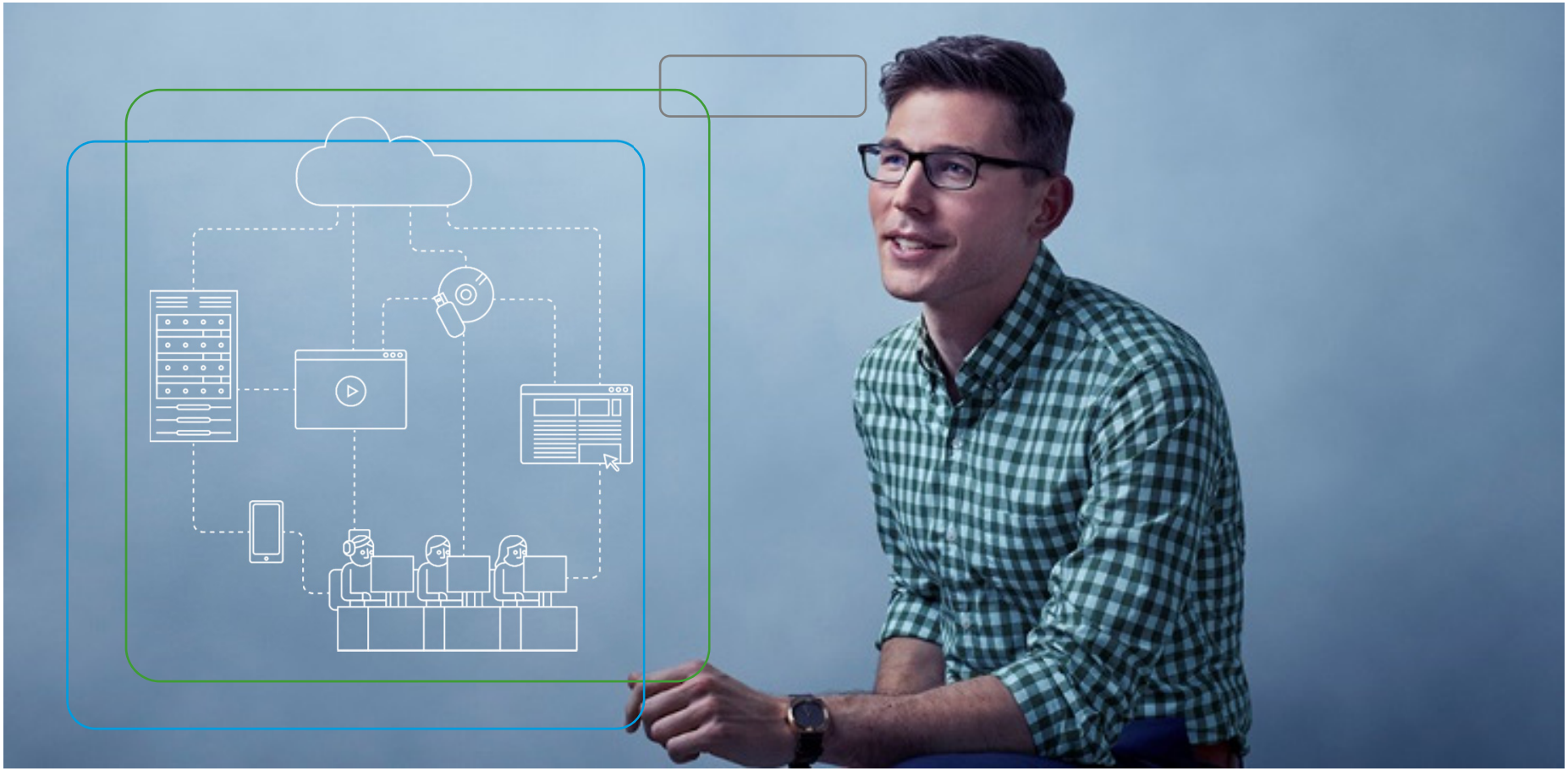


ASSESSING THE SECURITY OF MICROSOFT OFFICE 365

©2015 RSM US LLP. All Rights Reserved.

