EMR Privacy and Security

Threat Risk Assessment Checklist

December 14, 2022

Document Version and Status: 1.0 – DFC

Table of Contents

1. Overview

This document is a list of information required when submitting a TRA.

1.1 Related Documents, References and Sources

NAME	VERSION	DATE
Harmonized Threat and Risk Assessment Methodology (Government of Canada, 2022) https://cyber.gc.ca/en/tools-services/harmonized-tra-methodology	N/A	2022-05-15

2. AUDITOR INFORMATION

AUDITOR PROFILE	
Organization Name:	
Full Name:	
Certification Type:	*Note*: *Accepted certifications include CISSP and CISA. A Certified Ethical Hacker (CEH) certification is only accepted for a Penetration Test.*
Certification License Number:	

3. TRA CHECKLIST

This section identifies the information, documents and artifacts to provide to satisfy a TRA.

3.1   Section 1: Executive summary

Information to Include	Document Mapping (from Vendor's Substantiation) Page No. and/or Section Name is Required	Included?
Classification of Information		☐
Statement of Sensitivity (SoS) Summary		☐
Asset Summary		☐
Key Findings		☐
Key Recommendations Methodology		☐

3.2   Section 2: Introduction

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
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		☐
Security concerns		☐
The mandate for the Assessment		☐
In-scope		☐

Out of scope		☐
Limitation		☐

3.3 Section 3: Systems Information

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
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	

3.4 Section 4: Statement of Sensitivity

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
High-level summary of the Statement of Sensitivity		☐
The detailed Statement of Sensitivity will be in Appendix D		☐

3.5 Section 5: Asset Summary and Threat Summary

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
Capture in-scope assets		☐
External threat agents		☐
Internal threat agents		☐
Threat assessment		☐

3.6   Section 6: Risk Assessment

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
Vulnerability Assessment (not the same as the Technical Vulnerability Assessment Scan)		☐
Safeguard Assessment		☐
Residual Risk Assessment		☐

3.7   Section 7: Recommendations

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
Recommendations		☐
Risk Description		☐
Adjusted Residual Risks		☐

3.8   Section 8: 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

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
Statement of Acceptable Risk		☐

3.9   Section 9: TRA Team Composition

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
TRA Team Composition		☐

3.10 Section 10: STRA Work Plan

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
STRA Work Plan		☐

3.11 Section 11: Statement of Sensitivity

Information to Include	Document Mapping (from Vendor Substantiation) Page No. and/or Section Name is Required	Included?
a) Asset Category b) CIA Ratings	a) b)	☐