



Cloud Solution

for

Mathew Made Construction

By Preston Chee

Table of Contents

Cloud Principles and Design

Business Description and Research

- Deployment Model

- Service Model

- Infrastructure Diagram

Cloud Networking & Storage

- Additional Business Research

- Procedures when ISP goes down

- Virtual Private Network

- Kinds of Files Stored

- How will Business Connect?

- Domain Name System

- Storage Providers

- Content Delivery Network

Assessing Cloud Needs

- Research

- Framework Diagram

- Baseline

- Feasibility

- Gap Analysis

- Gap Analysis Diagram

Engaging Cloud Vendors

- Capital and Operating Expenditures

- Potential Cloud Vendors

- Variable and Fixed Costs

- Licensing Model

- Evaluation of Cloud Vendors

- Service Level Agreement

- Migration Principles

Management and Technical Operations


- Aspects of Operating

- Development & Operations

- Financial Planning

Governance and Risk

- Risk Assessment



- Risk Response
- Documentation
- Vendor Lock-In
- Policies and Procedures

Compliance and Security

- Data Sovereignty
- Regulatory Concerns
- Industry-Based Requirements
- International Standards
- Certifications
- Security Concerns, Measures, and Concepts

Business Research

Business Name	Mathew Made Construction
Number of Employees	30
Location(s)	Cedar City
How long has the company been in business	5
Purpose of the Business	General Construction
Existing Technologies	SaaS. Quick books, ZOHO, gmail, Dropbox. Router, desktops, Square. Ramp.
Other Notes	Storage options and Centralization of services

Deployment Model

The deployment model that would fit best for the Mathew Made Construction would be a hybrid cloud. Based on what I was told the company is looking for a storage solution that would enable them to store their files while also having access to their data offline as well. It also will allow the company to have more control over any sensitive data. Another reason why a hybrid is the best fit is since the company's storage demands variety from season to season. The hybrid will allow them to better adjust their storage needs all the while without having the need to invest in a big on-premise infrastructure.

Service Model

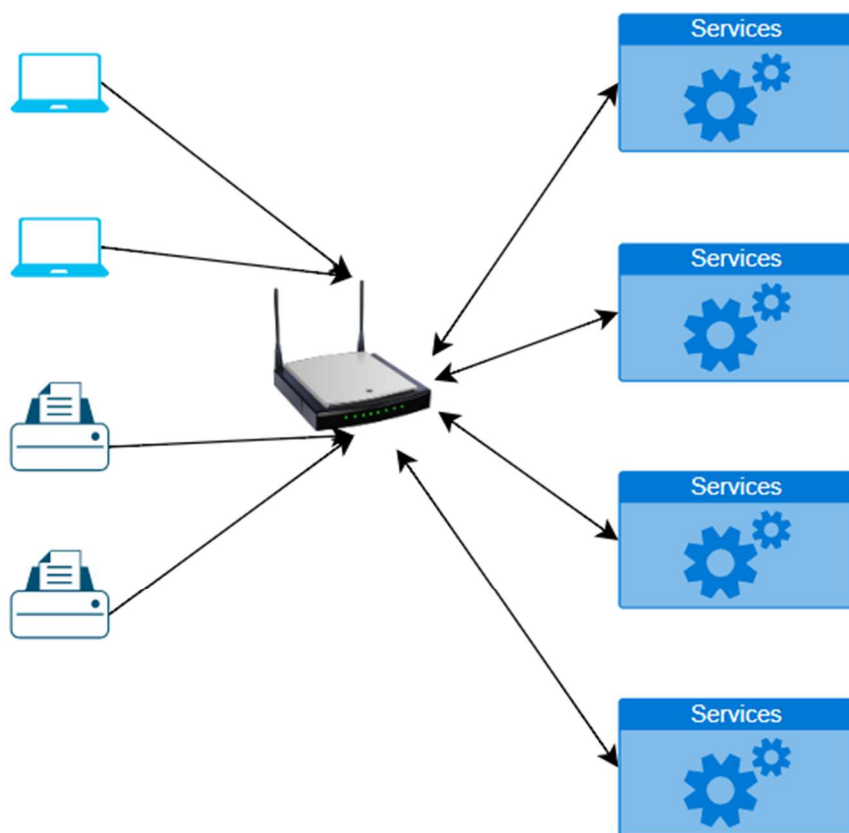
The best model would be a combination of SaaS (software as a service) combined with (Infrastructure as a service). The SaaS will help make sure that the company has access to user-friendly and maintenance free services. The IaaS will allow the company to host and manage its storage needs

dynamically. The IaaS model enables the company to build a flexible and scalable infrastructure to support their storage needs without requiring the physical hardware.