About Me – Diego Rosenfeld

- Principal at RSM US
- Advising private and public sector customers on Cloud solutions for the last 10 years.
- Lead a team that has deployed over 40,000 Office 365 “seats”.
- Consulting on security assessments and breach incident response.

©2015 RSM US LLP. All Rights Reserved.

RSM

Learning Goals

- Office 365 education
- Office 365 security deep dive
- Office 365 tools and demos

©2015 RSM US LLP. All Rights Reserved.

RSM

Microsoft is a *Cloud First* company

FY16 Annual Report Facts

- Commercial cloud annualized revenue run rate exceeded $12.1 billion, up more than 50% YOY.
- More than 70 million people use Office 365 everyday.
- Xbox Live monthly active users grew 33% YOY to 49 million.

©2015 RSM US LLP. All Rights Reserved.

RSM

Microsoft Products

Office 365

Dynamics 365

Windows IoT

©2015 RSM US LLP. All Rights Reserved.

RSM

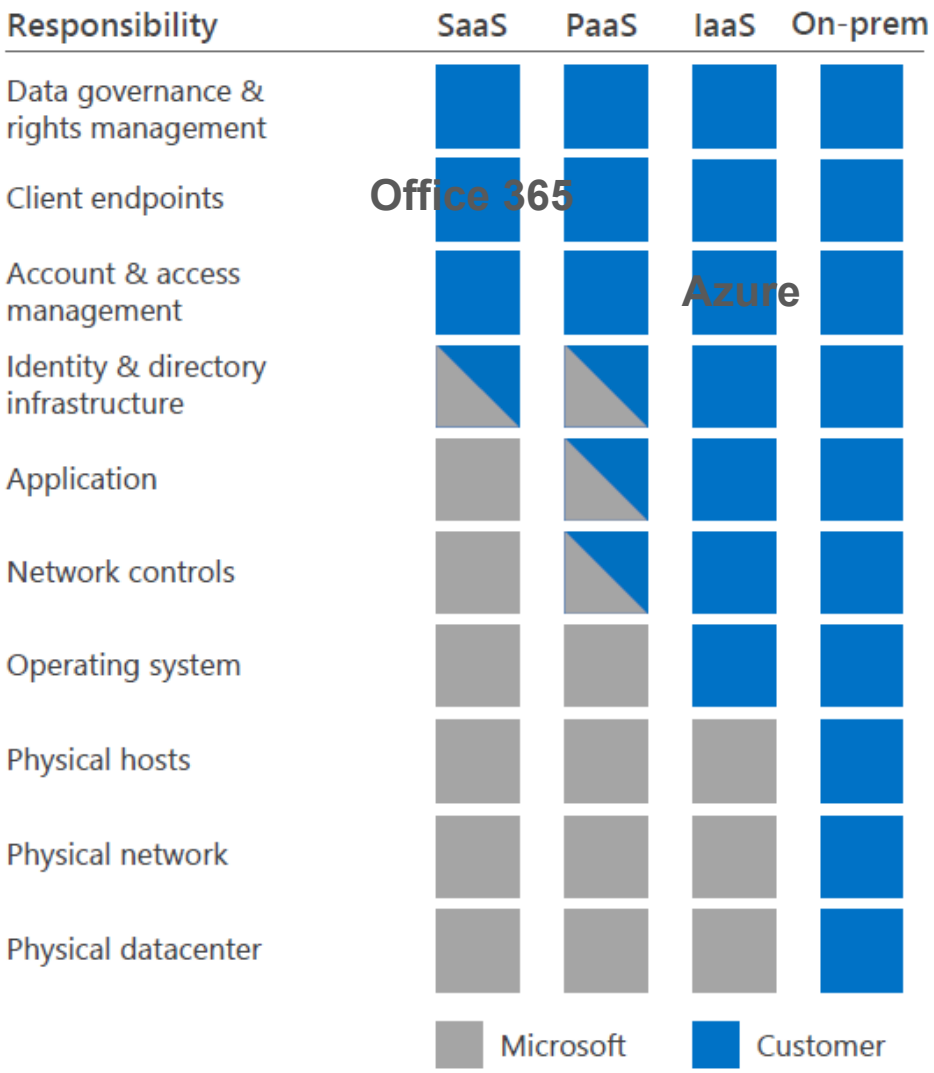
Office 365 Types

- Office 365 for Business
- Office 365 for Enterprise
- Office 365 for Government
- Office 365 for Government Defense (DOD standards)
- Office 365 for Education

