

Enterprise Risk Channel

What is a Risk?

A risk is something, such as an event, that could occur and negatively impact our objectives. Identifying risks enables IRS leadership to make more informed decisions earlier, when more options may be available to management

What is an Enterprise Risk?

An enterprise risk at the IRS is something (usually an event) that could happen and have a negative impact on the IRS as a whole, affect a large number of business units or taxpayers, or something that could attract significant media attention. Examples include a process or procedure not working as intended or causing undesired consequences.

What is the Enterprise Risk Channel?

The Enterprise Risk Channel provides a mechanism for employees to send potential risks to the Office of the Chief Risk Officer on a confidential basis. The Enterprise Risk Channel is not intended to be the first place where information about a risk is shared. Many channels are in place within business and functional units throughout the IRS where information about risks or problems can be raised, starting with sharing information about a risk with your manager. Risks can also be shared during group meetings, one-one-one meetings, operational reviews, program reviews, etc. In addition, many business units have established risk programs and processes where business unit risks can be raised. In order for risks to be addressed, they need to be shared and discussed, and once known, steps can be taken to consider and address the risks. If you are aware of a risk, you are encouraged to share and raise the risk through one of these existing channels or mechanisms first so that it can be considered and addressed as quickly and timely as possible.

If you are uncomfortable sharing information about a risk through one of these existing methods, or if you have previously raised the risk and remain concerned that it has not been fully addressed, a submission to the Enterprise Risk Channel may then be appropriate. Depending on the nature of the risk or problem you are aware of, however, your submission might be better suited for one of the other channels listed below.

Your submission might be better suited for one of these other channels:

Channel	Description
TIGTA	Report fraud, waste, mismanagement, and abuse in IRS programs and operations. Employees may also report personnel action(s) (actual or threatened) against an employee or applicant because they disclosed allegations of wrongdoing or gross mismanagement. Please refer to the TIGTA website: http://XXXX In case of a threat, assault or attempted assault against an IRS employee or infrastructure, including facilities and computer systems, immediately call your local TIGTA Office of Investigations.
Ethics Hotline	Report specific potential issues such as gifts, conflicts of interest, and post-government employment. Call XXXX or email at http://XXXX .
Executive Misconduct Unit	Report potential misconduct by a GS-15, IR-03/01, and/or executives that specify covered acts or omissions (e.g., false statements, document destruction, threatening audit, etc). Overview of unit: http://XXXX

Agency Grievance System	Request personal relief in a matter of concern or dissatisfaction relating to employment which is subject to the control of agency (IRS) management. See the IRM for more information: http://XXXX .
Employee Conduct & Compliance Office	Report potential Employee Tax Compliance issues and/or potential misconduct towards taxpayers (e.g., assault/threat to audit for personal gain/sexual harassment). Overview of Office: http://XXXX .
Equity, Diversity & Inclusion	Raise claims of employment discrimination: http://XXXX . Promotes a diverse workforce and inclusive working environment: http://XXXX
Commissioner's Corner Mailbox	General mailbox to receive direct feedback or input from any employee regarding any topic. Commissioner's Corner Website: http://XXXX
Taxpayer Advocate Service (TAS)	TAS identifies systemic issues (involving issues with IRS systems, policies, or procedures and involving protecting taxpayer rights, reducing burden, ensuring fair treatment, or providing essential taxpayer services) that affect multiple taxpayers and works with the IRS to resolve these issues. Systemic Advocacy Management System (SAMS) site: http://XXXX
Employee Suggestion Program	Submit proposals to increase productivity and save time and/or money for the IRS. Program Overview: http://XXXX .

Please note that if your submission is for an improvement, and you would like to be considered for an award, you must send your suggestion directly to the Employee Suggestion Program (ESP) at <http://XXXX>. We do not forward suggestions to the ESP.

How do I submit a potential enterprise risk?

1. Please read the confidentiality statement below.
2. Complete the [Enterprise Risk Channel Submission Form](#). (Do not include sensitive, personally identifiable information (PII) or taxpayer information (TPI) in the risk submission.)
3. E-mail the form to the following address: [*Enterprise Risk Channel](#)

What happens after I submit a potential enterprise risk?