Cloud Design for your Business

The design for the business puts focus on redundancy and high availability. The redundancy will be done through geo-redundancy ensuring the data remains available even when the region the data is stored is down. This will also include backups for disaster recovery. The high availability will be done by using load balancing and auto scaling features to maintain consistent performance when needed.

Infrastructure Diagram



Additional Business Research

Internet Service Provider Name	TDS
Data Connection Type	cable
Download and Upload speeds	100MBS/ 30MBS
More than one ISP?	No

Procedures when ISP goes down

Work offline and wait for connection to be restored.

Virtual Private Network

No VPN's currently in use.

Recommended: Secure VPN for remote employees accessing sensitive data.

How will the Business Connect?

Using direct internet access with multi-factor authentication. This will allow the company to connect to the cloud resources over the internet while ensuring secure login. This will allow staff to have access to all their SaaS application that they have with internet access. The second one would be utilizing the offline syncing capabilities of storage services in the event that they need to have access to their data but are not able to access the internet. The other option would be using a VPN that would allow staff to access their management tools and any other sensitive information from remote locations. VPNs provide secure channels of communication that will help keep their data safe during transmission.

Domain Name System

Enables businesses to communicate with the cloud services by resolving the IP address of websites to readable domain name such as google.com instead of 8.8.8.8 IP address. Thanks to the domain name system, it allows for seamless access to cloud applications and/or services.

Storage Providers

AWS Storage Gateway: Combines on-premises systems with cloud storage, allowing access to AWS cloud data while enabling offline caching.

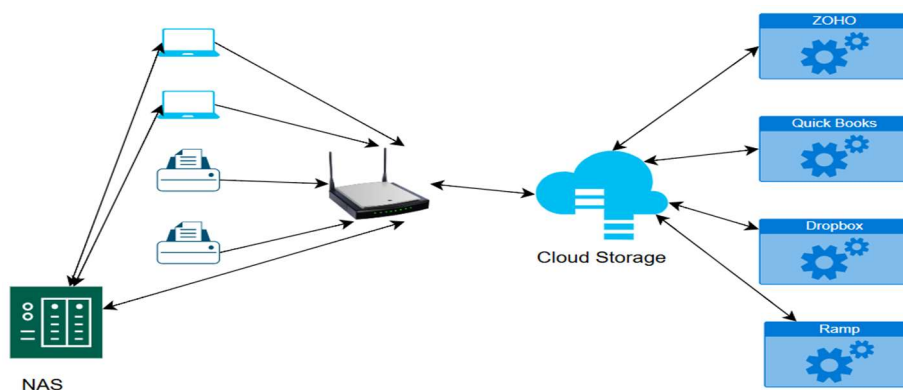
ZOHO workplace: Cost effective that offers email hosting and cloud storage. Since the company already uses Zoho resources, incorporating its storage would be easier and give a sense of familiarity. Also offer a variety of different plans.

Google Workspace: Provides different customizable storage needs. Allow file sharing and real-time editing. Easy to integrate with google features and applications. Provides offline access and file synchronization across devices. Also has advance security with data loss prevention and encryption.

Content Delivery Network

CDN stores copies of content on servers located in multiple locations worldwide. When a user requests content, it is delivered from the server closest to their physical location, reducing the time it takes for data to travel over the internet. CDNs use advanced routing techniques and algorithms to find the fastest and most efficient path for delivering content.