©2015 RSM US LLP. All Rights Reserved.

RSM

Sharing Responsibilities with Microsoft



©2015 RSM US LLP. All Right

Office 365 Suites

Features *Office 365 Services*	E1 $8	E3 $20	E5 $35
Business Class Email and Calendars *Exchange Online*	50 GB	Unlimited	Unlimited
Social, Video, Sites, Work Management *Yammer, O365 Video, SharePoint Online, Planner*	●	●	●
IM, Online Meetings, Meeting Broadcast *Skype for Business*	●	●	●
File Storage, Sharing, Information Discovery *OneDrive for Business, Delve*	●	●	●
Office Online	●	●	●
Office Client Apps *Office 365 ProPlus*		●	●
Archiving, Rights Management, Data Loss Prevention, Encryption		●	●
Advanced Security Management, Advanced eDiscovery, Secure Attachments and URLs, Access Control			●
Analytics *Power BI Pro, Delve Analytics*			●
Cloud PBX *Skype for Business*			●
PSTN Conferencing* *Skype for Business*			●
Enterprise Plan Add-ons			
PSTN Calling** *Skype for Business*			+$24
CRM Online Professional *Dynamics*		+$50	+$50

©2015 RSM US LLP. All Rights Reserved.

How can we trust Microsoft Office 365?

Security

Our priority is to safeguard your data with state-of-the-art technology, processes, and encryption.

Privacy and Control

Your data is your data, you own it, you control the privacy of your data, who has access to it, and where it resides.

Compliance

We will always offer the largest portfolio of compliance standards and certifications in the industry.

Transparency

You will always have complete visibility into where your data is located and how it's managed.

https://www.microsoft.com/en-us/trustcenter

©2015 RSM US LLP. All Rights Reserved.

RSM

Microsoft Office 365 Compliances

	Regulatory and Compliance Domain	Office 365
Broadly Applicable	ISO 27001	✓
	ISO 27017	
	ISO 27018	✓
	SOC 1 / SOC 2 / SOC 3	✓
	CSA Star	✓
United States Government	FedRAMP	✓
	CJIS	✓
	DoD DISA	✓ Level 4
	FDA 21 CFR Part 11	✓
	ITAR	✓
	IRS 1075	✓
Industry Specific	HIPAA / HITECH	✓
	PCI DSS Level 1	N/A
	FERPA	✓
	CDSA	N/A
Region/Country Specific	EU Model Clauses	✓
	UK G-Cloud v6	✓
	Australia CCSL (IRAP)	✓
	Singapore MTCS	✓
	Japan FISC	✓
	New Zealand GCIO	✓
	Spain ENS	✓

RSM

©2015 RSM US LLP. All Rights Reserved.

Office 365 and FedRamp

- 900 controls in the Microsoft security framework
- Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense have received an authorization to operate (ATO) at moderate impact level.
- Microsoft must recertify every year.

https://www.microsoft.com/en-us/TrustCenter/Compliance/FedRAMP

©2015 RSM US LLP. All Rights Reserved.

RSM

Office 365 Security

- Auditing and Logging
- Identity Management
- Encryption
- Threat Protection
- Backup and retention

©2015 RSM US LLP. All Rights Reserved.

RSM

Auditing and Logging

- Comprehensive audit log search tool
- 90 day storage of logs on 150 events
- Integration with SIEM tools
- Office 365 Management Activity API
- Integrated with DLP (data loss prevention)

https://protection.office.com/#/unifiedauditlog

©2015 RSM US LLP. All Rights Reserved.

