**Approach to evaluate internal organizational structures, IT infrastructure, security measures, and risk mitigation strategies**

#### 1. Introduction

This document helps us - Expert Cloud Consulting in evaluating customers Organization structure for Cloud and DevOps project to facilitate the Risk and mitigations in the early stages of the projects.

**Objective**:  
To assess the current organization structure for potential risks and define mitigation strategies before initiating AWS Cloud & DevOps projects.

**Scope**:  
This assessment covers the evaluation of IT infrastructure, security measures, and risk mitigation strategies.

**Audience**:  
IT Directors, VP-IT, Engineering Head, Product Managers, Project Managers, IT Administrators, Security Officers, and other stakeholders as applicable.

#### 2. Current State Assessment

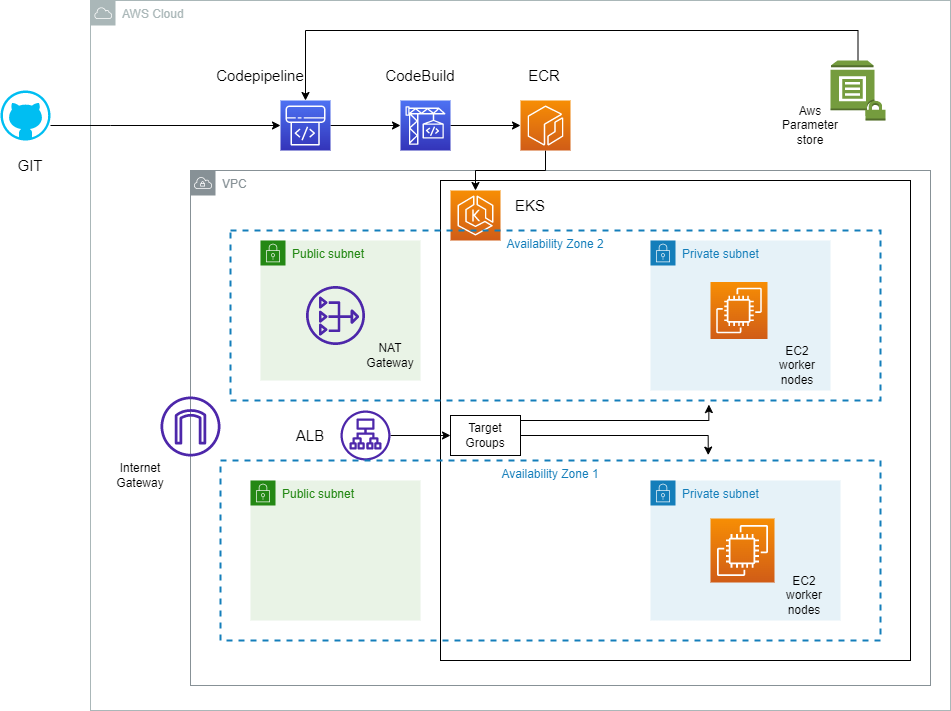
**Organization Overview**:

* Name: [Organization Name]
* Industry: [Industry]
* Size: [Number of Employees]
* Organization Structure chart [Obtain the high level org Chart for applicable departments/teams]

**IT Infrastructure**:

* Overview of existing hardware and software [Describe the scale and size of current IT landscape]

Sample cloud architecture for ready reference:



* Network architecture [high level architecture diagrams expected]
* Application/Server Architecture [high level architecture diagrams expected]
* Cloud services in use [high level architecture diagrams expected]

**Existing Projects / Programs and Workflows**:

* List of ongoing IT projects and Programs.
* Current development workflows

**Current Security Measures**:

* Data protection policies [List the name of the existing policies]
* Access control mechanisms [List both physical and logical access controls for data assets]
* Incident response plans [Should capture SLA’s at a minimum]

**DevOps projects related Measures:**

Conduct detailed assessment to capture current state related to below DevOps categories as per the template here - <https://docs.google.com/spreadsheets/d/1oxzrQ6DYXE6Ydk7Yhe-Fx5wQwRQgRll1/edit?gid=403510460#gid=403510460>

**Categories** to be covered as per the template above are -

* Collaboration and communication
* Agility and empowerment
* Automation and tooling
* CI/CD capabilities
* Cross-functional integration

#### 3. Risk Identification

**Data Security Risks**:

* Unauthorized access [Capture the level of exposure - High, Medium and Low with details as applicable]
* Data breaches [Capture details of the last 3 severe incidents,if applicable]
* Data loss [Capture details of the last 3 severe incidents, if applicable]

**Compliance Risks**:

* Non-compliance with regulations (e.g., GDPR, HIPAA, SOX, PCI)
* Audits and penalties [Capture details of the last 3 occurrences, as applicable]

**Operational Risks**:

* System downtimes [Capture details of the last 3 occurrences, as applicable]
* Dependency on third-party services [Capture details of the last 3 occurrences, as applicable]

