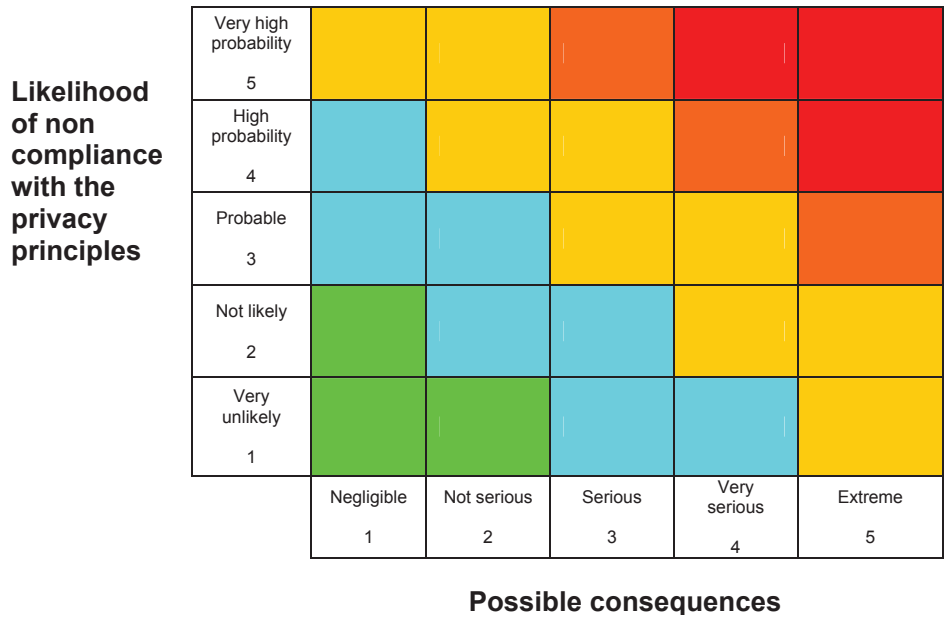


Appendix one – risk matrix

Risk Matrix

The *PIPEDA Self-assessment tool* developed by the Office of the Privacy Commissioner of Canada contains a risk matrix useful when conducting privacy self-assessments, on which the below is based.



The *likelihood of non compliance* refers to the chance of an event happening which would not comply with the privacy principles. The *possible consequences* refer to the potential outcome of that event.

Likelihood

Level	Descriptor	Description
5	Very high probability	The event has occurred regularly or often, or will almost definitely occur.
4	High probability	Event has occurred more than once, or has occurred in similar circumstances, or it is highly likely to occur.
3	Probable	Event has previously occurred, or has been observed in similar circumstances, or it may occur.
2	Not likely	Event has occurred infrequently to others in similar circumstances, but it has not occurred previously in the agency and it is not likely to do so.
1	Very unlikely	Event has almost never or never been observed, it may occur only in exceptional circumstances, or it is highly unlikely to occur.

Privacy self assessment guide

Possible consequences

Level	Descriptor	Description
5	Extreme	The outcome of the event would cause serious, long term damage to an agency and/or significant damage to the person's reputation or finances, or emotional distress.
4	Very serious	The outcome of the event could include significant concerns for an agency and/or significant damage to the person's reputation or finances, or emotional distress.
3	Serious	The outcome could cause problems for an agency but could be managed internally and/or could have moderate impact on the individual, such as the exposure of some financial information and further exposure is limited.
2	Not serious	The outcome might impact on the agency, but would be dealt with internally and be of low consequence and/or the impact on the individual could be contained within the agency and further exposure limited.
1	Negligible	The outcome might impact in a minimal way on the agency, but could be absorbed through normal agency activity and/or the impact would be of low consequence to the agency and the individual.