RSM

Identity Management

- ✓ Multi-Factor Authentication requires users to use multiple methods for access, on-premises and in the cloud. It provides strong authentication with a range of easy verification options, while accommodating users with a simple sign-in process.
- ✓ Microsoft Authenticator provides a user-friendly Multi-Factor Authentication experience that works with both Microsoft Azure Active Directory and Microsoft accounts, and includes support for wearables and fingerprint-based approvals.
- ✓ Password policy enforcement increases the security of traditional passwords by imposing length and complexity requirements, forced periodic rotation, and account lockout after failed authentication attempts.
- ✓ Token-based authentication enables authentication via Active Directory Federation Services (AD FS) or third-party secure token systems.
- ✓ Role-based access control (RBAC) enables you to grant access based on the user's assigned role, making it easy to give users only the amount of access they need to perform their job duties. You can customize RBAC per your organization's business model and risk tolerance.
- ✓ Integrated identity management (hybrid identity) enables you to maintain control of users' access across internal datacenters and cloud platforms, creating a single user identity for authentication and authorization to all resources.

©2015 RSM US LLP. All Rights Reserved.

RSM

Threat Protection

- Office 365 provides robust email protection against spam, viruses, and malware with Exchange Online Protection.

- Office 365 also offers Advanced Threat Protection (ATP), an email filtering service that provides additional protection against specific types of advanced threats.

©2015 RSM US LLP. All Rights Reserved.

RSM

Office 365 Encryption

- **For data in transit**, all customer-facing servers negotiate a secure session by using TLS/SSL with client machines to secure the customer data. This applies to protocols on any device used by clients, such as Skype for Business Online, Outlook, and Outlook on the web
- **For data at rest**, Office 365 deploys BitLocker with AES 256-bit encryption on servers that hold all messaging data, including email and IM conversations, as well as content stored in SharePoint Online and OneDrive for Business. BitLocker volume encryption addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers and disks.
- **In some scenarios, we use file-level encryption**. For example, the files and presentations uploaded by meeting participants are encrypted by using AES encryption. OneDrive for Business and SharePoint Online also use file-level encryption to encrypt data at rest.

©2015 RSM US LLP. All Rights Reserved.

RSM

Office 365 Backup, Retention, Recoverability

- Microsoft performs its own backups but designed for catastrophic data loss no single file/mailbox restores.
- Default deleted items recovery policy is 14 days, but can be changed to 30 days.
- Comprehensive policies available for “retain” and “delete” retention actions.
- Archiving and eDiscovery available in E3 plans or higher. Often companies put users on permanent legal hold.
- Many 3rd party “cloud to cloud” backup solutions for Office 365 to fill the gaps.

©2015 RSM US LLP. All Rights Reserved.

RSM

Office 365 Privacy and Transparency

- Who can access data and on what terms?
- Where is the data located?
- Your data when you leave?
- How Microsoft manages data?
- Responding to government requests?

