ISO/IEC 27001 requirements for backup and patching within AWS/Azure

Nicolai Böttger*, Norbert Piotrkowicz** and Jon-Steven Streller***
Faculty IV, Hochschule Hannover University of Applied Sciences and Arts
Hannover, Germany

Email:
*nicolai.boettger@stud.hs-hannover.de, **norbert-oskar.piotrkowicz@stud.hs.hannover.de, ***jon-steven.streller@stud.hs-hannover.de

Contents

I. Introduction

A. Motivation

Cloud computing is becoming more and more popular. It has a lot of advantages, mostly in the field scalability. New servers or storage can be quickly added ”on demand” with just one simple click of a button to increase total system capacity. This enables the developers to focus more on the development, rather than maintaining the hardware and infrastructure.

Another important factor of any system, besides its speed and capacity is the security. Of course a lot cloud providers are advertising how secure and how easy to maintain their solutions are and while this is true a lot of the work is taken away by the cloud itself since some things like patching or data backups must still be done to maintain high level of security.

Of course not everyone will be pleased with those activities, but if some company would want to store or use sensitive customer data, then they are often obligated to pass some certifications, like the ISO-27001.

The ISO contains a lot of requirements and recommendations on what Information Systems or ”ISMS” should contain and how some procedures should be handled. Of course since ISO is only a set of guidelines that can or can not apply to every system, not every activity is exactly specified.

Especially in the field of cloud computing, one needs to look at some specific points from a different angle. Of course cloud companies are advertising their compliance to ISO standard, but some systems that are running on their platform, can still be not compliant by default.

Both Azure and AWS have some tools that can help others in achieving compliance status. In this paper we will investigate how these tools - namely the Backup and Update Management Centers in Azure and AWS Backup and Systems Manager Patch - can assist in the achievement of the ISO compliancy.

B. Related Work

Some have already looked at a similar topic like [27], where AWS S3 and Azure Blob Storage and the technologies Microsoft and Amazon used for data encryption in transfer and at rest were compared

C. Cooperation with the insurance company HDI

This paper was produced in collaboration with HDI (part of Talanx AG, one of the largest insurance companies in Germany) as part of a Master's course in Applied Computer Science.

It aims to verify whether it is possible to perform backups and patching according to the ISO-27001 standard with the right configuration. This is essential for HDI, as the processing of sensitive (customer) data is part of their daily business.

The authors regularly met with HDI to present the latest research results and subsequently incorporated the feedback into the paper.

D. Cloud Computing Systems

Cloud Computing is characterized by several authors as a basic investment with the potential to sustainably change the IT industry. It has the potential to achieve a market structure and standardization of IT services, similar to other utility industries like gas, electricity, or water.

In this scenario, a global market infrastructure with standardized units emerges, where conditions (such as price per minute for instances with the same specifications) can be directly compared, resulting in increased market transparency [26].

A formal definition of what is meant by the term Cloud Computing exists only to a limited extent in literature. However, the National Institute of Standards and Technology (NIST) published a definition of what is meant by the term 'Cloud Computing':

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

The original definition can be found on:
https://csrc.nist.gov/publications/detail/sp/800-145/final

1) Business model: To meet the needs of the customer, there are various service models (XaaS). Generally speaking, the more the cloud computing provider takes over in terms of tasks (e.g. SaaS), the higher the costs will be. [26]

Infrastructure as a Service (IaaS):
With an IaaS, the cloud computing provider offers virtualization, servers, storage, and network according to the desired configuration. The customer takes care of the rest of the configuration, such as choosing the operating system. An IaaS is most similar to traditional server rental. [26]

Platform as a Service (PaaS):
In a PaaS, the cloud computing provider offers exactly the same as in an IaaS, but with the addition of the operating system, middleware, and a runtime. The goal of PaaS is to provide a complete platform with the desired development environment already pre-installed. This has the advantage that users don't have to worry about maintaining the operating system or security updates, and can fully focus on their task. [26]

Software as a Service (SaaS):
In a SaaS, the cloud computing provider offers exactly the same as in an PaaS, but SaaS also includes the provision of data and applications. This means that applications can be easily made available through the cloud with just one button press and can be accessed. [26]

This work will not focus on a specific type of XaaS. It will only show how the services are offered by cloud computing providers.

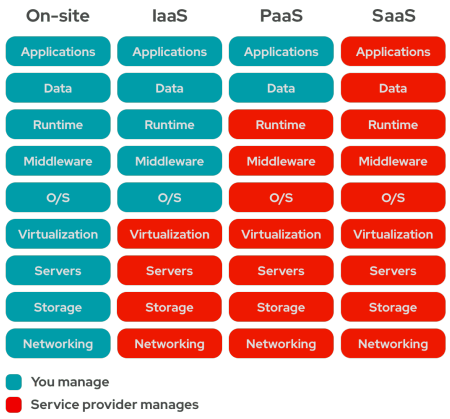

Fig. 1. A comparison between different 'Everything as a Service' (XaaS) models. [10]

II. ISO 27001

The ISO-27001 standard originates from the ISO-27000 family, which was introduced in 1995. The ISO-27000 family now includes more than 30 documents that define standards. [6]

A. Information Security Management System

An ISMS (Information Security Management System) is a systematic approach that sets out policies, objectives, processes, procedures, and regulations to achieve the goals of the organization.

It has the following focuses:

- Planning
- Implementation
- Monitoring
- Reviewing measures for data protection

To evaluate the quality of an ISMS, a value is calculated by means of a risk analysis. An ISMS is based on international standards such as ISO 27001.