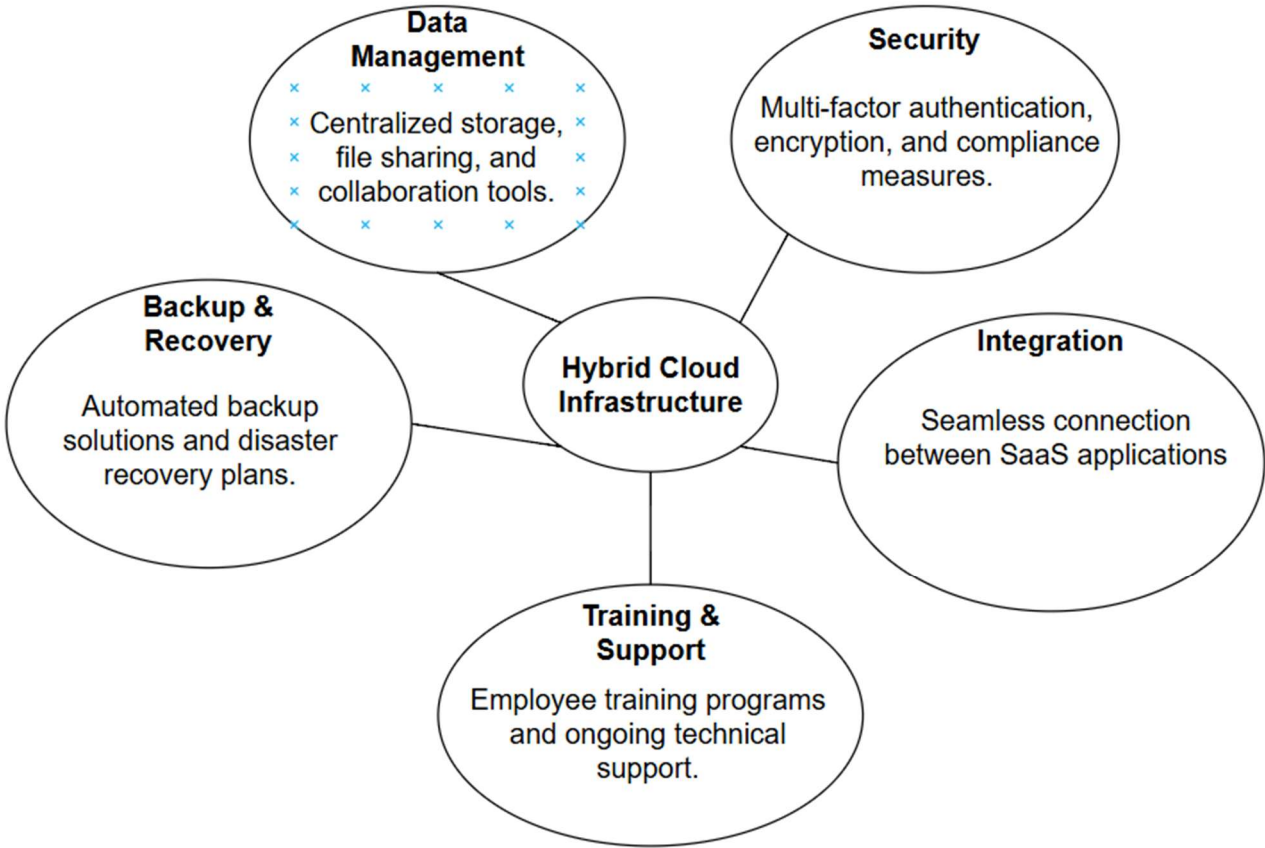
Updated Infrastructure Diagram



Research

Key Stakeholders	Mathew Forsyth
Single Point of Contact for each department	Mathew Forsyth
SPOC for the organization	Mathew Forsyth

Framework Diagram



Baseline

The current environment relies on SaaS tools (e.g., QuickBooks, Zoho) and basic cloud storage (Dropbox), which meets basic needs but lacks scalability and redundancy. Data retrieval speed: Moderate due to reliance on direct internet access. Collaboration: Limited to basic file sharing without advanced real-time editing tools.

Feasibility

Capabilities to Migrate to the Cloud:

Existing familiarity with SaaS tools like Zoho.

Moderate internet speeds (100 Mbps download, 30 Mbps upload).

Capabilities to Offload to the Cloud:

File storage, project management, and collaboration tools.

Data backups and disaster recovery systems.

Gap Analysis

Business: Mathew Made Construction currently uses a decentralized file storage system, which makes it difficult for employees to access information quickly and collaborate effectively. The goal is to implement a centralized hybrid cloud storage solution that streamlines data access and enhances collaboration.

People: The workforce has limited training on advanced cloud tools, which prevents them from fully utilizing new technologies. The desired future state is to provide comprehensive training programs that equip employees with the skills needed to effectively use cloud solutions.

Platform: The company relies on basic SaaS tools that do not integrate well with each other, leading to inefficiencies. The aim is to adopt an integrated cloud platform that allows for seamless data sharing and collaboration across applications.

Security: Current security measures are basic, relying mainly on passwords, which are not sufficient to protect sensitive data. The desired future state includes implementing advanced security measures like multi-factor authentication (MFA) and encryption to better safeguard data.

