VULNERABILITY RISK ASSESSMENT TOOL:
A TOOL FOR AGENCY MANAGERS[1]

Errors can happen at any time; they're a part of life. However, the Canada Revenue Agency (Agency) needs to prevent, as much as possible, errors that can have a **significant impact** on its **reputation** and on the **integrity** of its programs and operations.

Ask yourself, if an error occurred in your area, would it impact the following:

- **Taxpayer trust and confidence:** Could it impact the Agency's reputation?
- **Media coverage:** Could it garner media attention at the local, provincial and/or national level?
- **Service delivery:** Could it impact service delivery (e.g. the Agency's ability to deliver its mandate)?

If so, we want you to target and review those areas!

As an Agency manager or supervisor, **you have a key role to play** in reducing the risk of errors. This **two-step** process will help you identify potential vulnerabilities that could lead to errors so that you can **proactively address them**. **This tool is _not_ about adding new controls; it is about making sure you have the _right_ controls and that they are being followed.**

STEP 1: INSTRUCTIONS - Consider the following questions

NT#	INTERNAL PROCESS QUESTIONS TO CONSIDER	YES. THIS APLLIES TO MY AREA
1	In the past 12 months, has your team experienced a high[2] rate or continuous staff turnover?	
2	Do employees miss opportunities for training on key processes, procedures and refresher courses?	
3	In the past 12 months, has your team experienced a significant change in how you do business (e.g. business transformation or realignment)?	
4	Does your team communicate with external stakeholders (e.g. other government departments, tax preparers, and tax professional organizations), media, and/or taxpayers?	
5	Does your team work with large volumes of sensitive information?	
6	Does your team work with information (e.g. taxpayer information, phone numbers, etc.) that does not always get fact checked, prior to your area receiving it or sending it out and is used in Agency documents or correspondence3?	
7	Does your team work with customized or unique content (e.g. not using pre-existing templates or text)?	
8	Is your work unit dependent on the accuracy of information received from or sent to other areas in the Agency?	
9	a) Does taxpayer information get extracted from source systems by way of a mainframe macro application? If no, proceed to question 10. b) If yes, do employees save that information on their personal network drive ?	
10	Do some of the established approval processes get missed, bypassed, or changed?	
11	Does your team work with **at least one** of the following: • Quick turnaround times • Production targets • Legislative deadlines • Repetitive processes • Service standards	
12	Does your team have a high[2] volume of manual activities (e.g. manipulating data from source systems, data entry)?	
13	Do your employees work in one of the following manners: • Independently • Unsupervised • In silos	

---

[1] When using this checklist, please refer to the "" "Vulnerability Risk Assessment tool" presentation.

[2] Consider what "high" means in your operational context.

[3] Agency documents or correspondence refers to anything that is sent external to the Agency.

If you checked **any of the boxes in Step 1**, it is recommended that you **proceed to Step 2** to review your internal processes to address any vulnerability that could lead to an error.

STEP 2: REVIEWING AND/OR ENHANCING YOUR INTERNAL PROCESSES

It is recommended that you review those specific areas where you checked a box in Step 1.

To do this, consider the five enterprise guidelines to designing risk out of the system – the 5 RIGHTs:

Guideline 1: The RIGHT controls
Are the right controls in place to reduce the risk of errors?
Are the processes well defined, communicated, and being followed?

Guideline 2: The RIGHT knowledge
Are employees aware of the impacts and consequences of errors occurring?
Do they have the right job training and receive it in a timely manner?
Is training refreshed or renewed on a regular basis? Are the right courses available?

Guideline 3: The RIGHT communication
Is there open and constant communication with employees at all levels (front line employees and above) about error prevention?
When errors happen, are they communicated up?

Guideline 4: The RIGHT contingencies
Are the appropriate plans in place at all levels of the organization in case an error occurs?
Leverage best practices and solutions!

Guideline 5: The RIGHT planning
Are there plans in place for future continuous improvement for error prevention?

Consider the 5 RIGHTs as your defence system. By ensuring you have the five RIGHTS in place, the failure of one will have a limited impact given the other four are in place.

As you review your internal processes, the following are key considerations:

1. Talk with your team, colleagues, and similar work areas to discuss best practices and possible solutions on enhancing internal processes.
2. Think about what is and what is not within your control. Communicate up if there are process improvements that are not within your control.
3. Consider the need to have a balance between process improvements and controls (i.e. having the *right balance of the right controls*).
4. Do not increase red tape.
5. Think of *simple* solutions to enhance your processes.

It is recommended that you review this checklist **at least annually** or when changes occur in your operational environment.