It helps the organization to structure and improve critical

processes to ensure long-term data security. Certification according to ISO 27001 standards can enhance the trust of stakeholders. [24]

B. Explanation

On the one hand, ISO 27001 defines technical terms from the world of information security. In addition, it is a basic management system that provides instructions for the organization to effectively control activities and measures in the field of information security.

The 3 core aspects that the ISO defines for good security are confidentiality, integrity and availability.

Confidentiality means that only authorized persons have the right to access and read information.

Integrity ensures that information can only be changed by authorized persons.

Availability means the permanent availability of information to authorized persons, whenever these are needed.

Fig. 2. Confidentiality, integrity and availability (CIA triad)

In total there are 13 chapters that all address different measures that have to be taken into account to keep the ISMS secure. These range from internal organisation measures to personal security to access control to compliance measures. In principle, it is not always necessary to implement all the safety standards described in the ISO 1:1. Depending on the needs and intended use, certification can also be carried out for just a specific subsystem. vgl. [6]

The first version of ISO 27001 was published in 2005. Since then it has been changed and revised 2 times, once in 2013 and later on in 2022.

The changes in these versions are rather small and don't mean a complete rewrite of the ISO. For example from the 2013 to the 2022 version just a few chapters have been changed which resulted into a decrease in the number of security measures from 114 to 93. Both considered Cloud services in this work state that they are certified according to the ISO-27001:2013 version [5] [7].

Whether a company complies with the ISO standard is checked by certain certification bodies, which issue a certificate for 3 years if the result is positive.

C. Normative and Informative Standards

A distinction is made between necessary and recommended standards.

A necessary standard, also known as a normative standard, must be implemented compulsorily. This can be recognized by the fact that the standard's requirements contain the word "shall". [24]

A standard that is recommended contains the word "should" in its description. This type of standard is referred to as "informative". [24]

III. Backup / Patch-Management

A. Definition

1) Backup: In the process of data backup, data is copied to a separate data storage medium in order to have the ability to copy the data back to the original medium and restore the original state in case of data loss due to defects of the original storage medium or software errors. The data stored on a separate storage medium is also referred to as a backup copy.

2) Patching: Patching is the provision of a running system with (security) updates.

Legacy-Patching:

"Legacy-Patching" is largely done manually. Firstly it must be checked whether there are updates available for the current system and then reviewed before the installation can begin.

It must be ensured that the system and the applications running on it are not affected. As it is difficult to predict this in advance, a backup of the system should be created before each update.

In addition, the system is not available during the update and thus the availability (Fig. 6) is at risk.

If there are multiple systems, this whole process can be very time-consuming and costly for the company.

The described procedure is just an extreme example of how service patching can occur. Of course, there are also tools that can assist in maintaining legacy systems through automation. [25]

Cloud-Patching:

In contrast to "Legacy-Patching", where the update must be planned and executed manually or with the assistance of manually created automation procedures, the cloud provider takes over the provision of (security) updates and implements them on the service or system with "Cloud-Patching".

The goal of this approach is to fully automate the process and thus enable more regular patching. Additionally, there are approaches to ensuring zero downtime of the system by copying the service before each update and redirecting traffic to the copied service while the update is being installed on the original system.

Automation can save on personnel costs and the expertise of the cloud provider can ensure that security vulnerabilities are typically closed faster through patches than with the Legacy-Patching approach. [25]

B. Relevant characteristics from ISO 27001 (Annex A)

The ISO 27001 standard encompasses a total of 13 chapters (A.5 - A.18) that define both normative and informative standards (Chapter II-C). These standards also describe characteristics that can only be verified through on-site inspections or access to the system. Additionally, there are characteristics that have nothing to do with cloud computing.

Through these conditions, we have gone through all the standards and analyzed which ones are relevant for backup and patching. In the following chapters, all relevant ISO standards are listed and why they are interesting for this application case.

Access Control (A.9): Access control designates both access to the place and the premises, as well as access to the direct IT service itself (only access to the IT service is considered below).

An access control policy that lists and checks the security-relevant requirements is essential.

Users have access exclusively to networks for which they have been explicitly authorized. To enable the assignment of access rights to users, a formal process for registration and deregistration should exist.

The allocation of privileged access rights should be restricted and strictly controlled. A formal process for managing secret authentication information, such as users' passwords, exists and is followed.

User access rights are regularly reviewed and adjusted as necessary (e.g. upon termination of a business relationship or changes to contracts). Where required by the access control policy, access to systems should be controlled through a secure login procedure.

Third-party programs that could circumvent system protection measures should be strictly monitored and have limited usability.

Cryptography (A.10): A comprehensive security within the ISMS requires appropriate cryptographic measures to ensure authenticity, integrity, and confidentiality.

A documented security policy regulating the implementation and application of these measures forms the basis for this.

Another important security policy that should be in place relates to the use of cryptographic keys and lays out the life cycle of these keys.

Physical & Environmental Security (A.11): As cloud is a service that give you remote access to hardware, the hardware and location itself belongs to the cloud provider. Physical security is about physical access to the hardware itself, whether cables, power sources etc. are secure or redundant.

As the owner of project in the cloud has no influence, knowledge how such things are organized or have possibility to make changes to physical infrastructure of the data center, then this point as a whole should be handled by the provider itself. As the data centers are quite often also ISO certified, if one wants to certify themselves, then should also use ISO certified locations.