Operations: Operations involve manual backups and recovery processes, which are time-consuming and risky. The goal is to automate these processes using cloud technologies to improve efficiency and ensure data is protected and easily recoverable.

Gap Analysis Diagram

Category	Current State	Goal	Action Needed	Priority	Owner	Due Date
Business	Decentralized file storage and limited tools.	Centralized storage and advanced tools.	Implement hybrid cloud infrastructure.	High	Mathew Forsyth	July 2025
People	Limited training on advanced cloud tools.	Skilled workforce for cloud-based operations.	Provide cloud training programs.	medium	Mathew Forsyth	August 2025
Governance	Lack of formal governance policies and procedures	Established governance framework for cloud usage	Develop and implement governance policies	High	Mathew Forsyth	July 2025
Platform	Basic SaaS tools with no integration.	Integrated cloud platform.	Adopt scalable SaaS and IaaS solutions.	High	Mathew Forsyth	June 2025
Security	Basic security measures (passwords).	Advanced security (MFA, encryption).	Implement IAM and MFA policies.	High	Mathew Forsyth	May 2025
Operations	Manual backups and recovery processes.	Automated backups and disaster recovery.	Use AWS or Google Workspace tools.	Medium	Mathew Forsyth	July 2025

Capital and Operating Expenditures

Capital Expenditure

On-premise infrastructure: If Mathew Made Constructions decides to go with the hybrid model they would need maintain and purchase the storage, that includes the hard drives and the NAS unit itself.

Backup Power Supply: Ensures uninterrupted operations in case of power failures, which is crucial for storage and networking equipment.

Operational Expenditure

Cloud Storage subscription: Ensure that payment is set up for recurring cost of services used like Google Drive, AWS S3, or Zoho WorkDrive

Software Licensing Fees: When it comes to using different software like Zoho, Dropbox, or Clockify the usually come with monthly or annual fees

Potential Cloud Vendors

Zoho WorkDrive
Google Cloud Platform
AWS S3

These vendors were chosen because of their hybrid cloud support, security features, and integration with SaaS (Software as a Service) applications already being utilized by Mathew Made Construction.

Licensing Model

Per-User Licensing: SaaS tools like Zoho and Google Workspace charge a per-user fee, making it easy to scale costs as the company grows.

Pay-as-you-go Model: AWS and GCP offer on-demand pricing for storage, allowing flexibility in cloud usage.

Evaluation of Cloud Vendors

Proof of Value

Feature	Zoho WorkDrive	AWS S3	Google Cloud Storage
Cost	Lower	Pay-as-you-go	Pay-as-you-go
Integration	Best with Zoho	Broadest support	Best for Google apps
Collaboration	Strong	Limited	Strong (Google Docs)
Security	High	Enterprise-level	High
Offline Access	Yes	No (without third-party tools)	Yes (Drive Sync)
Scalability	Moderate	High	High

Service Level Agreement

AWS SLA:
Uptime: 99.99% for storage and compute services.
Compensation: Credits are issued based on downtime duration.

GCP SLA:
Uptime: 99.95% for standard services.
Compensation: Service credits provided for any outage exceeding agreed levels.

Zoho WorkDrive:
Uptime: 99.9% uptime commitment across its cloud applications.
Compensation: Does not offer service credits or financial compensation for unplanned outages.

Migration Principles

Data Integrity and Security
Ensuring data integrity during migration is crucial. Encryption will be used for data in transit and at rest, and backup copies will be maintained to prevent data loss.

Hybrid Cloud Transition
Since the company is adopting a hybrid cloud model, a step-by-step integration with existing on-premises infrastructure will need to be implemented. Cloud storage and applications will be gradually introduced to ensure on-premises and cloud environments are working.

Aspects of Operating

Data Management: Replication, Locality, and Backup	To ensure the data's availability and integrity, we will need to put in place data replication across different regions. The data will also need to have regular automated backups in place to help protect against data loss.
Availability: Zone & Geo-Redundancy	Cloud services will be distributed across multiple availability zones within a region, ensuring minimal downtime in case of failures. Critical data and applications will be stored in different regions to improve disaster recovery capabilities
Disposable Resources	the company will leverage auto-scaling and containerization strategies to deploy resources dynamically. Containers will then be used to help manage workloads that will allow quick replacements in case components fail to ensure service continuity.
Monitoring and Visibility: Alerts & Logging	Comprehensive monitoring will be implemented using cloud-native tools such as Google Cloud Operations Suite. These tools will generate real-time alerts for performance issues, unauthorized access attempts, and system failures.
Optimization: Auto-scaling & Right-Sizing	Auto-scaling mechanisms will dynamically adjust computing resources based on workload demand, ensuring cost-efficiency while maintaining performance. Right-sizing recommendations from cloud providers will be followed to optimize instance types and storage capacities, preventing over-provisioning and reducing wasteful expenditures.