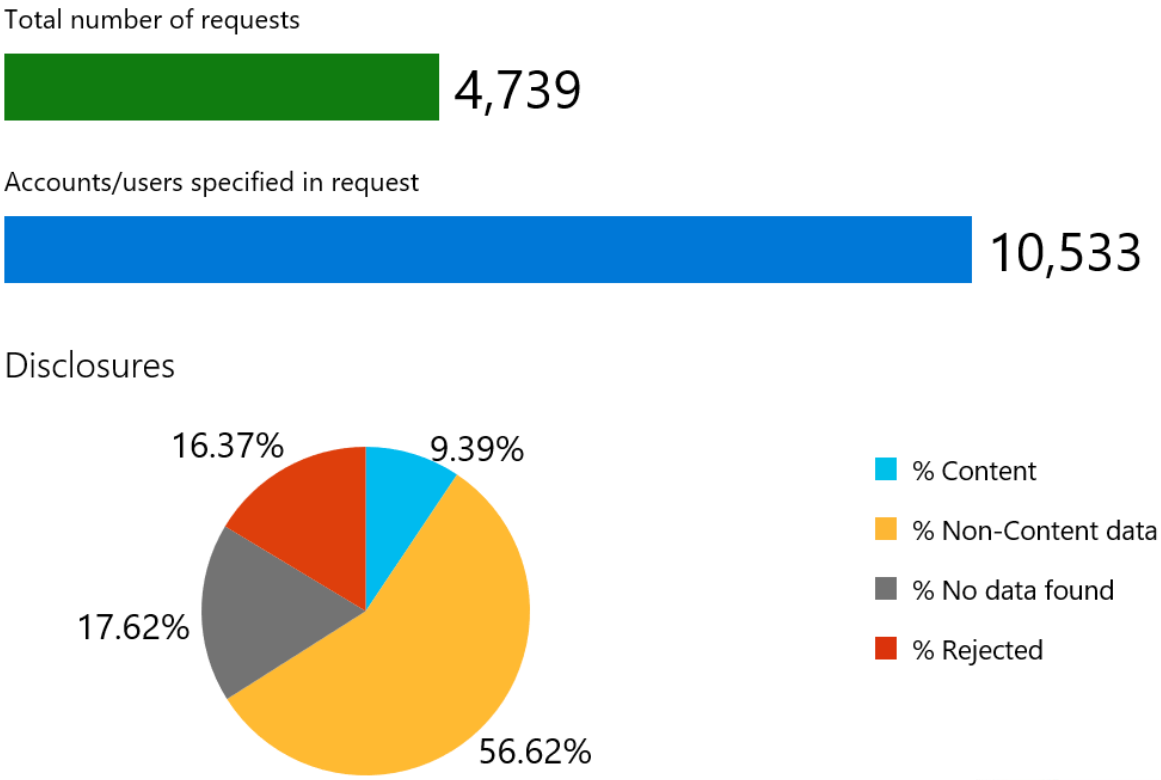
©2015 RSM US LLP. All Rights Reserved.

RSM

Government and Law Enforcement Request

Microsoft will not disclose customer data hosted in the Microsoft Cloud to a government or law enforcement except as you direct or where required by law.

Office 365 law enforcement requests for customer data Jul-Dec 2016



https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/

©2015 RSM US LLP. All Rights Reserved.

Who has access to your data and what terms

- Customer can export Office 365 data at anytime without notifying Microsoft.
- Microsoft engineers do not have access to customer data without being granted access.
- List of subcontractors fall under the *Microsoft Supplier Security and Privacy Assurance Program* and a list is publicly available.
- New Customer Lockbox feature

©2015 RSM US LLP. All Rights Reserved.

RSM

Where is Office 365 Data Stored?

- Microsoft follows a regional datacenter strategy. Publicly disclosed datacenters in Washington, Texas, Virginia, Iowa, California, and Chicago.
- Office 365 for Government logically separated from commercial customers. US datacenters only for Government.
- Under Government, access to content only by Microsoft employees that are US citizens with robust background screening. Criminal check, OFAC, BIS, FBI database check.

©2015 RSM US LLP. All Rights Reserved.

RSM

A Microsoft Datacenter

- 270 acres of servers in the high plains of Washington.
- Predictable climate and low cost hydroelectric power.
- Small town known for potato farming

©2015 RSM US LLP. All Rights Reserved.

RSM

What Happened to the Traditional Datacenter

- Microsoft designed ITPAC containers self contained with power, networking, servers, and trickle of water.
- Original datacenter had no walls! They built snow baffles to deal with piling up snow. New containers placed outside on concrete.

©2015 RSM US LLP. All Rights Reserved.