Operation Security (A.12): This standard ensures that information processing facilities are adequately controlled and managed. The basic measures for this are:

- Document operating procedures
- Change control
- Capacity control
- Separation of development, test and operational environments.

Measures to protect against malware must also exist. This includes Detection, prevention and recovery actions related to user awareness.

Other potential sources of danger, such as the exploitation of technical vulnerabilities, should also be prevented by regular checking and timely action when such a risk is identified. Additionally rules for installing software by users should exist.

Furthermore, backup copies of information and software should exist in accordance with a security policy.

Logging and monitoring measures are also defined in this standard. Event logs that record user activities and other incidents, but also activities of system administrators are generated and regularly checked. Another point is clock synchronization, which states that the clocks of all systems within an organization should be synchronized with a single reference source.

In order to check these points, regular audits should be carried out, which need to be carefully planned and should have minimal impact on business processes.

Redundancy (A.17.2): There is another sub-item in standard A.17 (Information Security Aspects of Business Continuity Management): redundancies. This point describes that the availability of information processing facilities should be ensured. As the name suggests, to accomplish this, there should be enough redundancy so that the desired systems can always be accessed.

C. Irrelevant characteristics from ISO 27001 (Annex A)

It was already mentioned in Chapter III-B that we only took a look at a specific selection of the measures in ISO-

27001. There reasons for that are that for one, it is just not possible to check certain measures with no further ado. The reason for that is that they would require an on-site inspection of the business premises. On the other hand many measures also are simply not interesting with concern to the topics backup and patching and cloud-computing like measures that are only regarding the internal organisation of the business (i.e. Leadership, Planning). For completeness the categories of these measures that were not considered are listed below.

- Leadership (A.5)
- Planning (A.6)
- Support (A.7)
- Operation (A.8)
- Communications Security (A.13)
- System Acquisition, Development & Maintenance (A.14)
- Supplier Relationships (A.15)
- Information Security Incident Management (A.16)
- Compliance (A.18)

D. Cloud-native services in Azure

1) Azure Backup: Azure Backup or Backup Center give the user an overview of all the backup activities. Such an overview can be very useful, not only because of its functionalities - which themselves can prove very useful indeed - but also in the spectrum of ISO certification. As for what it is, firstly - an overview of all backup activities, schedules, logs and alerts. Together with alerts functionality - which can also be set to notify some users directly with for example an email, Azure Monitor can help with the ”Operational Security (12.4)” ISO requirement which states that all errors and user actions must be logged and reacted upon. From there one can easily create new backups, policies or vaults. Items can be also restored here. [23]

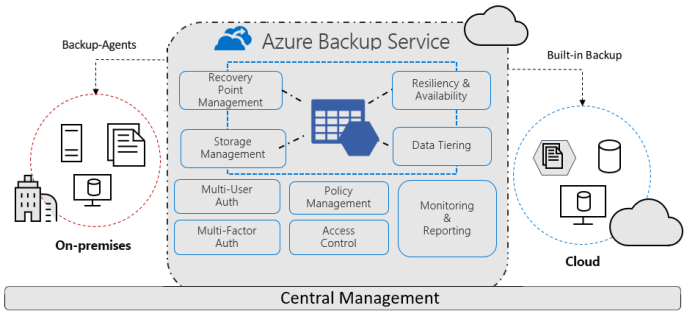

Fig. 3. Overview of Backup solutions for Azure

2) Azure Update Management: Azure Update Management [21] is very similar to the Backup Center. It also gives an overview, but consisting of Update status of virtual machines - both Windows and Linux. There you can see:

- the update status of machines (installing, rebooting or up to date),
- orchestration status that allows to schedule updates to individual machines and so update machines when they are not in use or to make sure, that enough machines will be available while some of them are updating,
- how many updates have been installed of failed to install,
- how many updates in how many machines are pending

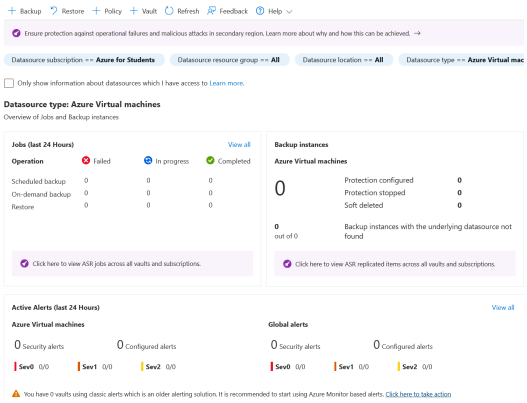

Fig. 4. Azure Backup center

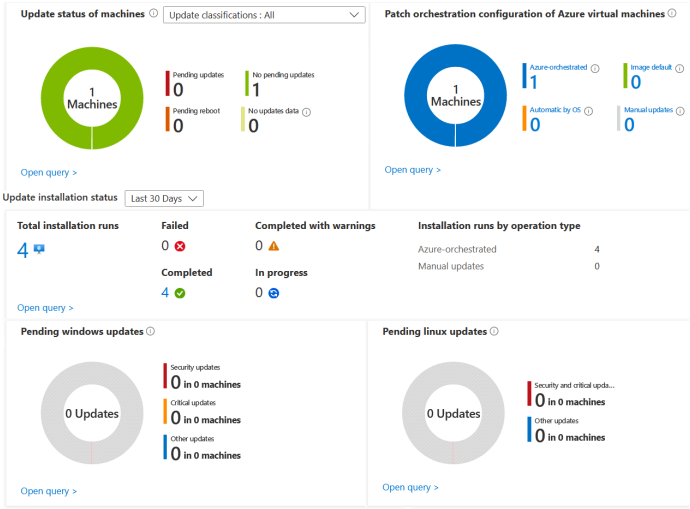

Fig. 5. Update Management center in Azure

E. Cloud-native services in AWS

1) AWS Systems Manager: AWS Systems Manager is a collection of features and tools that support the user in managing their deployed applications and infrastructure that runs in the AWS cloud. This provides options such as monitoring systems, managing services, and deploying software updates and patches (see III-E2). The goal of AWS Systems Manager is to efficiently and securely manage IT systems, compared to managing locally deployed infrastructure. [11]

