Data Resiliency and Governance in Microsoft 365

Authors

Maha AbuRumman - Compliance Technical Specialist
Graham Hosking - Compliance Technical Specialist

Introduction

In the bygone era of on-premises IT, many organisations held and maintained hardware, software and updates to their systems. Part of the standard IT operations included business continuity activities that occasionally required fully or partially redundant systems, intensive data backup processes, and data storage procedures.

It is still common today to incorporate all systems into a centralised backup on-premises, where data can be archived off to cheaper storage forms like tape. However, the growing complexity of data regulation and governance make these processes more difficult to manage.

Fast forward to the world today, where businesses are embarking on transformative journeys, with digital services being decentralised. Organisations are collaborating with third parties to provide internal and external services built on digital products that help them compete in their markets and achieve better financial results. This includes IaaS and PaaS platforms that enable them to develop products faster, collaborate with partners to co build solutions and reduce the time for delivery by reducing reliance on hardware being delivered to the data centre. It's in the SaaS subscriptions for services integral to the business such as email, data management, sharing of information and communications to promote productivity.

A major consideration for subscribing to a cloud service is the resiliency of that service. The move to the cloud has changed the landscape of business resiliency and data discovery. And the growing sophistication of cyberthreats as well as the high reliance on data in our digital world has brought laser focus on the issue of data resiliency.

As the provider of one of the most ubiquitously utilized productivity suites in the world, and the store for the majority of data created, shared and stored by individuals and businesses, Microsoft is keenly aware of the importance of the role we play in supporting the resiliency of our customers' data.

The threats of the digital world, combined with our modern operations mean we must revamp our resiliency strategies, and recognize that resiliency is no longer the sole responsibility of the data owner, but the joint responsibility of data owners and service providers.

In the next few pages, we will describe how Microsoft's M365 suite supports your data resilience needs in the available productivity tools, and how you can use the available compliance solutions to extend the protection and governance of that data as befits your business needs.

Shared Responsibility

Microsoft's responsibility

As the service provider, Microsoft partners with you to establish the baseline of resiliency for your data and services across our M365 offering. M365's business continuity strategy leverages hardware, network, and datacentre redundancy. Data replication between data centres provides high availability and reliability in the case of a catastrophic incident. It also increases resilience to mundane incidents such as isolated hardware failure or data corruption.

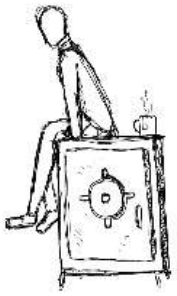
Microsoft 365 achieves service resilience through redundant architecture, data replication and automated integrity checking.

- Redundant architecture involves deploying multiple instances of a service on geographically and physically separate hardware, providing increased fault-tolerance for M365 services.
- Data replication ensures there are always multiple copies of customer data in different fault-zones, allowing critical customer data to be recovered if corrupted, lost or even accidentally deleted by the customer.
- Automated integrity checking increases data availability by automatically restoring data impacted by many kinds of physical or logical corruption.

In addition to the above, Microsoft also employs cyber defence tooling to protect customer data from cyber threats and attacks, such as malware, phishing campaigns, and others.

These built-in resiliency controls take the burden away from your organization of having to establish resiliency controls and tools to maintain data backups and perform restoration tests. Reducing the cost and management burden on your IT operations teams and enabling you to focus those resources on more fruitful efforts.

It remains then for your BCM planners and teams to validate and assess the suitability of the committed SLAs to your BC and DR plans and business needs. These provisions, however, are not the end of the line for your planning and commitments.



Customer Responsibility

Depending on where your organization operates, which industries you operate in, what services you offer and what data you process, your business might be subject to various laws, regulations and industry standards that might dictate data governance rules and controls that you must implement and apply to some or all of the data in your organization.

Microsoft is not able to manage these responsibilities for you but makes available to you tools that would help you manage these across your data estate.

Before you start using these tools, here are some things to consider:

- Where does your organization operate? In which geographies, countries, or jurisdictions?
- What laws, regulations and industry standards are you subject to?
- What types of data do you collect, process and share?
- Do the mandates for data protection and governance vary by location, data types, or other factors?
- What threats put your data at risk?
- In your organization, is data resiliency a regulatory requirement, a cyber threat mitigation or both?

It is essential that these questions are answered in cooperation with your legal, risk and compliance teams. Though IT and information security might be given the responsibility of applying appropriate controls and protection against that data, these controls must be aligned to the organization's responsibilities and contractual obligations.

Once you have your answers to these questions, and an understanding of the obligations well defined, you can apply the appropriate controls to your data and repositories.

Information protection

Many organisations today face the dilemma of knowing what data they actually have and where. M365 helps you solve this challenge by indexing and crawling through your data repositories to identify where sensitive information might live within the services we provide (SharePoint, OneDrive, Windows devices, Email, Teams chats, etc.).

By pattern matching the scanned data against predefined patterns, or data expressions we have documented, we can help you quickly determine if your organization is holding and processing personal information, financial information, or other predefined sensitive information expressions.

Why does this matter in the context of resilience?

Well, to start, it falls on your organization to determine the level of protection that must be applied to the data that resides in your M365 services. For example, must it be encrypted? Can it be freely shared externally or internally? And must it be retained for a specific period?

The intent is to enable your employees to be productive with minimal friction, but to protect your data from accidental or malicious accidents. To achieve this, classification labels can be applied to documents, and repositories denoting the sensitivity of the data. This serves two purposes; it informs end users of the files sensitivity ensuring awareness is spread of the classification, and it applies the relevant control to protect against accidents and misbehaviour.

