# STATEMENT OF ACCEPTABLE RISK GUIDELINES

## SECTION A – TRACKING INFORMATION

**Purpose of section:**

This section provides information needed for tracking and follow-up.

**Description of fields:**

**Assessment Reference Number** – This is a unique reference number to the ministry that the Primary Risk Evaluator creates and uses for a Security Threat and Risk Assessment (STRA). This reference number should be documented in the Statement of Acceptable Risk (SOAR) and in any supporting STRA documentation.

**System Name** – A short name that accurately describes the system that is the subject of the assessment.

**Branch & Division** – The Branch & Division of the Business Owner.

**Ministry** – The Ministry of the Business Owner.

**Contains Sensitive or Personal Information? (NO / YES)** – An acknowledgement of whether the system contains and protects sensitive or personal information. If the answer is yes it should be clear in the SOAR that the level of due diligence and assessment is commensurate to the sensitivity.

**Business Owner** – The person responsible for the delivery or operations of the system which is the subject of the assessment.

**Primary Risk Evaluator** – This is the person who has taken action to gather information, analyze, and document risks related to the system being assessed. Usually this is the Ministry Information Security Officer.

**Date supporting documentation was completed** – Provides SOAR signatories an indicator of how long a SOAR has been pending sign-off.

**Date SOAR review and sign-off is requested by** – The date which the submitter of the SOAR hopes to see review and sign-off completed by. This should reflect and support business needs.

**Critical System (NO / YES)** – Mark this as "Yes" if a system has been classified as such consistent with assessments that have already occurred as part of critical systems standard compliance, or otherwise is reasonably believed to be a critical system by the business owner.

**Description** – This field allows for context and explanation to be provided related to the system, the overall assessment, high level findings, and any noteworthy comments and recommendations that should be brought to the forefront.

## SECTION B – RISK ASSESSMENT TABLE

### Purpose of section:

This section documents the risks that were identified during the assessment.

### Instructions:

If more rows are needed copy from an existing row to keep drop-downs. If no risks are identified in the SOAR please provide a justification in the "System description, executive summary, and comments" box and reference the location of any existing related risk documentation.

### Description of fields:

**Risk Ref # -** This is a unique reference number within the STRA and SOAR for the risk.

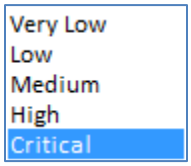
**Risk Name** – This should in a few short words portray the gist of the risk to the reader.

**Primary Risk Type** – This field is intended to help categorize the nature of the risk to help the reader better understand what the risk means to the organization.

Options are provided in a drop down for this field. Select one of these options, or clear the field and enter in your own response manually.

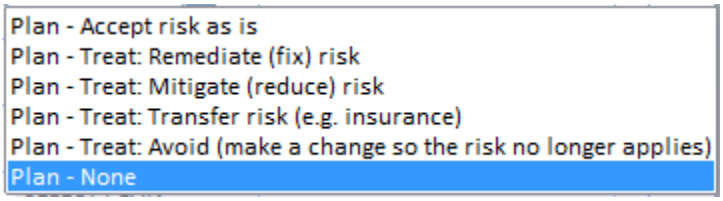
**Risk Rating** – This field is intended to provide the reader with a logical and plain language sense of how seriously they should take the risk.

Options are provided in a drop down for this field.




**Action Plan** – This field is not intended to be detailed. This field is intended to provide a very high level course of action.

Options are provided in a drop down for this field.




**Short Description** – This field is intended to provide the primary risk evaluator with a place to bring forward any information which they feel could assist the reader in better understanding the risk and or treatment. This should not be more than two sentences.

## SECTION C - ACCEPTANCE

### Purpose of section:

This section documents sign-offs.

### Instructions:

- Please do not remove or change the signature blocks marked “required” in the SOAR.
- Additional signature blocks may be added to address ministry needs.
- The Business Owner is typically the “responsible person” for the system being assessed.
- The MISO is typically the “responsible person” for the assessment and the “Primary Risk Evaluator”.
- The MCIO is typically the “accountable person”.
- Delegated signing must be permitted by the person you are signing on behalf of.
- Digital or printed signatures are acceptable and must be included with the SOAR.
- SOAR completion marks the completion of a Security Threat and Risk Assessment (STRA).
- SOAR completion requires all signatures.