

Privacy and Security

Threat and Risk Assessment Checklist

August 31, 2024

Document Version and Status: 1.1 – Final



1. INTRODUCTION

1.1 Overview

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

1.2 Version History

VERSION	REVISION DATE	REVISION NOTES
1.0	2023-10-30	Initial release
1.1	2024-08-31	<ul style="list-style-type: none"> a) Added Introduction section and version history b) Simplified section numbering c) Added Appendix E: Statement of Sensitivity d) Added Appendix F: Vulnerability Assessment Table e) Added Appendix G: Residual Risks

2. CHECKLIST

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or section name is required, where applicable
Auditor Information	
Organization Name	
Full Name	
Certification Type (e.g., CISSP, CISA)	
License or Certification #	
Section 1: Executive Summary	
Executive Summary	
Classification of Information	
Statement of Sensitivity (SoS) Summary	
Asset Summary	
Key Findings	
Key Recommendations Methodology	
Section 2: 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 Substantiation) Page No. and/or section name is required, where applicable
Section 3: 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 <ul style="list-style-type: none"> 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: Statement of Sensitivity	
High-level summary of the Statement of Sensitivity	

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or section name is required, where applicable
The detailed Statement of Sensitivity – See Appendix D	
Section 5: Asset Summary and Threat Summary	
Capture in-scope assets	
External threat agents	
Internal threat agents	
Threat assessment	
Section 6: Risk Assessment	
Vulnerability Assessment (not the same as the Technical Vulnerability Assessment Scan)	
Safeguard Assessment	
Residual Risk Assessment	
Section 7: Recommendations	
Recommendations	
Risk Description	
Adjusted Residual Risks	

3. 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 <i>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.</i>	
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	
Appendix E: Threat Assessment Table	
Asset	
Threat Agents	
Threat Event	
Likelihood and Impact	
Threat Level	
Appendix F: Vulnerability Assessment Table	
Asset	
Threats Facilitated	
Vulnerability	
Probability, severity and vulnerability analysis	

Information to Include	Document Mapping (from vendor's substantiation) Page # and/or section name is required, where applicable
Appendix G: Residual Risks	
Asset	
Asset Values	
Associate Threat	
Vulnerability	
Residual Risk Analysis	