Financial Planning

Infrastructure: Compute, Storage, and Networking

To integrate Google Drive with a local NAS (Network Attached Storage) device, storage infrastructure will be configured for seamless synchronization. Google Drive will serve as the cloud-based repository for active projects and collaboration, while the NAS will act as local backup storage to ensure data availability during internet outages. Cloud compute resources will be optimized by using lightweight virtual machines for remote access and processing, ensuring cost-effectiveness. Network configurations will prioritize secure VPN connections between cloud and on-premise storage for smooth data transfer.

Chargebacks: Resource Tagging

Resource tagging will be implemented to track cloud expenditures by project, department, or cost center. This will enable detailed financial reporting, allowing the company to optimize spending and allocate costs accurately.

Instances: Reserved and Spot

A combination of reserved instances (for predictable workloads) and spot instances (for cost-saving on flexible workloads) will be used to optimize cloud expenses. Reserved instances will provide cost savings for long-term usage commitments, while spot instances will be leveraged for non-critical, scalable tasks.

Data Sovereignty

Data sovereignty refers to the laws and regulations that govern data based on the country in which it is stored. For Mathew Made Construction, this means ensuring that cloud-stored data complies with U.S. regulations and Utah state-specific requirements. Using cloud services must include considerations for data residency, access controls, and compliance with federal and industry standards.

Regulatory Concerns

The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies. Cloud Service Providers (CSPs) seeking to work with government entities must meet FedRAMP security requirements, ensuring compliance with NIST 800-53 controls.

The Federal Information Security Management Act (FISMA) applies to federal agencies and contractors handling government data. Businesses working with federal agencies must adhere to FISMA requirements, ensuring security controls, risk management, and reporting standards are met. Mathew

Made Construction must ensure that its cloud vendors align with FISMA-compliant services if working with federal projects.

The Federal Information Processing Standards (FIPS) define cryptographic standards for securing sensitive but unclassified information. Cloud storage solutions used by Mathew Made Construction should be FIPS-compliant to protect project blueprints, financial data, and communications.

Industry-Based Requirements

The Financial Industry Regulatory Authority (FINRA) mandates record retention requirements for financial institutions. FINRA Rule 4511 ensures that businesses keep financial records for regulatory audits. If Mathew Made Construction were to expand into publicly funded projects requiring financial documentation, cloud storage solutions should support FINRA-compliant retention policies.

The Sarbanes-Oxley Act (SOX) enforces corporate accountability and transparency, requiring strict financial record-keeping. While Mathew Made Construction is not publicly traded, if it grows into a larger enterprise seeking public investment, SOX compliance would be necessary to maintain financial integrity and prevent fraud.

While the Motion Picture Association of America (MPAA) is primarily for digital content protection, similar principles apply to Mathew Made Construction's intellectual property, including proprietary blueprints, designs, and bids. The company must:

- Use watermarking and access control for shared documents.
- Encrypt intellectual property stored in the cloud.
- Restrict access to project files only to authorized employees and contractors.

Certifications

The CIA triad (Confidentiality, Integrity, Availability) applies to cloud-stored construction documents and financial records:

Confidentiality – Use encryption and access controls to protect sensitive project data.

Integrity – Ensure file versioning and backup policies prevent unauthorized alterations.

Availability – Use redundant cloud storage (e.g., AWS, Google Drive) to ensure uninterrupted access to project files.

Security Concerns, Measures, and Concepts

Security concerns include data breaches, unauthorized access, and downtime risks. Measures include:

- MFA for all cloud accounts.
- Encryption for stored and transmitted data.
- Regular security audits and access monitoring.

Example of a threat and how to identify one in Mathew Made Construction.

A phishing attack targeting employees with fake login pages could compromise cloud storage credentials. To identify:

- Train employees to recognize suspicious emails.
- Use email filtering and authentication tools.
- Enable MFA to prevent unauthorized logins.

