Privacy and Security

Threat and Risk Assessment Checklist

October 30, 2023

Document Version and Status: 1.1 – Final

1. CHECKLIST

This document is a list of information required when submitting a threat and risk assessment (TRA) report.

Information to Include	**Document Mapping (from vendor's substantiation)** Page # and/or section name is required, where applicable
Auditor Information	
Organization Name	
Full Name	
Certification Type	
License or Certification #	
Section 1.0: Executive Summary	
Executive Summary	
Classification of Information	
Statement of Sensitivity (SoS) Summary	
Asset Summary	
Key Findings	
Key Recommendations Methodology	
Section 2.0: Introduction	
Background	
Description of business line and operating environment	
Service delivery levels relevant to the TRA	
Legislated or regulated	
Service agreement	
The rationale for the assessment	
In-scope	
Out of scope	
Limitation	

Information to Include	Document Mapping (from vendor's substantiation) Page # and/or section name is required, where applicable
Section 3.0: Systems Information	
System Description	
Business Architecture	
Group and Role Components	
Information Systems Architecture	
Application Components	
Middleware Components	
Data Components	
Technology Architecture	
Server Components	
Storage Components	
Network Components	
Security Controls a) Information Security Policies b) Security Governance c) Asset Management d) Personnel Security e) Media Handling f) Identity and Access Management (IAM) g) Systems Access h) Physical Security i) End-point Security j) Backup Management k) Network Security l) Vulnerability Management m) Application Security n) Third-party Risk Management o) Business Continuity p) Security Incident Management	
Section 4.0: Statement of Sensitivity	
High-level summary of the Statement of Sensitivity	

Information to Include	Document Mapping (from vendor's substantiation) Page # and/or section name is required, where applicable
The detailed Statement of Sensitivity is in Appendix D	
Section 5.0: Asset Summary and Threat Summary	
Capture in-scope assets	
External threat agents	
Internal threat agents	
Threat assessment	
Section 6.0: Risk Assessment	
Vulnerability Assessment (not the same as the Technical Vulnerability Assessment Scan)	
Safeguard Assessment	
Residual Risk Assessment	
Section 7.0: Recommendations	
Recommendations	
Risk Description	
Adjusted Residual Risks	

2. CHECKLIST APPENDICES

Information to Include	Document Mapping (from vendor's substantiation) Page # and/or section name is required, where applicable
Appendix A: Statement of Acceptable Risk	
Statement of Acceptable Risk *List the potential threats to the system identified and rated by the Threat Model analysis; the rating of each, the current controls, and their rating in the system to protect against each threat.*	
Appendix B: TRA Team Composition	
TRA Team Composition	
Appendix C: STRA Work Plan	
STRA Work Plan	
Appendix D: Statement of Sensitivity	
Asset Category	
Confidentiality, Integrity and Availability (CIA) Ratings	