2) AWS Systems Manager - Patch Manager: AWS Systems Manager Patch Manager is a part of AWS Systems Manager. This enables users to ensure that their deployed systems and applications are updated with the latest patches and software updates. With AWS Systems Manager Patch Manager, users can automatically deploy patches, subject the patches to a

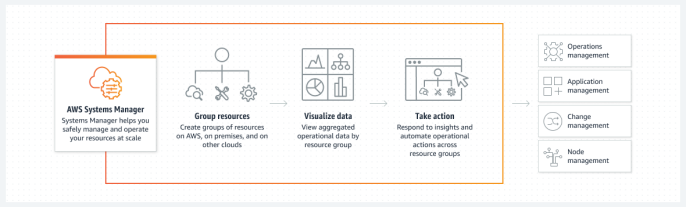

Fig. 6. Confidentiality, integrity and availability (CIA triad)

review beforehand to ensure that the respective patch can be applied successfully to the system. In addition, reports can be generated to monitor the status of the patches and the systems and applications. In this way, it can be ensured that the systems and applications are always up-to-date and have a maximum level of security. [1]

IV. Azure: Policies

In order to be ISO-27001 compliant in Azure, it is not enough to just look at the respective services that exist explicitly for backup and patching. Some points of the ISO can only be accomplished and secured by correct configurations of the Azure subscription. If this is not considered, the individual services within Azure are also not ISO-27001 compliant.

In Azure subscriptions, it is possible to add policies that check whether certain conditions apply to accounts and resources working with this subscription. Below, the main ones are summarized in their corresponding chapters of the ISO 27001 and briefly explained.

A. Access Control (A.9)

Rule: **"Management of privileged access rights"**: There are multiple different policies in azure to monitor accounts. One of them offers the possibility to check whether all accounts in the Azure subscription that have write or owner permissions have multi-factor authentication. Another checks whether there are any external accounts with write and owner permissions in the subscription. Last but not least the usage of custom-made RBAC-rules is monitored.

Rule: **"Management of secret authentication information of users**: This rule adds additional policies for managing authentication data. For example, it checks that a general password policy exists. In addition, another policy controls the management of authenticators and the deactivation of them. Additionally, the authenticator lifespan is checked.

Rule: **"Review of user access rights"**: Consists of policies that monitor user permissions, account provisioning protocols, and the status of user accounts. In addition, this rule oversees the conditions for role membership.

Rule: **"Removal or adjustment of access rights"**: Monitors old accounts and accounts with ownership-permissions that should be removed from the subscription. Additionally it contains rules to check and reeveluate account permissions and to monitor notifaction and change of access permissions upon personnel changes.

Rule: **"Secure log-on procedures"**: One guideline in this rule is setting a threshold for consecutive failed login attempts. Another guideline requires automatically ending a user session after extended periods of inactivity. Additional guidelines in the rule may enforce, for example, user uniqueness or biometric authentication mechanisms.

B. Cryptography (A.10)

Rule: **"Policy on the use of cryptographic controls"**: This rule contains several guidelines for checking the cryptographic processes in individual Azure systems. For example, it is checked that a data protection policy exists and is documented and that Privacy notices are provided. Furthermore there are policies to check disk encryption on vms and that secure transfer to storage accounts is enabled.

C. Blueprint

These (and many more) Policies to check conformity with ISO 27001 are all part of a blueprint in Azure called *ISO 27001 Shared Services* which can be added to a subscription to check whether it is in line with the ISO norms [3].

V. Object-Storage

A. Explanation

Object Storage is a technology that allows the storage of very large amount of data of various kind. Instead of organizing it into folders like in standard file system, every item contains metadata and a unique ID which both help with efficient data retrieval. For that usually multiple APIs like REST exist that can insert new data or query existing files. Ideally Object Storage is used within Cloud where it can be very easily scaled or distributed across multiple machines or even data centers. [12] [13]

B. Microsoft Azure Blob-Storage

So as written in the explanation, Blob Storage is used to save different data types to be accessed by applications or as simple storage service. It is important to know, that to use blobs you need to create a "storage account" first. In this account a blob container must be created. All files will then be stored in such a container.

As for backup, there are multiple options:

- Blob snapshots - every blob can be backed up with a snapshot that will be marked with a timestamp. The problem with it is that the container with multiple blobs can not be backed up as a whole. If a blob gets overwritten, its old snapshots containing data from the time of snapshot creation can still be found by using a link with the snapshot parameter. If the blob should be deleted, it can only be done after deleting all its snapshots.
- Soft Delete - after deletion of some blob, if soft delete was activated for given storage account, an item can be recovered. In Azure portal "Show deleted blobs" option can be checked to see and possibly recover the file. The files will be held for the time specified on creation of the storage account.

