CLOUD4C
A CtrlS Company

Risk Acceptance Communication to Cloud4C customers

At Cloud4C, security is our top priority. We understand the importance of transparency and collaboration with our Cloud Service Tenants (CSTs). This document outlines a framework for defining acceptable risk levels, adhering to the National Cybersecurity Authority (NCA) of Saudi Arabia's Cloud Cybersecurity Controls (CCC) control 1-2-P-1-1, and empowering you to make informed decisions about cloud security within your environments.

Shared Responsibility and NCA CCC Compliance

The cloud security landscape operates under a shared responsibility model. We, the CSP, are responsible for the security of the underlying infrastructure. However, you, the CST, are responsible for securing your data, applications, and access controls within the cloud services you use. NCA CCC control 1-2-P-1-1 emphasizes the importance of defining acceptable risk levels for these cloud services.

Defining Your Acceptable Risk Levels

Here's a simplified approach for you, the CST, to define acceptable risk levels for your cloud deployments, following NCA CCC control 1-2-P-1-1:

1. **Identify Cloud Assets:** Catalog the cloud services you use (hosted by us) and the data they store. Classify this data based on its sensitivity (Highly Sensitive, Moderately Sensitive, Public).
2. **Consider Potential Threats:** Familiarize yourself with common cloud security threats relevant to your industry, such as unauthorized access, data breaches, and service disruptions.
3. **Evaluate the Impact:** Assess the potential consequences of a successful attack on each data category. Consider factors like financial loss, reputational damage, and regulatory non-compliance.
4. **Set Your Risk Tolerance:** Based on the impact assessment, determine your acceptable risk level for each data category (Low, Medium, High). This reflects your willingness to tolerate certain risks.

Sample Risk Acceptance Levels

Data Category	Example Data	Acceptable Risk Level
Highly Sensitive	Financial records, Personally Identifiable Information (PII)	Low
Moderately Sensitive	HR documents, customer purchase history	Medium
Public Data	Non-confidential marketing materials	High

Collaboration with Your Security Team

- **Prioritize Security Efforts:** Focus resources on implementing controls that mitigate risks exceeding your acceptable tolerance levels, aligning with NCA CCC control 1-2-P-1-1.
- **Develop Secure Configurations:** Ensure secure configuration of access controls, encryption settings, and other security features within your cloud services.

Risk Letters Based on NCA CCC Alignment

Based on your specific cloud deployments, we at Cloud4C will generate **Risk Letters**. These letters will outline:

- Identified risks
- Your organization's chosen risk acceptance levels, aligned with NCA CCC control 1-2-P-1-1 (to the best of our knowledge based on your cloud usage)

These Risk Letters will be shared with your organization's designated contact to ensure complete transparency and alignment with NCA CCC requirements.

Transparency and Communication

We are committed to open communication with our CSTs. If you have any questions or require further information regarding risk management practices or NCA CCC compliance, please do not hesitate to contact us.