Control Environment Narrative

Beyond

August 2023

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC2.1, CC2.2, CC2.3, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3

Table 2: Document history

Date	Comment
Aug 14 2023	Initial document
Aug 18 2023	Initial review

1 Control Environment Narrative

The following provides a description of the control structure of Beyond.

The intent of this description is to enumerate the logical, policy, and procedural controls that serve to monitor Beyond's application and data security. Changes uncovered by these procedures in the logical, policy, procedural, or customer environment are addressed by remediations specific to the noted change.

2 Logical Controls

Beyond employs several logical controls to protect confidential data and ensure normal operation of its core product.

- Mandatory data encryption at rest and in motion
- Multi-factor authentication for access to cloud infrastructure
- Activity and anomaly monitoring on production systems
- Vulnerability management program

3 Policy Controls

Beyond employs several policy controls to protect confidential data and ensure normal operation of its core product. These policies include, but are not limited to:

- Access Control Policy
- Encryption Policy
- Password Policy
- Vendor Policy
- Workstation Policy

4 Procedural Controls

Beyond has numerous scheduled procedures to monitor and tune the effectiveness of ongoing security controls, and a series of event-driven procedures to respond to security-related events.

- User onboarding procedure
- User offboarding procedure
- Network and Application vulnerability management procedures (WIP)

4.1 Scheduled Security and Audit Procedures

- Review Access [quarterly]
- Review Security Logs [On alerts & annually]

- Review Cyber Risk Assessment (enumerate possible compromise scenarios) [annually]
- Review Data Classification [On new launches & annually]
- Apply OS Patches [quarterly]
- Conduct Security Training [annually]
- Review Security Monitoring and Alerting Configuration [quarterly]
- Third Party Penetration Test [annually]

4.2 Event-Driven Security and Audit Procedures

- Onboard Employee
- Offboard Employee
- Investigate Security Alert
- Investigate Security Incident

5 Remediations

Beyond uses the outcomes of the aforementioned controls and procedures to identify shortcomings in the existing control environment. Once identified, these shortcomings are remediated by improving existing controls and procedures, and creating new controls and procedures as needed.

6 Communications

Beyond communicates relevant information regarding the functioning of the above controls with internal and external parties on an as-needed basis and according to statutory requirements.

6.1 Internal

Beyond communicates control outcomes, anomalies, and remediations internally using the following channels:

- Slack
- Email
- Jira ticketing

6.2 External

Beyond communicates relevant control-related information to external parties including shareholders, customers, contractors, regulators, and government entities as needed according to contractual and regulatory/statutory obligation.