- Versioning - if blob versioning is enabled in the storage account, even if the blob gets overwritten, similar to snapshots, older versions can be viewed and recovered, or simply set as current version.
- operational backup - or in different words ”point in time restore” - is a solution created in the backup vault. Although such vault is made for storing backups, it is not storing any blob data. In case of blobs it is just like an overview. It uses other techniques that were just mentioned to back up the data in the storage container itself and not the vault. It also has some limitations, like when a container gets deleted and no container soft delete is active, all the data is gone, since operational backup was also stored in the same container. Good thing is that such backups do not need to be scheduled, it will be continuously backed up, so it is restorable to any point in time.

1) Access Control (A.9): Azure RBAC (Role based access control) - One can define roles which can be assigned to users or applications. Such roles can have set of permissions like read or write access to a specific resource. An example for such a role for application is the backup vault that needs the ”Storage Account Backup Contributor” role to be able to back up data available in the storage account. All these roles can be seen in the Access Control (IAM) panel of the storage account. Possible built-in roles include from basic ”Reader”, ”Owner”, ”Contributor”, to more granular ”Storage Blob Data Reader”, ”Storage Account Backup Contributor”. It is also possible to create completely new roles. [16]

2) Cryptography (A.10): Every blob that was written to Azure Storage after October 20, 2017 is automatically encrypted with Azure Storage encryption [15]. Older blobs can be downloaded and re-uploaded to encrypt them. For storage keys, Microsoft managed keys or customer managed keys can be used. All customer keys must be added to the azure key vault. Besides that, data can be double encrypted with additional infrastructure encryption which can be used to encrypt some or every file with a separate key [18].

3) Physical & Environmental Security (A.11): As already written in the section III B., this part is handled by the cloud provider. All that could be done in the Blob Storage context is setting the right region for data storage.

4) Operation Security (A.12): Monitoring for backup activities consisting of Blobs can be seen directly in the Backup center. After selecting ”Datasource type” to Azure Blobs, an Overview screen containing some basic data shows up. Here one can see how many planned or manual jobs were applied successfully or failed, which backup instances are configured and which had some errors. Lastly a list of active alerts is shown with different severity levels and type.

For more details, one could go through the ”Monitoring + reporting” tab which contains 4 items.

- Backup jobs - is again just an overview with a bit more details than the standard overview. It shows when and how long it took to backup an Instance, from where to where the data was copied and with what result it ended.
- Alerts - as in the overview screen, it shows what alerts got triggered. Additionally some processing rules and action groups can be set here. If alert gets thrown, according to rules set, an action can be triggered, whether to send some notification or to trigger some other more complex function on some resource which in turn can help with some other points of ISO-27001 like (A.16)(Information Security Incident Management) in particular parts about reporting and reacting on errors.
  As for messages there are four options which include SMS, e-mail, Voice notification (available only in US) and push notification to mobile app. Another notification option is to choose notified persons by their role like Reader or Owner of Resource and so sending e-mails to multiple persons at once.
  Next step is to set an Action. Possible choices are: Automation Runbook, Azure Function, Event Hub, ITSM, Logic App, Secure Webhook or Webhook. Runbooks can for example restart a virtual machine or run some user defined script. In Azure function it is possible to create some function in standard programming language to for example respond to HTTP requests or run any arbitrary function [2]. Event Hubs use Events to integrate to the Apache Kafka platform [4]. Logic Apps is a tool to create automated workflows with a graphical interface with only small amount of code [19] and Webhooks can send some data wrapped in JSON package to Microsoft Teams and other similar services.
- Metrics - makes plots of different metrics like for example backup count in last the 24 hours. Some alerts and actions could also be set here that can react on a given threshold of some metric.
- Backup reports - a reporting solution that uses Azure Monitor logs and Azure workbooks. Azure Monitor Logs can query collected data and analyze the results. The Workbooks are used as a canvas to visualize captured data. With reports it is easy to see which systems take up resources and create possible future resource usage predictions.

5) Redundancy (A.17.2): As for redundancy, as mentioned above, operational backup will be stored on the same machine as the original data. The good thing about the Microsoft approach here is that you can choose the Replication strategy for your storage account containing blob container. This needs to be specified at the time of creation of the storage account. Available replication options are [17]:

- LRS - Locally redundant storage, minimum what can be chosen, it copies the data three times in the same data

center. In case of hardware failure, data can be restored. In case of fire or flood, data could be lost for ever. This tier could still be useful, if for example, data must be stored in the same country due to other requirements.

- ZRS - Zone-redundant storage - In this case all the data will be copied to three separate data centers in the same region. If some problem in one data center emerges, that would make it unavailable, the application can become unavailable for a short amount of time, until the calls get redirected to other data centers from the same zone. Of course, if all regions in the zone get somehow disabled, then all data will not be available or gone. Here one should also check the availability, since not all regions support ZRS. If premium storage account is in use, not every region can support ZRS.
- GRS - Geo-redundant storage - Data will be stored in two different regions. Inside these regions it will additionally be copied using LRS.
- GZRS - Geo-zone-redundant storage - Data will be stored like in case of ZRS and additionally copied to a different region where LRS will be used.