Once your submission is received, it will be reviewed. The information you provide will be handled according to our internal policies and guidelines, and action will be taken, as appropriate. You will not receive a notification of resolution of your submission.

If your submission is for an improvement, we will **NOT** forward to the Employee Suggestion Program. If you would like to be considered for an award, you must submit your suggestion directly to the Employee Suggestion Program.

Do I have confidentiality when identifying a potential risk?

When you identify an enterprise risk, you can choose whether or not to disclose your identity.

Choosing to disclose your identity

If you choose to disclose your identity, enter the requested information in the "Submitter's SEID, Name and Phone Number" field on the Enterprise Risk Channel Submission Form.

The Enterprise Risk Channel may disclose your identity under the following circumstances:

- If there is a need to contact you for more information to complete the review of your submission and to implement corrective actions, if any;
- If disclosure is required by law; and/or
- If it is determined that disclosure is necessary to address matters contained in the submission, including specific dangers to health, safety, or national security.

Choosing not to disclose your identity

If you choose not to disclose your identity, do not enter any information in the “Submitter’s SEID, Name and Phone Number” field on the Enterprise Risk Channel Form.

The Enterprise Risk Channel will make every effort to protect your identity however, this may affect our ability to review and appropriately address the submission.

Please keep in mind the Enterprise Risk Channel cannot guarantee complete confidentiality of your identity if disclosure is required by law or regulation, or we determine that disclosure is necessary to address threats to health, safety, or national security.

Do I have protections under the Whistleblower Protection Act?

An employee who discloses information that could constitute an enterprise risk may be protected from retaliation by the Whistleblower Protection Act. This protection applies as long as the employee reasonably believed that the disclosure identified gross mismanagement; gross waste of funds; abuse of authority; substantial and specific danger to public health or safety; or violation of law, rule or regulation. Self-reporting an unethical or illegal action does not protect the submitter from disciplinary or legal actions.

Enterprise Risk Channel Submission

Do not include sensitive, personally identifiable information (PII) or taxpayer information (TPI) in the risk submission.

Purpose: The purpose of this form is to confidentially document and raise a potential risk(s) through the Enterprise Risk Channel. E-mail completed forms to *Enterprise Risk Channel.

Submitter's name <i>(see confidentiality information below)</i>	SEID	Telephone number	Date
BOD/FOD/Special unit	Office <i>(if applicable)</i>		

Describe the potential risk(s) *(include as much information as possible)*

Explain why you think this is a risk

Have you already reported this through a different channel, and if so, which channel

Comments *(use this section to include any additional information or relevant attachments)*

Confidentiality when identifying an enterprise risk

When you identify an enterprise risk, you can choose whether or not to disclose your identity.

Choosing to disclose your identity

If you choose to disclose your identity, enter the requested information in the “**Submitter’s name, SEID, and Telephone number**” fields on the Enterprise Risk Channel Submission Form.

The Enterprise Risk Channel may disclose your identity under the following circumstances:

- If there is a need to contact you for more information to complete the review of your submission and to implement corrective actions, if any;
- If disclosure is required by law; and/or
- If it is determined that disclosure is necessary to address the matters contained in the submission, including but not limited to specific dangers to health, safety, and/or national security.

Choosing not to disclose your identity

If you choose not to disclose your identity, do not enter any information in the “Submitter’s name, SEID, and Telephone number” fields of the Enterprise Risk Channel Submission Form.

The Enterprise Risk Channel will make every effort to protect your identity; however, this may impact our ability to review and appropriately address the submission.

Keep in mind the Enterprise Risk Channel cannot guarantee complete confidentiality of your identity if disclosure is required by law or regulation, or we determine that disclosure is necessary to address threats to health, safety, or national security.

Whistleblower Protection Act

An employee who discloses information that could constitute an enterprise risk may be protected from retaliation by the Whistleblower Protection Act. This protection applies as long as the employee reasonably believed that the disclosure identified gross mismanagement; gross waste of funds; abuse of authority; substantial and specific danger to public health or safety; or violation of law, rule or regulation. Self-reporting an unethical or illegal action does not protect the submitter from disciplinary or legal actions.