Third Party Risk Management Life Cycle

Note:

- TPRM team uses Sure Cloud Tool for the purpose of assessments.
- When the assessment will be initiated Supplier and Business will receive mail from Sure cloud to create their accounts on Sure cloud to be able to work on assessment .
- Once the account is created Supplier will be able to update the assessments responses.
- Requesters will be receiving Automated notifications from Infosec.vrm @Unilever.com for any reminders or after completion of tasks assigned.
- Business Owner will be copied in all the communications sent to supplier, however there would be no action required from them.
- A dedicated TPRM owner is assigned to you throughout the assessment cycle, for any help or query you can reach out to the TPRM owner directly or drop an email at InfoSec.vrm@unilever.com.

Roles and Responsibilities in TPRM process

Unilever Business Owner

1. Define and share the complete scope of the service with the TPRM team. This will form the basis of the initiation of the TPRM assessment.
2. Any incomplete or incorrect information shared at the time of assessment is the sole responsibility of Business Owner.
3. If the TPRM team receive no response from the supplier in relation to the assessment and supporting evidences, the Business Owner need to aid for the assessment to be completed.
    - If no response to identified vulnerabilities is received within 7 working days, this is to be escalated to the supplier.
4. At any point of time if there is any change to the scope of service the supplier provide to Unilever, the Business Owner need to inform the TPRM team.

Supplier

1. Supplier must ensure the assessment timelines for the TIA process is followed.
2. All Suppliers engaged by Unilever are required to report:
    - Actual and/or confirmed breaches, or compromises affecting
    - Unilever data, or environments where
    - Unilever data is stored and/or processed.
3. The Supplier must directly inform Unilever's ISOC (Intelligent Security Operations Centre) of any incidents or investigations affecting Unilever systems or data within the agreed timelines (stated in the contract).
    - ISOC team must be contacted via email and a supporting phone call using the contact details provided in the below guidelines (also included in the contract)
4. Unilever expects all Suppliers to conduct their investigations in line with their own formally documented procedures.

Guidelines for Reporting Cyber Security Incident

1. Supplier must directly inform the Unilever's ISOC team via email and a supporting phone call using the contact details provided below.
    - Unilever's ISOC (Intelligent Security Operations Centre) at E-mail: ISOC@unilever.com
    - Landline: +91 803 915 0065 / +91 803 915 0066
    - Mobile: +91 734 928 1716 / +91 734 928 1719
2. All emails to the ISOC team must have a Subject line that starts with the words "SUPPLIER NOTIFICATION "and include the supplier's normal Unilever business relationship owner in the CC field

For queries contact: Infosec.VRM@unilever.com

Unilever