BLACK CELL
Protecting critical infrastructures

Audit of cloud services

Table of Contents

1. Introduction 3
  1.1. The importance of cloud services 3
  1.2. Purpose and structure of the whitepaper 3
2. Cloud services short overview 3
  2.1. Cloud deployment models 3
  2.2. Cloud service models 4
3. The role of audit in security and compliance 4
4. Determining the need for an audit 4
5. Audit types 5
6. Audit programs 5
  6.1. Audit programs supporting comprehensive audit 5
  6.2. Audit programs supporting targeted audit 6
  6.3. Service provider specific audit programs 6
7. Necessary knowledge for conducting cloud audit 6
8. Usability of the audit results 7
9. Future trends and challenges 7
10. Summary and recommendations 7

1. Introduction

The proliferation of cloud services is inevitable and as these solutions are outside of the enterprise perimeter with less oversight and management possibilities, they are prone to cyberattacks. We must understand the weaknesses of cloud services utilised by our enterprise to effectively tackle them. To this end, conducting a specialized audit might be beneficial. Our whitepaper contains best practices and recommendations on the audit of cloud computing services.

1.1. The importance of cloud services

In our post-pandemic hybrid- and teleworking environments cloud services are of paramount importance. These services are increasingly being used by individuals and organisations for their cost-effectiveness, scalability, and ease of use. Today, it is inconceivable that anyone who is involved in any form of computing or information technology does not use cloud services.

There are many benefits to using cloud services, but there are also risks one must consider. Any system is secure if the three pillars of information security, i.e., confidentiality, integrity, and availability (CIA triad) are guaranteed. The only way to ensure compliance is to audit the cloud service. The result of an audit highlights areas that require improvements along the CIA-triad and provides recommendations for the security of cloud services.

1.2. Purpose and structure of the whitepaper

The whitepaper briefly describes the architecture, operation, advantages and disadvantages of different types of cloud services, and identifies the methods to consider when auditing different cloud services. In addition to defining the audit methodologies, this paper covers the knowledge required to conduct an audit, when, by whom and the type of audit recommended to conduct in order to achieve the audit's purpose.

2. Cloud services short overview

In this chapter, the service and deployment models for cloud services are reviewed. The deployment and service model of the cloud service is to be considered when planning the audit.

2.1. Cloud deployment models

Public Cloud: Public clouds are hosted and managed by third-party cloud service providers. They offer on-demand resources, making them cost-effective and scalable for businesses. Examples include AWS, Azure, and Google Cloud.

Private Cloud: Private clouds are dedicated to a single organisation and are hosted on-premises or by a third-party provider. They provide more control and security but can be more expensive to set up, manage and maintain.

Hybrid Cloud: Hybrid clouds combine public and private cloud resources, allowing data and applications to move seamlessly between them. This provides flexibility and the ability to keep sensitive data on the private cloud while utilizing the scalability of the public cloud.

2.2. Cloud service models

IaaS (Infrastructure as a Service): IaaS provides virtualized computing resources over the internet. Users can rent servers, storage, and networking, giving them more control over the infrastructure. Examples include Microsoft Azure, AWS and Google Cloud.

PaaS (Platform as a Service): PaaS offers a platform and environment for developers to build, deploy, and manage applications. It abstracts much of the infrastructure management, focusing on application development. Examples include Google App Engine, AWS Lambda and SAP Cloud Platform.

SaaS (Software as a Service): SaaS delivers software applications over the internet. Users can access applications without the need to install or maintain them locally. Examples include Google Workspace, Microsoft 365 and Salesforce.

3. The role of audit in security and compliance

Individual’s usage of cloud computing services does not necessitate a standalone audit, although it is worth considering reviewing the cloud provider's recommendations for configuration, hardening and security enhancement. This whitepaper focuses on auditing cloud services by enterprises once they are deployed and in use. It is important to note here that an advantage/disadvantage analysis is required prior to deploying a cloud service, which has audit elements. It may not always be the case that a cloud-based solution should be chosen.

Organisations may also be required to audit cloud services by directives (NIS2 Directive - security audits), legislation (varying from state to state), standard compliance (ISO 27017 and ISO 27018 Cloud security standards) and internal policies (Cloud security policy). All of these have a compliance constraint that requires an audit, and addressing the deficiencies in the audit findings ensures compliance. So, it is not only necessary to perform an audit at a time that the organisation deems important (after an incident), but to ensure compliance with various norms.

4. Determining the need for an audit

This chapter explains when an audit of cloud services is necessary. As defined in the previous section, when a legal or other regulatory or standard compliance requirement is imposed, an audit is mandatory.

However, some organisations are not subject to legislation or standards, in which case it is up to the organisation's need for security to audit the cloud services it uses or operates.

If the management of an organisation wants to ensure that the data (or possibly customer data) controlled and processed in cloud services is secure, an audit is necessary to see where the gaps are. This is a preventive audit, which is not common, especially in small and medium sized businesses.

Usually, the need for a cloud services audit arises when an organisation suffers an incident with significant negative financial or reputational implications. This is a reactive audit, actually part of the incident management, which is performed or conducted by an organisation to see what the failures were, what the further risks are and to prevent the same security incident from occurring.

As mentioned above, where legislation or standards require an audit, it is usually a public authority or certification organisation that audits the cloud service, focusing on areas it considers to be risky. As with all audits, this can be prepared for, but the stakes are higher from a compliance perspective for these audits than for internal audits required by recommendations or internal regulators, or even those that arise from a self-imposed requirement.

You can build security into cloud services, but without an audit you won't see the gaps, the vulnerabilities or risk areas.

