Minimum Requirements for Third Parties During Assessment

Third Parties are required to have the following minimum requirements fully implemented at the time of assessment. These requirements are considered high risk and are essential for ensuring compliance and safeguarding all relevant interests throughout the evaluation process.

You may send the Excel file titled "MinimumRequirements_TP" to inquire whether the Third Party can provide this information.

1. If this is not present at the time of assessment, this automatically results in an **Unsatisfactory** status:
    - A current independent audit report such as HiTrust (i1 or r2), SOC 2 Type II, ISO 27001, FISMA, or FedRamp is available at the time of evaluation. ***Important***: independent audit reports provided by cloud vendors including AWS, Google, Azure, or Salesforce are not accepted as substitutes for the third party's own independent audit report.

2. If any of these are not present at the time of assessment, the outcome will be either **Unsatisfactory** or **Satisfactory with Findings**, based on the quantity of missing controls.
    - Results of your last business continuity exercise.
    - Results of your last disaster recovery exercise.
    - Evidence for your security awareness program.
    - Technical evidence that IDS/IPS is in place.
    - Technical evidence that TLS 1.2 or greater is leveraged.
    - Technical evidence that AES-256 is leveraged.
    - Technical evidence that Data Loss Prevention (DLP) on endpoints is in place to protect sensitive information.
    - Technical evidence that the Web Application Firewall (WAF) is in place.
    - Technical evidence of a recent application penetration test result.
    - Technical evidence of a recent network penetration test result.
    - Technical evidence of Dynamic Application Security Testing (DAST).
    - Technical evidence of Static Application Security Testing (SAST).