cloudatmo
The experts in cloud management

TRANSITIONING TO THE CLOUD SUCCESSFULLY

- THE ULTIMATE CHECKLIST ☑

CLOUD IT SERVICES FOR GROWING BUSINESSES
PHONE: (07) 3667 7397
EMAIL: SALES@CLOUDATMO.COM.AU
WWW.CLOUDATMO.COM.AU

YOUR TRANSITION TO THE CLOUD CHECKLIST

As businesses transition to cloud computing, they open themselves up to a world of benefits, from increased flexibility to cost-effective solutions. However, with great benefits come great responsibilities, and it is essential to ensure that your move to the cloud is a successful one, with all the appropriate measures taken to protect your business.

Our Transition to the Cloud Checklist provides you with a comprehensive guide to the critical steps and considerations needed for a successful transition to the cloud, all while maintaining the security and integrity of your data. Our checklist covers a range of areas, including multi-factor authentication, email spam and protection, backups and disaster recovery, licensing, governance, compliance, data management, automation, and monitoring.

In this checklist, you'll find detailed explanations of each area, along with examples of how these steps can help safeguard your business. By following this checklist, you'll be better equipped to make a successful transition to the cloud, with your business's security and wellbeing at the forefront of the process.

☐ Multi-Factor Authentication:

Multi-Factor Authentication (MFA) is a critical security measure that adds a second layer of protection to you and your staff members accounts. By requiring multiple forms of verification, such as a password and a one-time code from a mobile app, MFA significantly reduces the risk of unauthorised access.

For example: If your password is ever stolen and someone attempts to access your account, they will also require a one-time code that is sent to your phone.

☐ Email Spam and Protection:

Implementing robust email spam protection is vital to filter out malicious emails and protect your organisation from phishing attempts and malicious attacks. These solutions use advanced algorithms to detect and quarantine spam, phishing, and malware emails, helping to maintain a secure environment.

For example: You can minimise and block malicious emails from reaching your staff. This reduces the risk of them accidentally clicking on emails and infecting business computers.

☐ Backups & Disaster Recovery:

Backups and disaster recovery (DR) are the lifelines that ensure business continuity in the face of catastrophises. A comprehensive DR plan should include regular backups of critical data, well-defined recovery procedures, and periodic testing. Having a well-documented and regularly tested disaster recovery plan is essential to minimise downtime and data loss in case of disasters.

For example: A staff member accidentally deletes a folder containing important company files. This can quickly be recovered with little downtime to the business.

☐ Licensing:

Licensing in the context of cloud services involves choosing the right license model for your organisation's needs and ensuring you're using the licensed services effectively. It's important to select the most cost-effective licensing options that align with your usage patterns. Actively monitoring your license usage to avoid overpaying or underutilising your licenses, ensuring you get the best value from your cloud investments.

For example: You can choose the most expensive license and only use a portion of its features, or you can purchase licenses that align with the direction of the business and accounts for growth and features that will be used.

☐ Governance:

Governance in the cloud refers to the establishment of policies, procedures, and controls that guide how cloud resources are provisioned, managed, and utilised. This includes practices like resource tagging, which helps with cost allocation and tracking, as well as cost show back and chargeback to ensure accountability. Effective governance is essential for maintaining control over your cloud environment, optimising costs, and ensuring compliance with organisational policies and regulations.

For example: You receive a bill for thousands of dollars with line items detailing what these are for. This can sometimes take hours to check what each of these line items are for, however, with correct governance you can match this back to what makes sense to the business (usually applications) and understand the cost per application that you run.

☐ Compliance:

Compliance is a critical consideration for organisations both big and small. Cloud services should adhere to these regulations, and organisations should implement controls to ensure compliance. This involves maintaining proper documentation, enforcing standards, and continuously monitoring and adapting to changes in your organisation's framework.

For example: if the business enforces that all staff cannot use USBs in the office anymore, you can now roll out a standard that USB devices are blocked on all business devices.

☐ Data Management:

Efficient data management is crucial for organising and securing data in the cloud. Labels and classifications help categorise data based on sensitivity, allowing for tailored access controls and encryption. Data protection mechanisms should be in place to safeguard sensitive information, ensuring it is only accessed by authorised personnel. Effective data management practices help maintain data integrity and confidentiality.

For example: You can enforce rules within your business where specific files cannot be emailed externally or copied to external devices such as USBs.

☐ Automation:

Automation simplifies repetitive tasks, enhances efficiency, and reduces the risk of human error. In a cloud environment, automation can be used for provisioning resources, scaling infrastructure, and responding to security threats. Implementing automation not only saves time but also improves consistency and reliability 24/7.

For example: You can automatically install applications and enforce all security baselines on new computers that are setup for staff members.

☐ Monitoring:

Continuous monitoring is essential for gaining real-time insights into the performance, security, and health of your cloud resources. Monitoring tools and solutions help detect and respond to issues promptly, ensuring uninterrupted service delivery. Proactive monitoring enables organisations to identify and address potential problems before they impact operations, contributing to a more robust and reliable cloud environment.

For example: If a malicious attack is attempted on key accounts to the business, a monitoring system would alert on this happening, and preventative actions can be taken to block any further attempts.

IF YOU WOULD LIKE ANY ASSISTANCE WITH YOUR TRANSITION, PLEASE DO NOT HESITATE TO REACH OUT TO US - (07) 3667 7397