RSM

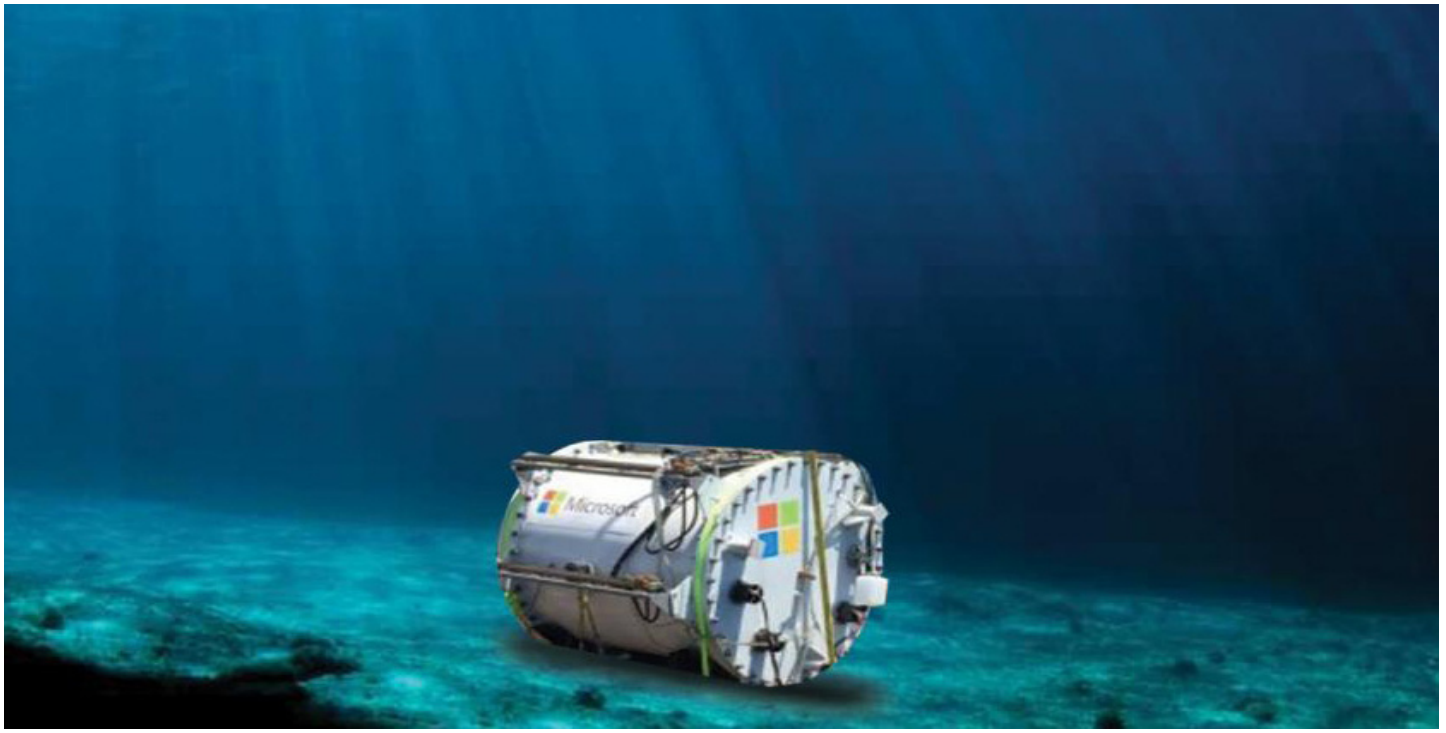
Let’s go back to the original design

- Microsoft realized the container maintenance was challenging and now moving to a traditional “rack” design that is based on the Open Compute Project hardware.
- This means higher density, software designed datacenters with easier maintenance when adding servers and new services.

©2015 RSM US LLP. All Rights Reserved.

RSM

What's Next (Project Natick)



- Testing underwater datacenter off the coast of California 30ft deep.
- Designed to be 5 year maintenance free.
- Addresses high real estate costs of coastal cities.

©2015 RSM US LLP. All Rights Reserved.

RSM

What happens when you leave the service

Microsoft contractually commits to specific processes when a customer leaves a cloud service or the subscription expires. This includes deleting customer data from systems under Microsoft's control.