**Financial Risks**:

* Cost overruns [Capture details of the last financial year or at least last 2 quarters at high level]
* Budget constraints

**Human Resource Risks**:

* Skill gaps [Capture gaps in key areas]
* Employee turnover [If possible capture per person revenue]

**DevOps Projects Risks:**

* Collaboration and communication [Current set of tools, & processes]
* Agility and empowerment [Current set of tools, & processes]
* Automation and tooling [Current set of tools, & processes]
* CI/CD capabilities [Current maturity of the cicd pipelines, approvals & version controlling]
* Cross-functional integration [Capture current effectiveness, timelines, delays to release application features, time to market and associated processes]

#### 4. Risk Analysis

Rank the below risks basis details obtained from customers. Below is a sample table for reference.

| **Risk** | **Likelihood (High/Medium/Low)** | **Impact (High/Medium/Low)** | **Priority (High/Medium/Low)** |
| --- | --- | --- | --- |
| Unauthorized access | High | High | High |
| Data breaches | Medium | High | High |
| Non-compliance | Medium | Medium | Medium |
| System downtimes | Low | High | Medium |
| Cost overruns | Medium | Medium | Medium |

#### Risk Analysis for DevOps Projects

Rank the below risks basis details obtained from customers. Below is a sample table for reference.

| **DevOps Project Category** | **Risk** | **Likelihood (High/Medium/Low)** | **Impact (High/Medium/Low)** | **Priority (High/Medium/Low)** |
| --- | --- | --- | --- | --- |
| Collaboration and Communication | Lack of communication between teams | High | High | High |
| Collaboration and Communication | Poor collaboration tools | Medium | High | High |
| Collaboration and Communication | Inadequate feedback mechanisms | Low | Medium | Medium |
| Agility and Empowerment | Slow response to changes | High | High | High |
| Agility and Empowerment | Lack of empowerment | Medium | High | High |
| Agility and Empowerment | Inefficient agile processes | Low | Medium | Medium |
| Automation and Tooling | Outdated tools | High | High | High |
| Automation and Tooling | Manual processes | Medium | High | High |
| Automation and Tooling | Infrequent deployments | Low | Medium | Medium |
| CI/CD Capabilities | CI/CD pipeline failures | High | High | High |
| CI/CD Capabilities | Bottlenecks in CI/CD | Medium | High | High |
| CI/CD Capabilities | Unsuccessful builds and deployments | Low | Medium | Medium |
| Cross-Functional Integration | Silos between departments | High | High | High |
| Cross-Functional Integration | Hindered cross-functional collaboration | Medium | High | High |
| Cross-Functional Integration | Lack of cross-functional initiatives | Low | Medium | Medium |

#### 5. Mitigation Strategies

**Preventive Measures**:

* Implement robust access controls [Arrive at the list of controls as applicable]
* Regular security training for employees [Identification of the need of training areas for processes and technology]

**Detective Measures**:

* Continuous monitoring [Arrive at recommended monitoring tools, technology and process at high level]
* Regular security audits [Suggest Frequency, Auditing Authority/Vendors, and expected compliance levels]

**Corrective Measures**:

* Incident response plans [Gaps to fix the expected incident response times, as applicable]
* Data backup and recovery solutions [Validate and suggest basis the companies RTO and RPO objectives]

**Risk Transfer**:

* Insurance policies [Ensure appropriate Risk Coverage]
* Outsourcing certain operations [Risk Transfer ]

#### 6. Recommendations

**Short-term Actions**:

* Conduct immediate security audit [Risk Evaluation plan, and frequency]
* Implement MFA for all critical systems [Risk Mitigations]

**Long-term Actions**:

* Develop a comprehensive security policy [Inputs to enhance current security policy]
* Regularly update and patch all systems [Inputs to enforce the security measures]

**Tools and Technologies**:

* AWS Security Hub [leverage necessary tools]
* Terraform for infrastructure as code [Suggest version controlled and approved code and roll back mechanisms]
* CI/CD pipelines with Jenkins [Suggest automation to avoid human errors and increase efficiencies]

#### 7. Implementation Plan

Arrive at the detailed roadmap and schedule with customers for necessary approved budget, skill enhancements, vendor engagements, risk coverage and for agreed risk and compliance projects. Below is the sample high-level example for reference.

**Roadmap**:

* Q1: Initial security audit and quick fixes
* Q2: Implement MFA and access controls
* Q3: Develop and deploy comprehensive security policy

**Resource Allocation**:

* Security team: 2 FTEs
* DevOps team: 3 FTEs

**Timelines**:

* Initial assessment: 2 weeks
* Short-term actions: 1 month
* Long-term actions: 6 months

#### 8. Conclusion

**Summary**:  
The assessment highlights key risks in data security, compliance, and operations. Immediate actions and long-term strategies have been recommended to mitigate these risks.

**Next Steps**:

* Approval from stakeholders
* Kick-off meeting for implementation
* Regular progress reviews and updates