A threat is a potential attack (e.g., hackers targeting construction contracts).

A vulnerability is a weakness that makes the threat possible (e.g., using weak passwords for cloud accounts).

Primary tools for security assessment for Mathew Made Construction.

Google Security Center

Purpose: Identifies security risks in Google Workspace, Drive, and Gmail.

Use Case: Detects unauthorized access, phishing emails, and data sharing risks in cloud storage.

Penetration Testing

Purpose: Simulates cyberattacks to find security weaknesses in cloud systems.

Use Case: Tests Google Drive and VPN security to prevent unauthorized access.

Wireshark

Purpose: Network traffic analysis.

Use Case: Ensures secure data transmission between office networks and cloud storage

CrowdStrike Falcon

Purpose: Endpoint protection against malware and ransomware.

Use Case: Protects office desktops, laptops, and mobile devices used to access cloud storage from cyber threats.

Three categories for data security and their meaning for Mathew Made Construction.

- Data at Rest – Encrypt stored project files on Google Drive.
- Data in Transit – Use VPNs and HTTPS for secure file transfers.

- Data in Use – Restrict access to only necessary employees.

Difference between access and authorization for Mathew Made Construction.

Access – Determines who can log in (employees, contractors).

Authorization – Determines what actions they can perform (e.g., viewing vs. editing blueprints).

Risk Assessment

The Company Assets

Printer, laptops, and mobile devices

Network Devices (Gateway/router, NAS)

Project blueprints and physical construction plans

Cloud-stored files (project documents, contracts, financial data)

Customer and vendor databases

Qualitative Risks associated with the Mathew Made Construction

Data Breach (**Critical** level 5) - Unauthorized access to client and project data.

Downtime due to ISP failure (**Medium** level 3) - Inability to access cloud-stored data.

Ransomware attack (**Critical** level 5) - Encryption of crucial files leading to financial and operational loss.

Loss of intellectual property (**Medium** level 3) - Unauthorized access to proprietary blueprints.

Compliance Violation (**High** level 4) - Failure to meet regulatory standards, leading to penalties.

Risk/Asset Owner: Mathew Forsyth (Company Owner/Manager)

Risk Response

Risk Response Definition

Risk response involves the strategic approach Mathew Made Construction takes to identify, mitigate, accept, avoid, or transfer risks associated with its cloud infrastructure and data security.

Mitigation Strategies (Current and Suggested)

- Multi-Factor Authentication (MFA) for all cloud applications.
- Regular Backups using Google Drive to prevent data loss.
- Employee Cybersecurity Training to reduce phishing and social engineering attacks.
- Firewall & Endpoint Protection to monitor and prevent malicious activity.

Risk Acceptance

Some risks, such as minor service disruptions or vendor dependency, may be accepted as long as they don't critically impact operations.

Risk Avoidance as a Preferred Response

Avoiding risks through proactive security measures ensures business continuity and reduces potential threats before they arise. If there is no threat or vulnerability, which is great because that better ensures the safety of the company's assets.

Cloud and Risk Transference

The reason the using the cloud is an example of risk transference is because the responsibility of risk management is taken on by the CSP based on the service being used. Instead of investing in security measures and hardware maintenance the company can instead relies on the CPS's expertise to reduce operational risks.

Documentation

A few of the reasons that documentation is vital in the IT world is because:

- Ensures consistency – Provides a clear reference for system configurations, policies, and troubleshooting procedures.
- Aids in compliance – Helps meet industry regulations and security standards.

A few examples are:

- Identify when there is misconfigured cloud storage leads to unauthorized access.
- Lack of audit logs to track user activities, making compliance verification difficult

Policies and Procedures

Data Privacy and Impact:

Mathew Made Construction must protect client contracts, financial records, and blueprints from unauthorized access. A data privacy policy ensures:

- Employee access is restricted to relevant files only using Google Drive permissions.
- Encryption and multi-factor authentication (MFA) secure sensitive project data.

Two Important Policies for the Company:

- Access Control Policy – Employees access only necessary files, reducing exposure to security risks.
- Backup and Disaster Recovery Policy – Google Drive automatic backups ensure quick recovery from accidental deletions or cyberattack

Change and Resource Management for Mathew Made Construction

Changes in cloud storage usage should be reviewed to avoid unnecessary costs.

Managing resources efficiently (e.g., removing inactive user accounts) ensures that only authorized employees access sensitive data.