- If you terminate a cloud subscription or it expires (except for free trials), **Microsoft will store your customer data in a limited-function account for 90 days** (the "retention period") to give you time to extract the data or renew your subscription. During this period, Microsoft provides multiple notices, so you will be amply forewarned of the upcoming deletion of data.

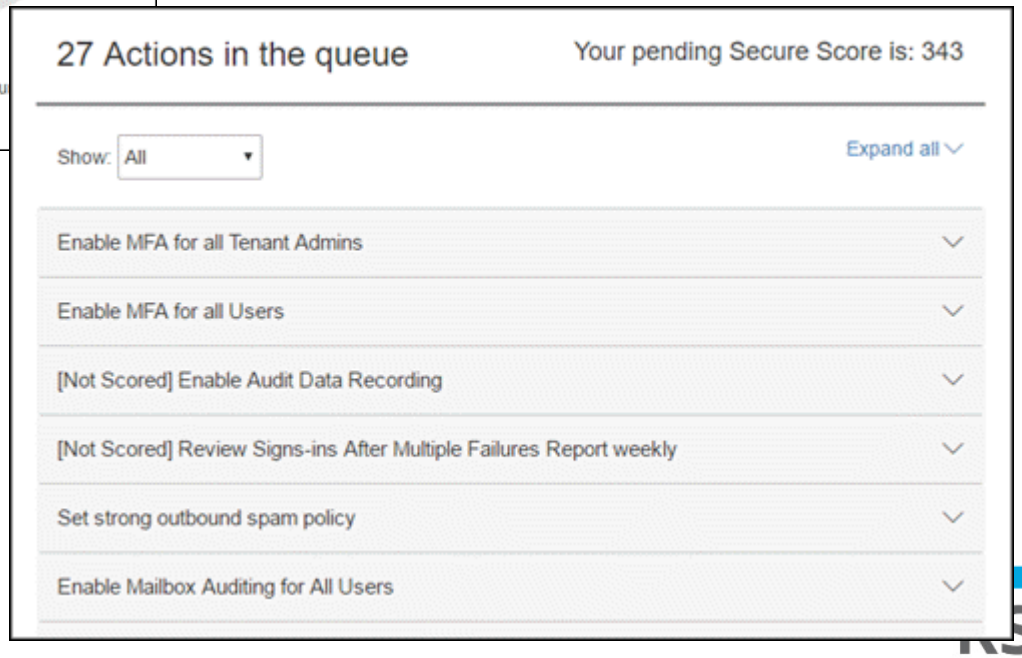
- After this 90-day retention period, Microsoft will disable the account and delete the customer data, including any cached or backup copies. For in-scope services, that deletion will occur within 90 days after the end of the retention period. (In-scope services are defined in the Data Processing Terms section of our Online Services Terms.)

©2015 RSM US LLP. All Rights Reserved.

RSM

Secure Score, “credit score for security”

Secure Score figures out what Office 365 services you’re using (like OneDrive, SharePoint, and Exchange) then looks at your settings and activities and compares them to a baseline established by Microsoft. You’ll get a score based on how aligned you are with best security practices.



If you want to improve your score, review the action queue to see what you can do to help increase security and reduce risks.

©2015 RSM US LLP. All Rights Reserved.

365 Command

Security Reports

O365 Audit Log	Office 365 Audit Log
Forwarding	All mailboxes that are forwarded.
External Forwarding	All mailboxes that are forwarded outside of your organization.
Search Audit Log	Search O365 Audit Logs.
Search Audit Log	Search O365 Audit Logs.
Full Access & Send As to Mailboxes	Mailboxes with users who have full access.
Compliance	Mailboxes with legal hold status.
Password Options	User's password expiration and strength settings.

- Powerful tool to automate many security reports that otherwise would require advanced power shell knowledge
- Mapping feature validates data location in Microsoft datacenters.

©2015 RSM US LLP. All Rights Reserved.

Demos

©2015 RSM US LLP. All Rights Reserved.

RSM

Q&A

Diego Rosenfeld
Principal
617-241-1170
Diego.Rosenfeld@rsmus.com

©2015 RSM US LLP. All Rights Reserved.