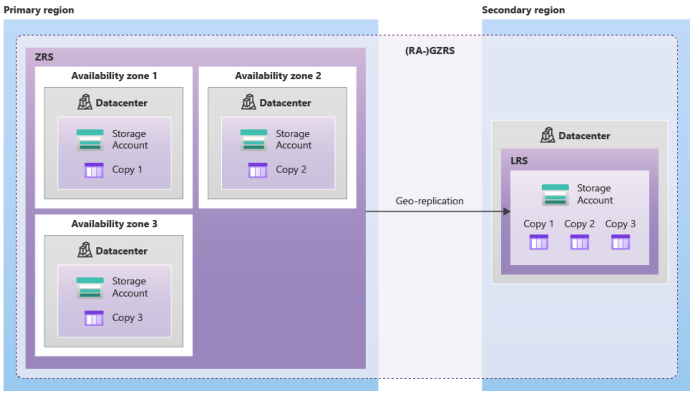

Fig. 7. GZRS as a whole, on the right only LRS and on the left ZRS can also be seen

C. Amazon Simple Storage Service S3

Amazon Simple Storage Service, also known as ”Amazon S3”, is an object storage technology (Chapter V-A). However, to configure this object storage to be ISO-27001 compliant, prerequisites must first be met. To create a backup from an S3 bucket, the respective S3 bucket must have the ”data versioning” option enabled in the bucket configuration. [9]

1) Access Control (A.9): In order to comply with ISO-27001, it is necessary to have the ability to either restrict or expand access to the created S3 backup. This can be achieved using Amazon “Identity and Access Management”, which limits access to all Amazon resources (e.g. Buckets or Objects) to the account owner. The account owner can then grant access to the backup to other individuals through the creation of access policies. Since the S3 backup is only accessible to the account owner in its default configuration, no modifications need to be made in order to meet the ISO-27001 standard.

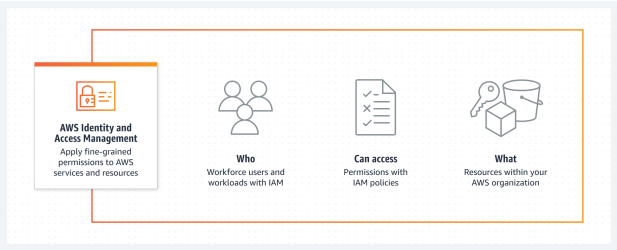

Fig. 8.

2) Cryptography (A.10): In the ISO-27001 standard, cryptography plays a crucial role. Thus, it is important to ensure that these normative standards are met. To meet these standards, the S3 bucket must be encrypted. When creating or configuring a bucket, there is no possibility to create or configure an unencrypted version of a bucket. By default, S3 buckets are AES-256 encrypted and thus meet the desired requirements.

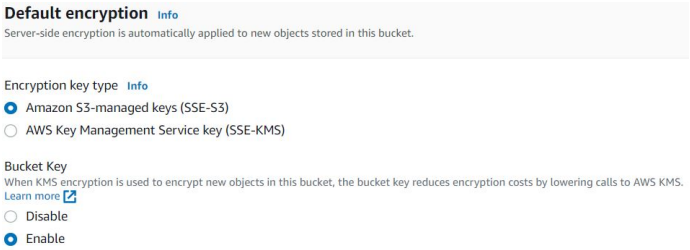

Fig. 9. The crucial configuration parameters can be seen in the figure

3) Physical & Environmental Security (A.11): For compliance with the standard, it is important to ensure that the location of the S3 bucket and the backup are stored in a certified location. The certified locations can be taken from the official ISO-27001:2013 certification for AWS.

4) Operation Security (A.12): By default, tracking backups in an S3 bucket is not configured. However, AWS provides two useful tools that can track different activities related to backing up S3 buckets.

Amazon CloudWatch:

With the CloudWatch monitoring tool, it is possible to track metric data and create multiple alarms that are triggered when, for example, a value falls below a certain threshold. The alarm then triggers the Amazon Simple Notification Service (SNS), which sends a push notification via the previously defined communication channel (HTTP(S), SMS, mobile push message, etc.). [8]

Amazon EventBridge:

Every job that is executed is associated with a backup. With the EventBridge monitoring tool, it is possible to closely

examine and monitor these jobs or events. [8]

5) Redundancy (A.17.2): By default, an S3 bucket is backed up in two different locations within the same region. Similar to Microsoft Azure's solution, it is possible to store object storage backups across multiple regions. Whether cross-region backup solution is necessary to maintain compliance is uncertain. It should suffice if the redundancy is stored in two different locations.

Fig. 10. Example configuration of an S3 backup across multiple additional regions:

VI. Virtual Machine

A. Explanation

A virtual machine is a software solution that allows managing multiple operating systems and applications on a single physical computer.

This is achieved by creating a virtual environment that mimics the hardware of the actual computer. Each virtual machine has its own virtual hardware components, including CPU, memory, and storage devices.

To virtualize hardware, a hypervisor is needed which is usually installed on the computer's operating system and enables accessing the host computer's hardware resources.

The use of virtual machines has many advantages, including the ability to run multiple operating systems and applications on a single physical computer, the ability to use resources more efficiently, and the ability to make IT infrastructure more flexible and scalable.

B. Update Management Center and Virtual Machines in Azure

No system is perfect and there are many vulnerabilities that can affect the safety of the whole system, thus it is very important to keep everything up to date. Of course as more and more machines get added to the system and there are multiple types of machines, different versions of Linux and Windows, the more complex the update process would get.