5. Audit types

There are different types of audits, depending on why you need to audit cloud services. A comprehensive audit is one that examines all aspects of a cloud service. It covers the entire organisation including regulatory, compliance, security, and other areas.

There are target tests that examine a certain slice of the security, compliance, and performance of cloud services. These audits are, of course, shorter term and focus only on subsections.

There are administrative, physical, and logical audits, which are carried out depending on the purpose of the audit. Administrative audits focus on the regulatory, record-keeping and documentation parts, physical audits are based on the shared responsibility model and are in most cases the responsibility of the operator rather than the organisation using the cloud service, and there are logical audits, penetration and stress tests, which examine configuration and hardening.

Of course, every cloud service is different, as such there are also service-specific audits that are designed to audit a specific vendor's solution and not cloud services in general.

The need for an audit usually also determines whether the audit is carried out by an external auditor or an internal auditor. In this respect, a distinction can be made between external and internal audits.

6. Audit programs

Once one identifies the type of cloud service to audit and the purpose of the audit, one needs to decide between a comprehensive or a targeted audit. The audits are planned in audit programs, which can vary depending on the service and the methods for audit.

6.1. Audit programs supporting comprehensive audit

Comprehensive audits, which are not service-specific but provide a general control test to ensure the audit, examine the entire environment from administrative, physical, and logical perspectives. Such an audit program could be the Cloud Controls Matrix published by the Cloud Security Alliance, which can be used to test architectural relevance per control, governance compliance by selecting the service delivery model under audit. The Excel spreadsheet issued for conducting the audit contains the provider and user responsibilities per control. In case the organisation has other standards or other compliance, the control matching will assist in conducting the audit.

An excellent methodology for conducting comprehensive audits is the IS AUDIT/ASSURANCE Program Cloud Computing, which is an audit program compiled by ISACA. The program covers the entire cloud service audit with a focus on Governance and Operations controls using COBIT5 as a reference.

6.2. Audit programs supporting targeted audit

Comprehensive audit programs are suitable for auditing only sub-areas. Whether you want to audit selected areas regarding risks (access management, hardening, data transfer etc.) or you want to audit the target area during the detection phase of an incident management, the controls of the comprehensive programs are suitable for this purpose.

6.3. Service provider specific audit programs

Service-neutral audit programmes have been presented so far. However, it is important to note that there are also audit programs specific to the solutions offered by separate cloud service providers. This allows us to audit our cloud-based systems offered by large cloud service providers in a comprehensive manner. Such audit programs are also available for Microsoft, Google, Amazon. It is important to note that these cloud services also have built-in audit modules to assist the auditor in performing the audit.

7. Necessary knowledge for conducting cloud audit

Auditing cloud-based systems requires special preparation and knowledge. It is important that the auditor is aware of the knowledge required to conduct an audit. For this purpose, it is recommended to have a certificate presenting the auditing profession at your disposal. Such knowledge can be presented by the CISA (Certified Information Systems Auditor) certificate or the ISO/IEC 27001:2022 Internal or Lead auditor certificate. These are the most common auditor certificates in Europe.

In addition to the basic auditor knowledge, knowledge of cloud services is required, so it is recommended to have the general knowledge, which can be demonstrated by the CCSK - Certificate of Cloud Security Knowledge.

However, there is also a certificate for auditing cloud services, which allows certified persons to carry out comprehensive and targeted audits effectively. Such a certificate is the CCAK - Certificate of Cloud Auditing Knowledge, managed by the Cloud Security Alliance.

These certificates can be used for general cloud audits. However, service provider specific audits can only be performed effectively if the auditor has the specific expertise. For this reason, it may be recommended that the auditor has for example the AZ-900, AZ-500 etc. certificates for Microsoft.

In addition to expertise, experience also plays a crucial role in auditing cloud-based systems.

Skills are not only acquired through certification, but self-paced training is also important. There are several training materials available to help you acquire the necessary knowledge. These include the Controls & Assurance in the Cloud: Using COBIT 5 book, which provides practical guidance for enterprises using or considering using cloud computing. It identifies related risk and controls and provides a governance and control framework based on COBIT 5.

Publications in various journals and websites can also help the auditor to prepare.

8. Usability of the audit results

The usual result of an audit is the report that identifies non-compliances and deficiencies and provides confirmation that controls are working properly.

The result of the audit can be used to demonstrate compliance, i.e. that the organisation has fulfilled its obligation (legal or standard) to have an independent audit of its cloud services. This is a compliance use case.

The audit report can also be used as a checklist to address deficiencies and non-compliances, and thus as an action plan. It also highlights weaknesses and conditions that need more attention if the cloud service is to be used securely.

9. Future trends and challenges

The use of cloud services is becoming more and more prevalent in organisations due to the many benefits that can be realised from cloud services. On-premises systems are still present, but the trend shows that more and more organizations switch to cloud-based information systems.

Cyber attackers are aware of this trend, and they are constantly developing exploits for known vulnerabilities of cloud services, as well as developing new attack techniques to successfully gain access to these systems.

Protection can be successful if we are aware of the weaknesses in our cloud-based systems, which we can only identify through audits. We must be able to anticipate where and how an attacker wants to access our systems to achieve their goals. For this reason, it is necessary to map the gaps as thoroughly as possible so that we can patch them later.

10. Summary and recommendations

Auditing cloud services is not an easy task. You need to plan exactly what you need, what methodology and audit program you can use to achieve it. It is important to be aware of the specifics of the audit and cloud services and start the process accordingly.

If your organisation needs external assistance, please feel free to contact our firm, either for audit consulting or for the audit tasks to be performed. Contact: compliance@blackcell.io