Common examples include employees sharing files and data with partners that might contain sensitive IP that the organization deems confidential. Though the partners might be involved with the project, it might not be acceptable to share

certain IP information outside the organization. Encryption that was applied to this document through the “confidential” classification label travels with the file, and the external users would not be able to decrypt it.

Other scenarios are around sharing of financial data, like credit card information. Say a customer sale or support agent collects credit card information and is sharing with a colleague to complete a sale, this can be prevented from occurring on unsanctioned work channels, and the users would be notified of the breach of policy. Ensuring user awareness continues to build and protecting the organization from legal or regulatory liability.

Information protection capabilities can be extended to on-premises data as well with the Azure Information Protection Scanner (AIP Scanner).

Retention and Disposition

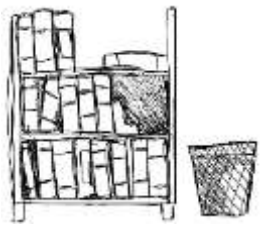
Microsoft services have some built in retention capabilities for data being deleted by end users. On a high level, Exchange emails are retained for 14 days in a recoverable items folder after users delete them. SharePoint Online retains files for a period of 93 days in multistage recycle bins. In both cases, Microsoft Teams data is retained forever. This includes chat messages in public and private channels as well as files shared in teams.

However, many organisations are subject to regulations, contractual requirements and laws that require them to retain certain data for longer periods of time and purge it upon end of life. To enable you to achieve these requirements M365 offers retention and data disposition capabilities that enable you to retain the data without having to move it out to a different location.

Commonly, organisations setup a default retention policy of 7 years. This would cover any data that resides in the core repositories of Exchange and SharePoint. Teams will continue to retain data indefinitely unless a policy is set to mandate deletion.

After the default policy is setup, it is important for the business to determine what regulations or standards affect the data the organization holds and processes. A file plan must be documented detailing the applicable retention requirements to the relevant data. This is where the previous exercise of knowing what data is held where becomes invaluable again. Knowing what data the organization holds in which locations, the organization can define retention and disposition policies to be applied depending on data type being held in the files and documents.

The policies can be setup to retain the data for a period and then automatically purge it or send the data through a disposition review cycle before it is permanently purged. If a file is subject to multiple retention policies, then there is an order of priority that it will fall under.



This order of precedence is designed to minimise the risk to the organization from a compliance perspective. Ensuring data is not deleted before its due date, and it isn't maintained for longer than it should be.

Records Management

Retention of data is one requirement many organisations are subject to whether by external mandate or by internal policy. However, some organization might have additional retention requirements known as records management.

Records are information and data created in the normal course of business activity that organisations must maintain as potential evidence in case legal need. They represent activities that were carried out in the normal business operations, such as: banking transactions, contractual agreements, invoices and other documents.

Not all documents would be classified as records. As records would comprise evidence of activity performed for delivery or receipt of service and are retained as evidence of action.

With M365, our records management solution enables you to declare files and data as records or regulatory records, this has the effect of locking the file to maintain an original document or file in an immutable state.

A retention schedule, depending on the type of data would be defined that would specify the retention period as well as the record state. Once the policy is applied, the initial file that was declared as a record is held in an immutable form and as a separate version of all subsequent copies which are stored in place.

This is essential for organisations that might be subject to records management and archival requirements by law, like in many public sector and health care organisations. And is critical for corporations that are subject to regulatory standards such as the Sarbanes Oxley and others that must maintain immutable records of their business transactions. Additionally, it is useful for organisations seeking to implement a records management system to their contractual obligations and maintain these records for potential defensibility and legal purposes.

All these capabilities enable our customers to enhance their data resiliency capabilities in M365, and fully manage the life cycle of data being created in the various documents and files by employees and users.

Businesses in various industries are subject to regulations and laws that mandate retention and preservation of records. Compliance Officers are burdened with the tasks of measuring compliance against various industry standards and regulations. They track their compliance efforts against multiple requirements, many of which are duplicated and sometimes even conflicting, and must report on them internally and externally. Some examples include:

- HMRC – Record Keeping (VAT Notice z00/21): requires businesses to maintain all business and VAT records for at least 6 years.
- Regulation 12, The reporting of Injuries, Diseases and Dangerous occurrences Regulations 2013: requires any incident information to be kept for at least 3 years.
- Article 49 of the regulation (EC) No 1272/2008 of the European Parliament and of the council: This regulation governs the movement of substances, mixtures and articles deemed hazardous to humans and the environment. It requires that suppliers maintain and keep all information for a period of at least 10 years after the substances or mixture is last supplied by them.
- The Registered Pension Schemes (Provision of Information) Regulations 2006: requires pension providers to preserve documents for the tax year related to them and 6 years following that.

Microsoft provides tools to help customers on their way to meeting these types of requirements, one of which is Compliance manager which provides a dashboard that indicates your compliance score in relation to your data protection and compliance posture. This includes recommendations to further improve data protection and export the evidence to a regulator if required.

Conclusion

If your organization is subject to laws and regulations that require you to implement controls to manage the data lifecycle, then you can trial the capabilities in M365 today by accessing purchase services in your M365 tenant and subscribing to the relevant trial. Alternatively, you can sign up for an E5 trial at: https://aka.ms/e5trial

You can learn more about our capabilities for information protection and governance by watching these sessions:

- MyIgnite - Manage risk and secure information across your environment (microsoft.com)
- MyIgnite - Information risks keeping you up at night? Deploy intelligent information protection and data loss prevention (microsoft.com)
- Data retention capabilities – Microsoft official documentation
- Trigger retention policies with Events in Advanced Data Governance
- Compliance Manager and Compliance Score

Authors

Graham Hosking - Compliance Technical Specialist
Maha AbuRumman -Compliance Technical Specialist

Illustrations

Becky Cholerton – Security & Compliance Technical Specialist