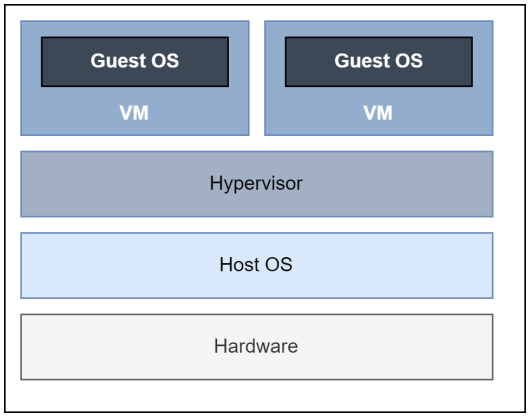

Fig. 11. Type-2 Hypervisor (Hosted Architecture)

Sometimes not only the operating system needs update, but also the programs running on it.

To help with this task, Microsoft came up with the Update Management Center. This gives the maintainer a quick overview about current condition of the machines and also let easily run, plan or even automate future updates. As for the ISO norm, there are some points that can be applied to the update process and we choose same points as in the part about backup processes.

An important term that will be used in this part of work is the "Availability first principle" - it means, that the service will be updated so, that the service running on these machines, should be disturbed only as much as needed while update process takes place. It means, that a only portion of virtual machines will be updated at once. [20]

1) Automatic VM guest patching: There are multiple possibilities to update virtual machines from within Management Center:

- Automatic by OS (Windows only) - uses standard Automatic updates, does not support availability first principle.
- Manual (Windows only) - this option should be only used if some custom patching solution will be used.
- ImageDefault (for given image, Linux only) - depending on Linux distribution, it will use some standard way of installing the updates. similarly to "Automatic by OS" no availability can be guaranteed.
- Azure-orchestrated or AutomaticByPlatform - as per availability first principle, Azure will control which and when machines will be prompted to install their updates and reboot if needed. It can be set while creating the VM, "Update settings" screen or with a property "osProfile.[linuxConfiguration, windowsConfiguration].patchSettings.patchMode=AutomaticByPlatform" It is also required that the image of the VM is supported for orchestrated updates, but the list is very long and contains most of the popular Windows Server versions and Linux distributions. Other requirements include that Windows VMs have to have Azure VM Agent installed

and Windows Update service running. For Linux Azure Linux Agent must be installed and at least version 2.2.53.1. Both Windows and Linux must have access to their respective update endpoints like Windows Update servers as they will be used to check and download the update packages. [20]

2) Access Control (A.9): As for Access Control, this functions exactly the same as within Backup as written in the subsection with same name in the ”Object-Storage” section. The only difference lies within the role that can be used by default which is this time ”Virtual Machine Contributor”.

3) Cryptography (A.10): For cryptography, the only point that applies here would be the distribution of update files. As the files will come directly from either Windows Update service or Linux software repositories. Just like in other standard update routines, the same security standards apply.

4) Physical & Environmental Security (A.11): This chapter applies the same for VMs as with Object Storage and so a data center should be chosen that is ISO-27001 compliant.

5) Operation Security (A.12): This chapter is about the Management of the running system, which the Update Center clearly does as from there changes to running systems can be maintained by installing newer versions of Programs, thus also removing potential security flaws in current versions of the system. For Operational Security it is also important to monitor all the actions and changes to the virtual machines. From Update management center there are multiple positions visible that can help with those tasks. [14]

- Manage Machines - similar to the overview, this time a set of machines can be chosen from a list and updates can be checked, forced or some schedules assigned.
- History - in this tab all update actions are listed. It is shown which machine got updated or assessed with the number of updated packages and a result of the operation and timestamps of those operations.
- Workbooks - similar as with the Backup Reports, Workbooks make it possible to create graphs and overviews that could be used to show current and predict future capacities and problems.
- Update Settings - here the orchestration settings can be changed or periodic check for updates enabled. There is also a Hotpatch option available there, but it is only for Windows Server 2022 Datacenter Machines. It only reduces the number of needed restarts, but still some are needed to install big cumulative updates.
- Schedule Updates - provides the maintainer the possibility to set an update date to a specified day and time for selected machines, so downtimes and unwanted restarts can be managed and set for a later date if needed. There is a maintenance period setting too, where if updates do not manage to install in a given time, the machine will not restart or not all updates will install in this maintenance session. Such informations will be gathered in logs and available to check by its maintenance run ID where all the updates and their status will be listed.
- One time update - lets the user choose a virtual machine and selects updates that the maintainer wants to install and set whether the operating system can or should restart after installation.

6) Redundancy (A.17.2): One of the most important things in updating is the redundancy. Some updates take a lot of time and then also require a restart. Of course the update process should not be received by the users of the system, so when using Azure-orchestrated updates some steps are made to make the process as smooth as possible. For the availability first principle, updates are installed mostly in off-peak hours, when the impact of a few missing machines in the system will be the lowest. The patches are then downloaded and installed automatically. A thing to mention here is that only security and critical patches will be installed. Other non critical programs need to be scheduled manually.

When the update takes place, it will be phased in a way that:

- Geo-paired regions will not be updated at the same time and second region will continue only if first were successful. These regions are for example Europe that contains North Europe and West Europe regions. Thus if an update in some region like West Europe fails, it will not be installed in the North Europe one and so leaving at least one of them running. [22]
- Within same region - VMs in different Availability Zones are not updated at the same time and VMs that are not included in any Availability Set are batched so, that not all VMs of single subscription are updated at once.
- Availability Set - All VMs that are in a single Update Domain will be updated together. If the machines are not in same Update Domain, then they will be updates sequentially.

