

NAME : CHIDOKORI PRIMROSE

REG NUMBER : C23156755R

PROGRAMME : BSIT

MODULE : CUPEM309

ASSIGNMENT 2

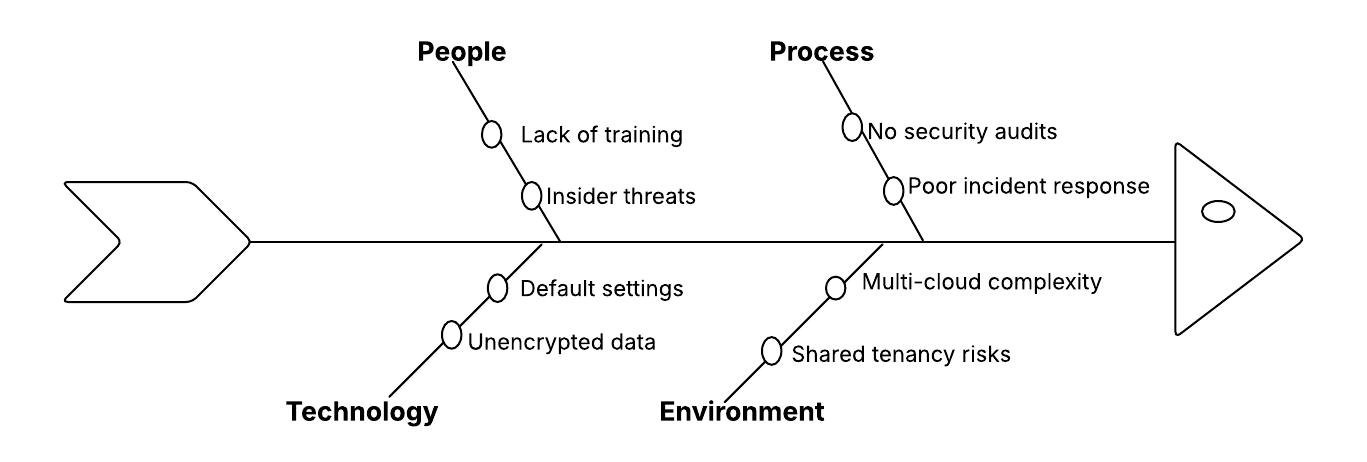
Step 1: Identify the Problem

There is frequent data breaches and compliance violations in cloud environments due to misconfigurations for example: exposed storage, weak access controls, leading to unauthorized access and financial losses.

Evidence: 80% of cloud breaches stem from misconfigured settings (IBM Security).

Example: Capital One breach (2019) due to AWS S3 bucket misconfiguration.

Step 2: Possible Causes (Fishbone Diagram)



Distribution graph

The main cause is people because they lack knowledge to secure the data.

Step 3: Possible Solutions

1. Automate Security: Tools like Amazon Web Services Configuration, Prisma Cloud.

2. Adopt Zero Trust: Least-privilege access, Multi-Factor Authentication (MFA).

3. Encrypt Data: Enable Transport Layer Security (TLS) 1.3, AES-256 encryption.

4. Train Staff: Regular phishing simulations, cloud security certifications.

Step 4: Decision Matrix

(Scale: 1-5)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Solution | Cost (1=Low) | Impact (1=Low) | Ease (1=Hard) | Total |
| Automate Scanning | 3 | 5 | 4 | 12 |
| Zero Trust Policies | 2 | 5 | 3 | 10 |
| Encryption | 4 | 4 | 2 | 10 |
| Training | 1 | 3 | 5 | 9 |

Result: Prioritize automation (highest impact) and zero trust.

Step 5: Implementation (Gantt chart)

| Task | Q1 (Weeks 1-4) | Q2 (Weeks 5-8) | Q3 (Weeks 9-12) |

|---------------------------|---------------------------|----------------------------|--------------------------|

| Risk Assessment | ██████████ | | |

| Deploy Scanning | | ██████████ | |

| Update IAM Policies | | ██████ | ██████ |

| Employee Training | | | ██████████ |

Step 6: Evaluation

Metrics to Monitor:

(i)Reduction in misconfigurations (monthly scans).

(ii)Number of unauthorized access attempts (SIEM logs).

(iii)Compliance audit results (e.g., GDPR/HIPAA).