[20]

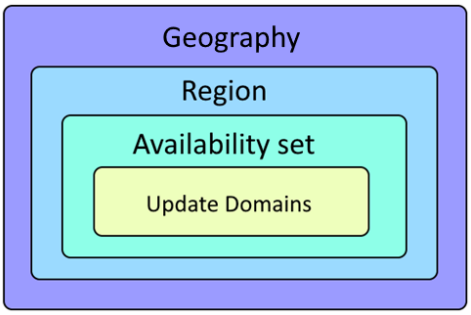

Fig. 12. Update regions structure

VII. Conclusion

From our perspective, it is not always easy to apply ISO guidelines to Backup and Patching. Quite often it needs to be looked at a lot deeper than just the Backup and Patching parts themselves. For example if the accounts that are used to access the backup and patching options of the cloud providers are not secure (compliant with ISO-27001) requirements then it does not matter if the stated options are perfectly compliant with the ISO standards. The options that are available through the Backup and Update centers of both providers can definitely help as written and explained in respective parts of this work. Some parts of the ISO-27001 standard are very general, and to see if some settings are enough to pass the certification would require a lot more expertise from our side and more specialized view on the data and systems that need to be certified. For example the Redundancy point, as it is written in the ISO - it needs to be redundant enough to satisfy the availability concern. For this we can not give a clear answer if local redundancy is enough here, or even cross-region redundancy.

References

[1] AWS Systems Manager Patch Manager - AWS Systems Manager. https://docs.aws.amazon.com/de_de/systems-manager/latest/userguide/systems-manager-patch.html.

[2] Azure Functions documentation. https://learn.microsoft.com/en-us/azure/azure-functions/.

[3] Control mapping of the iso 27001 shared services blueprint sample. https://learn.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-shared/control-mapping.

[4] Event Hubs—Real-Time Data Ingestion — Microsoft Azure. https://azure.microsoft.com/en-us/products/event-hubs/.

[5] Iso- und csa-star-zertifiziert. https://aws.amazon.com/de/compliance/iso-certified/.

[6] Iso/iec 27001 - isms-zertifizierung. https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/iso-27001.

[7] Microsoft Azure Deutschland erfüllt internationale Zertifizierungsnorm für Informationssicherheitsmanagementsysteme (ISO 27001) und den Schutz von personenbezogenen Daten in Public Clouds (ISO 27018). https://news.microsoft.com/de-de/microsoft-azure-deutschland-iso-zertifizierungen/.

[8] Monitoring. https://docs.aws.amazon.com/aws-backup/latest/devguide/monitoring.html.

[9] Using versioning in s3 buckets. https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html.

[10] Vergleich von iaas, paas und saas. https://www.redhat.com/de/topics/cloud-computing/iaas-vs-paas-vs-saas.

[11] Was ist AWS Systems Manager? - AWS Systems Manager. https://docs.aws.amazon.com/de_de/systems-manager/latest/userguide/what-is-systems-manager.html.

[12] Was versteht man unter objektspeicher? https://aws.amazon.com/de/what-is/object-storage/.

[13] What is object storage. https://cloud.google.com/learn/what-is-object-storage.

[14] Assessment options in update management center (preview)., 11 2022. https://learn.microsoft.com/en-us/azure/update-center/assessment-options.

[15] Check the encryption status of a blob - azure storage, 11 2022. https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blob-encryption-status?tabs=portal.

[16] Choose how to authorize access to blob data in the Azure portal - Azure Storage, 12 2022. https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal.

[17] Data redundancy - Azure Storage, 12 2022. https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy.

[18] Encryption scopes for Blob storage - Azure Storage, 12 2022. https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview.

[19] What is azure logic apps?, 9 2022. https://learn.microsoft.com/en-us/azure/logic-apps/logic-apps-overview.

[20] Automatic vm guest patching for azure vms - azure virtual machines, 1 2023. https://learn.microsoft.com/en-us/azure/virtual-machines/automatic-vm-guest-patching.

[21] Azure automation update management overview, 1 2023. https://learn.microsoft.com/en-us/azure/automation/update-management/overview.

[22] Cross-region replication in Azure, 1 2023. https://learn.microsoft.com/en-us/azure/reliability/cross-region-replication-azure.

[23] What is Azure Backup? - Azure Backup, 2 2023. https://learn.microsoft.com/en-us/azure/backup/backup-overview.

[24] M. Brenner, N. gentschen Felde, W. Hommel, S. Metzger, H. Reiser, and T. Schaaf. *Praxisbuch ISO/IEC 27001 : Management der Informationssicherheit und Vorbereitung auf die Zertifizierung*. München: Hanser, 2020.

[25] Hai Huang, Salman Baset, Chunqiang Tang, Ashu Gupta, K N Madhu Sudhan, Fazal Feroze, Rajesh Garg, and Sumithra Ravichandran. Patch management automation for enterprise cloud. In *2012 IEEE Network Operations and Management Symposium*, pages 691–705, 2012.

[26] Jonas Repschläger, Danny Pannicke, and Rüdiger Zarnekow. Cloud computing: Definitionen, geschäftsmodelle und entwicklungspotenziale. *HMD Praxis der Wirtschaftsinformatik*, 47(5):6–15, Oct 2010.

[27] Iman Saeed, Sarah Baras, and Hassan Hajjdiab. Security and privacy of aws s3 and azure blob storage services. In *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, pages 388–394, 2019.